39XX/51XX Switches and Platforms

Fault and Performance Management

SAOS 6.21.2

What's inside...

New in this release
Fault management fundamentals
Fault management using SNMP and RMON
Fault monitoring and analysis
Link flap detection for fault management
Alarm management
Logging configuration
Virtual Link Loss Indicator (VLLI) configuration
Fault management troubleshooting
Performance monitoring configuration
CPU rate limiting

009-3458-009 - Standard Revision A
March 2022

Copyright© 2022 Ciena® Corporation. All rights reserved.

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 PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing CIENA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit www.ciena.com.

Copyright© 2022 Ciena® Corporation. All Rights Reserved

Use or disclosure of data contained in this document is subject to the Legal Notices and restrictions in this section and, unless governed by a valid license agreement signed between you and Ciena, the Licensing Agreement that follows.

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		*www.ciena.com/support/*
Sales and General Information	North America: 1-800-207-3714 International: +44 20 7012 5555	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 India	+91-22-42419600	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training		E-mail: learning@ciena.com

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

READ THIS LICENSE AGREEMENT (“LICENSE”) CAREFULLY BEFORE INSTALLING OR USING CIENA SOFTWARE OR DOCUMENTATION. THIS LICENSE IS AN AGREEMENT BETWEEN YOU AND CIENA COMMUNICATIONS, INC. (OR, AS APPLICABLE, SUCH OTHER CIENA CORPORATION AFFILIATE LICENSOR) (“CIENA”) GOVERNING YOUR RIGHTS TO USE THE SOFTWARE. BY INSTALLING OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND AGREE TO BE BOUND BY IT.

1. License Grant. Ciena may provide “Software” to you either (1) embedded within or running on a hardware product (together with Software, “Product”) or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. The terms of this License apply to your use of the Software and associated documentation whether such has been provided by Ciena, an affiliate of Ciena, or by means of an authorized reseller or distributor. Subject to these terms, and payment of all applicable License fees including any usage-based fees, Ciena grants you, as end user, a non-exclusive, non-transferable, personal License to use the Software only in object code form, subject to any applicable authorized use, activation requirements, usage levels, scope of functionality and release level of the Software, as set forth in the applicable quote accepted by Buyer upon Buyer's issuance of an acceptable purchase order (“Order”), and in accordance with the detailed ordering information in the Ciena's generally available, applicable, Product documentation as of the date of such Order. Unless the context does not permit, Software also includes associated documentation. Where an Order is for a (a) perpetual license, you may use the Software and associated documentation for as long as you use the Product for internal business use, or a (b) subscription license, you may only use the Software and associated documentation during the subscription term. A subscription license includes Software upgrades and/or technical support Services during the subscription term (that are not included in a perpetual license), in accordance with the Order and as further described in the applicable Ciena's service description as of the date of the applicable Order. Prior to the expiration of each subscription term, Ciena will send you a quote for the annual renewal fee(s). To renew the subscription Software license(s) for additional subscription terms, you issue an Order in advance of the then-current expiration date of such subscription term.

2. Open Source and Third-Party Licenses. If any Software is subject to an open-source license that provides the end user with rights that are broader than this License, then such rights shall take precedence. Ciena warrants that using Software in accordance with its documentation will not subject you to any obligation to disclose, distribute or license your own software that interacts with Software.

3. Title. You are granted no title or ownership rights in or to the Software. Unless specifically authorized by Ciena in writing, you are not authorized to create any derivative works based upon the Software. Title to the Software, including any copies or derivative works based thereon, and to all copyrights, patents, trade secrets and other intellectual property rights in or to the Software, are and shall remain the property of Ciena and/or its licensors. Ciena's licensors are third party beneficiaries of this License. Ciena reserves to itself and its licensors all rights in the Software not expressly granted to you.

4. Confidentiality. The Software contains trade secrets of Ciena. Such trade secrets include, without limitation, the design, structure and logic of individual Software programs, their interactions with other portions of the Software, internal and external interfaces, and the programming techniques employed. The Software and related technical and commercial information, and other information received in connection with the purchase and use of the Software that a reasonable person would recognize as being confidential, are all confidential information of Ciena (“Confidential Information”).

5. Obligations. You shall:

i) Hold the Software and Confidential Information in strict confidence for the benefit of Ciena using your best efforts to protect the Software and Confidential Information from unauthorized disclosure or use, and treat the Software and Confidential Information with the same degree of care as you do your own similar information, but no less than reasonable care;
ii) Keep a current record of the location of each copy of the Software you make;
iii) Use the Software only in accordance with the authorized usage level;
iv) Preserve intact any copyright, trademark, logo, legend or other notice of ownership on any original or copies of the Software, and affix to each copy of the Software you make, in the same form and location, a reproduction of the copyright notices, trademarks, and all other proprietary legends and/or logos appearing on the original copy of the Software delivered to you; and
v) Issue instructions to your authorized personnel to whom Software is disclosed, advising them of the confidential nature of the Software and provide them with a summary of the requirements of this License.

Copyright© 2022 Ciena® Corporation

6. Restrictions. You shall not:

i) Use the Software or Confidential Information a) for any purpose other than your own internal business purposes; and b) other than as expressly permitted by this License;
ii) Allow anyone other than your authorized personnel who need to use the Software in connection with your rights or obligations under this License to have access to the Software;
iii) Make any copies of the Software except such limited number of copies, in machine readable form only, as may be reasonably necessary for execution in accordance with the authorized usage level or for archival purposes only;
iv) Make any modifications, enhancements, adaptations, derivative works, or translations to or of the Software;
v) Reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Software;
vi) Make full or partial copies of the associated documentation or other printed or machine-readable matter provided with the Software unless it was supplied by Ciena in a form intended for reproduction;
vii) Export or re-export the Software and/or the associated documentation from the country in which it was received from Ciena or its authorized reseller unless authorized by Ciena in writing; or
viii) Publish the results of any benchmark tests run on the Software.

7. Audit: Upon Ciena's reasonable request you shall permit Ciena to audit the use of the Software to ensure compliance with this License.

8. 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 Software and any accompanying technical data (collectively “Materials”) are commercial within the meaning of applicable Federal acquisition regulations. The Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this License, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, the Software is commercial computer software and the use of the Software is further restricted by this License.

9. Term of License. This License is effective until the applicable subscription term expires or the License is terminated. You may terminate this License by giving written notice to Ciena. This License will terminate immediately if (i) you breach any term or condition of this License or (ii) you become insolvent, cease to carry on business in the ordinary course, have a receiver appointed, enter into liquidation or bankruptcy, or any analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. Upon any termination of this License, you shall destroy and erase all copies of the Software in your possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased. Your obligations to hold the Confidential Information in confidence, as provided in this License, shall survive the termination of this License.

10. Compliance with laws. You agree to comply with all laws related to your installation and use of the Software. Software is subject to U.S. export control laws and may be subject to export or import regulations in other countries. If Ciena authorizes you to import or export the Software in writing, you shall obtain all necessary licenses or permits and comply with all applicable laws.

11. Limitation of Liability. ANY LIABILITY OF CIENA SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU TO CIENA OR ITS AUTHORIZED RESELLER 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 LICENSOR OF CIENA. NEITHER CIENA NOR ANY OF ITS LICENSORS 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.

12. General. Ciena may assign this License to an affiliate or to a purchaser of the intellectual property rights in the Software. You shall not assign or transfer this License or any rights hereunder, and any attempt to do so will be void. This License shall be governed by the laws of the State of New York without regard to conflict of laws provisions. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This License constitutes the complete and exclusive 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.

Copyright© 2022 Ciena® Corporation

Publication history

March 2022

Standard revision A.

First standard release of this document for SAOS 6.21.2.

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Contents

About this document xiii

New in this release 1-1

Fault management fundamentals 2-1

System fault management 2-1
- Traps 2-2
- Alarms 2-2
- Events 2-3
- Log types 2-6

System failure notification 2-6
Syslog 2-9
Flash log 2-12
RAM log 2-14
Command log 2-14
- Command log exceptions 2-15

Virtual Link Loss Indication 2-15

Fault management using SNMP and RMON 3-1

SNMP 3-1
- SNMP architecture 3-2
- SNMPv1 3-3
- SNMPv2c 3-6
- SNMPv3 3-7
- Alarm inputs 3-15
- SNMP inform notification 3-15
- Inform queue per trap server 3-16

RMON 3-19

List of procedures

3-1 Disabling the SNMP agent 3-21
3-2 Enabling or disabling an SNMP notification 3-22
3-3 Displaying SNMP notifications 3-23
3-4 Configuring a device to send SNMPv1 traps 3-24
3-5 Configuring a device to send SNMPv2c traps 3-27
3-6 Configuring a device to send SNMPv3 traps 3-30
3-7 Configuring global SNMP settings 3-34
3-8 Creating SNMPv3 users 3-36

Copyright© 2022 Ciena® Corporation

3-9 Configuring SNMP notification entries 3-38
3-10 Configuring SNMP source address checking 3-39
3-11 Configuring SNMP reliable traps 3-42
3-12 Setting or unsetting the maximum SNMP inform queue length 3-50
3-13 Showing or clearing SNMP inform statistics counters 3-51
3-14 Configuring alarms 3-53
3-15 Configuring events 3-58
3-16 Configuring statistics 3-61
3-17 Troubleshooting SNMP and RMON configuration 3-63
3-18 Displaying RMON information 3-64

Fault monitoring and analysis 4-1

List of procedures
4-1 Monitoring door status 4-3
4-2 Monitoring fan speed status 4-4
4-3 Monitoring temperature and status 4-5
4-4 Monitoring power supply status 4-9
4-5 Monitoring device-id status 4-12
4-6 Enabling and disabling POSTs 4-13
4-7 Monitoring POSTs 4-14
4-8 Enabling and disabling dying gasp 4-15
4-9 Configuring dying gasp informs 4-16
4-10 Displaying dying-gasp 4-17
4-11 Set and unset source port for dying gasp 4-18
4-12 Displaying device archives 4-19
4-13 Saving device archives to flash 4-20
4-14 Displaying device identification attributes 4-21
4-15 Displaying platform capabilities 4-22
4-16 Displaying the chassis MAC address 4-24
4-17 Configuring port traps and servers 4-25
4-18 Displaying an alarm entry 4-26
4-19 Monitoring system health and resources 4-27
4-20 Displaying the event severity to Syslog severity mapping 4-35

Link flap detection for fault management 5-1

Link flap detection 5-1

List of procedures
5-1 Configuring link flap detection 5-2

Alarm management 6-1

Alarm Manager 6-1
Alarm classes 6-2
Alarm instances 6-2
Alarm severity levels 6-2
Types of alarms 6-3
Occurrences 6-3
Timers 6-4
Escalating severity 6-4

Copyright© 2022 Ciena® Corporation

Escalating severity with count 6-5
Rate threshold 6-5
Thresholds with escalating severity 6-5
Alarm tables 6-5
Active alarm table 6-5
Alarm history table 6-7
Alarm indication table 6-7
Alarm records 6-7
External alarms 6-9
Alarm differences 6-12
Alarm instances 6-12
Alarms and corresponding events 6-13
World Wide Packet traps and corresponding events 6-18
Ciena traps and corresponding events 6-25
Standard traps and corresponding events. 6-28

List of procedures
6-1 Enabling and disabling alarms 6-34
6-2 Deleting an alarm 6-35
6-3 Acknowledging an alarm 6-36
6-4 Enabling and disabling visible alarm output by severity 6-37
6-5 Configuring alarm attributes 6-38
6-6 Displaying alarms 6-40
6-7 Clearing alarm history 6-46
6-8 Clearing alarms 6-47

Logging configuration 7-1

Logging of events 7-1
Event log formatting 7-4

List of procedures
7-1 Configuring Syslog 7-6
7-2 Configuring a flash log filter 7-9
7-3 Configuring flash log packet filters 7-22
7-4 Displaying flash log and flash log packet filter configuration 7-27
7-5 Displaying the flash log 7-29
7-6 Creating a RAM log filter 7-31
7-7 Configuring RAM log packet filters 7-34
7-8 Displaying RAM log and RAM log packet filter configuration 7-36
7-9 Displaying the RAM log 7-39
7-10 Clearing the log RAM file 7-41
7-11 Repeating commands 7-42
7-12 Enabling and disabling command logging 7-45
7-13 Displaying the command log 7-46
7-14 Clearing the command log 7-49
7-15 Exporting the command log 7-50

Virtual Link Loss Indicator (VLLI) configuration 8-1

List of procedures
8-1 Configuring instance groups 8-2

Copyright© 2022 Ciena® Corporation

8-2 Configuring action groups 8-5
8-3 Displaying recovery and fault counter information 8-7

Fault management troubleshooting 9-1

List of procedures
9-1 Sending log test messages 9-2
9-2 Resetting log file configuration to defaults 9-3

Performance monitoring configuration 10-1

PM instances 10-1
PM profiles 10-4
- ExtendedTxRx 10-4
- QueueGroup 10-5
- BasicTxRx 10-6
- BasicTx 10-7
- BasicRx 10-7
- BasicTxRxBiDir 10-8
- TdmPortOpticalStats 10-9

Port performance management statistics 10-13
- Port statistics 10-13
- Statistics for TDM CEM pseudowire/EVCs 10-21

PM bins 10-23
- PM bin types 10-23
- PM bin states and PM bin state priority 10-24
- System time 10-28
- Time changes 10-29

Maximum PM instances 10-31
PM configuration at system level 10-31
- PM Mgr persistence file 10-32
- NTP 10-32

BulkStats collection 10-32
- BulkStats-instance configuration 10-33
- BulkStats-collector configuration 10-35
- BulkStats file 10-37
- IP address selection rules 10-37

PM threshold crossing alerts 10-38

List of procedures
10-1 Configuring PM at the system level 10-41
10-2 Creating a PM instance 10-42
10-3 Enabling/disabling PM for a specific PM instance 10-46
10-4 Deleting a specific PM instance 10-47
10-5 Clearing the statistics for a specific PM instance 10-48
10-6 Displaying PM instances 10-49
10-7 Creating PM bulkstats 10-56
10-8 Adding and removing statistics from PM bulkstats 10-62
10-9 Enabling and disabling PM bulkstats 10-64
10-10 Deleting PM bulkstats 10-66
10-11 Clearing PM bulkstats 10-67

Copyright© 2022 Ciena® Corporation

10-12 Displaying bulkstats configuration information 10-68
10-13 Configuring bulkstats-collector xftp settings 10-71
10-14 Transferring the bulkstats-collector's statistics file 10-73
10-15 Configuring the bulkstats-collector's remote filename prefix 10-74
10-16 Configuring PM threshold crossing alerts 10-76
10-17 Clearing a threshold associated with a PM 10-77
10-18 Deleting a threshold interval profile 10-78
10-19 Setting a PM threshold attribute 10-79
10-20 Displaying a PM threshold 10-80

CPU rate limiting **11-1**

List of procedures
11-1 Setting CPU rate limits 11-2
11-2 Resetting CPU rate limits to default 11-5
11-3 Enabling CPU rate limiting 11-6
11-4 Disabling CPU rate limiting 11-7
11-5 Displaying CPU rate limiting configuration 11-8
11-6 Displaying CPU rate limiting statistics 11-10
11-7 Clearing CPU rate limiting statistics 11-11
11-8 Displaying CPU rate limiting configuration in the configuration file 11-12
11-9 Configuring CPU rate limiting 11-13

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

About this document

This document contains information that supports the tasks performed by operations personnel related to managing or preventing faults, troubleshooting, and monitoring and improving the performance of SAOS.

Conventions used in this document

Hyperlinks are indicated by blue text in this document.

In procedures, the following text conventions are used:

- `courier` text, for system responses
- *italic* text, for expected results
- **bold** text, for user input

Copyright© 2022 Ciena® Corporation

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. The following table summarizes command syntax symbols.

Symbol	Description
< >	Encloses a variable or literal value that must be specified. Some examples include: server <IpAddress> priority <NUMBER: 1-7> dns <on|off> description <String[31]> For server <IpAddress>, the attribute could be entered as server 10.10.11.100 or server www.ciena.com. With priority <NUMBER: 1-7> the text within <> indicates that 1 - 7 are valid values. In the example of dns <on|off>, either the literal value of on or off is valid, such as dns on. For description <String[31]>, 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: cfm mip create {vlan <VlanId>} {port <PortNameList>} [level <NUMBER: 0-7>] The vlan and port arguments are required. The level argument is optional.

|	Separates mutually exclusive items in a list, only one of which can be entered. For example, in the syntax:
	`dhcp client options set subnet <on|off>`
	Either on or off must be specified, for example:
	`dhcp client options set subnet on`

[ ]	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax:
	`arp show [interface <Interface>]`
	You can enter a value for interface <Interface> or not. For example:
	`arp show`

Copyright© 2022 Ciena® Corporation

Symbol	Description
{ [ ], [ ], [ ] }	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.

Documents in the 39XX/51XX documentation suite

For descriptions of documents in the 39XX/51XX Switches and Platforms documentation suite, see *39XX/51XX Switches and Platforms Product Fundamentals*.

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

New in this release

Revision A

This section provides a summary of the changes made in *39XX/51XX Switches and Platforms Fault and Performance Management* for SAOS 6.21.2.

- The *<encrypted-password-attr>* command is removed from the system and all instances of this command is deleted from all procedures in this guide, primarily in the following sections:
  - Procedure 7-15, “Exporting the command log”
  - Procedure 10-7, “Creating PM bulkstats”
  - Procedure 10-13, “Configuring bulkstats-collector xftp settings”
  - Procedure 10-15, “Configuring the bulkstats-collector’s remote filename prefix”

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Fault management fundamentals

This chapter provides an overview of fault management on the 39XX/51XX platform. Topics are:

- "System fault management"
- "System failure notification"
- "Syslog"
- "Flash log"
- "RAM log"
- "Command log"
- "Virtual Link Loss Indication"

System fault management

A system fault occurs when an alarm either reaches a critical level or when a system component fails. Fault detection is managed by various sub-components within the system's hardware devices.

Sub-components that handle fault detection include:

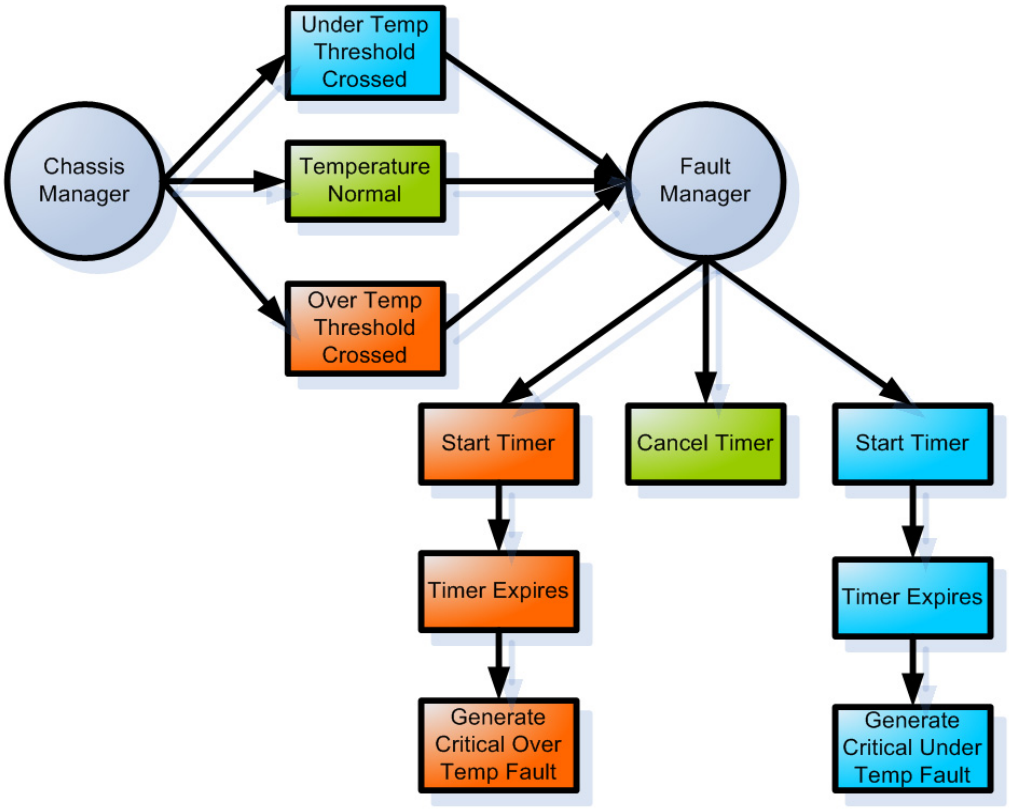
- individual managers
- error handlers
- device drivers

The Fault Manager is responsible for fault monitoring, fault logging, fault policy management, and fault policy execution. The Fault Manager is designed to protect system hardware from potential damage.

As an example, the Fault Manager receives an event that is generated by a temperature sensor threshold that is crossed. The Fault Manager will begin to time the event. If the event is not resolved within the specified time-frame, a critical fault will be generated as shown in Figure 2-1.

Copyright© 2022 Ciena® Corporation

Figure 2-1
Fault management flow



Traps

Traps are messages of a fault in an SNMP network element. The device sends traps as defined by traps and notifications in the MIBs.

SNMP is configured to send the traps to a server.

Alarms

Alarms are generated when a failure or fault is detected in the network elements. Events are correlated into alarms based on their significance. Alarms are messages that call for an operator or administrator's attention. When an alarm is created, the problem associated with the alarm must be resolved.

Copyright© 2022 Ciena® Corporation

Alarm severity levels

Table 2-1 lists alarm severity levels and provides definitions.

Table 2-1
Alarm severity levels

Alarm severity level	Definition
Critical	Indicates a service-affecting condition has failed and an immediate corrective action is required, for example, a managed object is completely out-of-service and capability must be immediately restored.
Major	Indicates a service-affecting condition has developed and an urgent corrective action is required, for example, a server degradation condition has occurred and must be immediately corrected.
Minor	Indicates a non-service affecting condition has developed and corrective action is required, for example, a server degradation condition exists, but is not currently degrading the server capacity.
Warning	Indicates the detection of a potential or impending service-affecting condition before any significant effects have occurred. Closer examination is required to reduce the potential for the alarm escalating to a higher level.
Cleared	Indicates the alarm has been disabled.

Events

An event typically refers to an error condition in the system that has an associated alarm severity; some events may be converted into SNMP traps.

The system supports a maximum of four event log files. Each event log supports a maximum of 1000 lines. If there are less than 990 lines in the file when the system reboots, the same file is used after a reboot. If there are more than 990 lines in the event log file before the system reboots, a new event log is generated. If there are four event log files in the system already, a new event log file is generated when the system reboots. The event log file with the oldest number is removed and replaced.

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.

Copyright© 2022 Ciena® Corporation

Table 2-2 list the types of logs supported by the system software.

Table 2-2
Types of logs

Type of log	Description
Syslog	Messages sent to collectors which are added (configured) by means of the 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 written to flash files.

Messages are written to the logs with timestamps based on the system time settings: 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.

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 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.

Copyright© 2022 Ciena® Corporation

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              |
...
+--------------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Log types

The differences between the log types guide the configuration of the event logging process. These differences are described inTable 2-3.

Table 2-3
Log types

Log Type	Description
Flash logs	• may contain up to 4000 messages • messages are persistent across reboots up to a maximum of four reboots
Syslog collectors and trap servers	• have configuration options external to SAOS that may include how many messages are retained and for how long • multiple syslog collectors can be configured, but only one min-max severity range per collector • syslog message facility number and prefix string can be specified per CLI-configured collector
Flash and RAM logs	• have considerable flexibility as multiple filters may be created to specify the severity range, source manager and port • information specified by the filters is logged • users can review flash logs to identify or review older events
Command logs	• are persistent across reboots • contain up to 2500 entries

System failure notification

System failure notification notifies 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 notification is transmitted. The dying gasp notification allows the network operator to differentiate at the Network Operations Center between a power failure and a device failure.

Copyright© 2022 Ciena® Corporation

- On power-up, the system provides notification regarding the reason for the failure. 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.

Dying gasp messages are sent as best effort. The order and priority of such packets are as follows:

- SNMP dying gasp trap
- EOAM dying gasp packet
- Syslog dying gasp message

SNMP dying gasp supports the option to force the notification to be an inform if the target is set up to send informs. The following outlines the authentication limitations to the dying gasp:

- If the authoritative engine is not known, the security information is set to NULL. If the authoritative engine data is later learned, the packets are updated only when the SNMP target server related information is updated. This process will take several seconds.
- After the packet is generated, it never updates the authoritative engine boots, engine time, request ID, or message ID. Some SNMP managers may drop the packet due to security issues.
- SNMP dying gasp packets are regenerated when the target servers are updated. Security information is also updated on the chassis when the dying gasp inform is toggled on or off.
- MG-SOFT or other SNMP managers may not register the inform because it is not considered trusted. In this case, the packet must be inspected with a tool like Wireshark. Wireshark marks the packet as invalid if the engine ID, engine time, and engine boots are not populated. If this occurs, it is likely that the SNMP agent and manager did not communicate when the packet was created and stored in the buffer. This is one of the stipulations of the dying gasp inform.

EOAM dying gasp applies on ports that are configured for EOAM dying gasp.

The dying gasp notification has a severity of critical. It can be saved to the internal flash. The dying gasp notification also generates a syslog message that is delivered based on the users syslog configuration. In addition, the system generates an associated SNMP trap (wwpLeosChassisDyingGaspNotification).

If a system failure occurs, devices will:

- Generate an event on any administrative reboot, either forced reboot or reset to factory defaults and indicate the reason.

Copyright© 2022 Ciena® Corporation

- Attempt to generate an event on any system crash or unexpected reboot. Note that there are some conditions where transmitting a notification is not possible.
- Attempt to generate an event when a power failure occurs.

Note that:

- Dying gasp works with IPv6.
- On the following devices, dying gasp packets are transmitted on all ports:
  - 3903
  - 3904
  - 3905
  - 3906
  - 3926
  - 3928
  - 3942
  - 5142
  - 5160
- As of SAOS 6.10, the UDP source port associated with dying gasp packets is set to 0. Ensure that all devices required to reach the SNMP/Syslog server are configured to allow a UDP packet with a source port of 0.
- In the case of IPv4, the Dying Gasp notification (Syslog/SNMP) is supported over IP interface, local interface, and remote interface. The notifications are sent to the next-hop interface based on the routing table (longest prefix matched to the destination).
- **Software Limitation**:
  - If there is any change over the reachability of the Syslog/SNMP server, the Dying Gasp notification (Syslog/SNMP) frame will update after 5 seconds. In case of a power failure during this duration, the Dying Gasp trap might not be able to send out the notification correctly.
  - The Dying Gasp may not work over the IP interface on the SAOS 390x platform (6x device) due to limited routing capability.

See the following dying gasp procedures:

- "Enabling and disabling dying gasp" on page 4-15
- "Configuring dying gasp informs" on page 4-16
- "Displaying dying-gasp" on page 4-17

Copyright© 2022 Ciena® Corporation

Syslog

Syslog messages can be sent to the Syslog Server or a standard UNIX or NT-type Syslog daemon. Syslog messages contain all the parts of the Syslog packet, as described in section 4.1 of RFC 3164. Table 2-4 describes the syslog messages.

Table 2-4
Syslog messages

If the original message has a	Then
timestamp in the header	• Specify this value in the local time of the device within its time zone and in GMT (UTC).
hostname field	• The hostname is contained as itself. • If it does not have a hostname field, it contains its own IP address.
TAG value	• It is the name of the program or process that generated the message.

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, transmits Syslog messages to the specified IP address or addresses 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 by means of 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, that is, external systems with IP address, may be configured (added) by means of the SAOS CLI and/or by means of DHCP.
- Each collector added by means of the CLI has a configurable min-max severity range.
- Each collector added by using the CLI has a configurable facility number.

Copyright© 2022 Ciena® Corporation

- 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 by means of 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 2-5 defines event severities.

Table 2-5
Event severities

Syslog severity	Definition
Critical	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	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	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	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	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	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	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	Indicates a configuration change. It is primarily used for communicating configuration changes through the system and to external entities.

Copyright© 2022 Ciena® Corporation

Table 2-6 defines syslog severities. The network element must log all messages except debugging, and send all log data to a syslog server.

Table 2-6
Syslog severities

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	warming	warning	4
7	config	notice	5
8	info	informational	6
9	debug	debug	7
10	local	debug	7

Table 2-7 provides a description of Syslog attributes.

Table 2-7
Syslog Attributes

Field	Default	Valid values	Description
Admin State	Enable	• Enable • Disable	Indicates 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	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

Copyright© 2022 Ciena® Corporation

Field	Default	Valid values	Description
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)	Identifies the UDP port that the syslog message will be transmitted to on the collector IP Address. Used for the source port of the sender when using UDP for transport.

A mnemonic field has been added to syslog messages to help quantify events. This field consists of three parts separated by dashes:

- Source of the event
- Event severity
- 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).

Flash log

The system software logs various events (critical, reboot, power failure) to local flash files.

Copyright© 2022 Ciena® Corporation

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 2-8 provides a description of event filter attributes.

Table 2-8
Event filter attributes

Field	Default	Valid values	Description
Admin State	Enabled	• Enable • Disable	Identifies the administrative state of this collector.
Operational State	Enabled	• 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.

Copyright© 2022 Ciena® Corporation

Field	Default	Valid values	Description
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	Specifies 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	Specifies 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.

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.

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

Copyright© 2022 Ciena® Corporation

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.

Command log exceptions

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. The command log files can also be exported to a remote server for later use.

> ***Note:*** Limited users cannot display or repeat commands requiring superuser access.

Virtual Link Loss Indication

Virtual Link Loss Indication (VLLI) allows network elements at the UNI-N of an EVC to signal to the UNI-C of the customer premise equipment (CPE) if:

- The remote UNI attachment interface has failed or recovered.
- The EVC connection has failed or recovered causing end-to-end client traffic to be transported.

VLLI applies to EVCs with a point-to-point topology.

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Fault management using SNMP and RMON

This chapter describes how to use SNMP and RMON to perform fault management procedures. See the following topics:

- “SNMP”
- “RMON”

SNMP

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.

Copyright© 2022 Ciena® Corporation

SNMP architecture

The system software supports SNMP versions v1, v2c, and v3 as described in RFC 3584. Table 3-1 lists the components in the SNMP architecture.

Table 3-1
Components in the SNMP architecture

Component	Description
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.

Copyright© 2022 Ciena® Corporation

Table 3-1
Components in the SNMP architecture

Component	Description
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. The system supports the following • RFC 4022 for the Transmission Control Protocol (TCP) • RFC 4087 for IP tunneling and routing • RFC 4113 for the User Datagram Protocol (UDP) • RFC 4292 for IP Forwarding Table MIB • RFC 4293 for Internet Protocol ((IP) • RFC 4807 for IP Security • RFC 4898 TCP Extended Statistics MIB 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). Refer to the MIB Reference Manual for details about MIB files included with this release.

SNMPv1

SNMPv1 is defined by RFC1157 (SNMPv1), RFC1155 Structure of Management Information Version 1 (SMIv1), RFC1212, and RFC1215.

Copyright© 2022 Ciena® Corporation

Table 3-2 lists the operations supported by SNMPv1.

Table 3-2
Operations supported by SNMPv1

Operation	Description
Get Request	manager requests the current value of a specified managed object from the agent. To optimize performance when retrieving large table views while browsing MIBs, use SNMP v2 Get Bulk instead of SNMP Get.
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.

Note: Prior to release 6.8, only SNMPv1 traps were supported.

The SNMPv1 trap packet includes the source agent IP, which is 32 bytes. The source agent IP can only accommodate the IpAddess type, which is specific to IPv4. If an IPv6 agent sends the packet then this address is all 0s or the loopback address of the agent. The source agent IP is only in the SNMP v1 trap.

The main source IP, that is, from the IP layer, contains the IPv6 address.

The following is an example of an SNMP v1 trap:

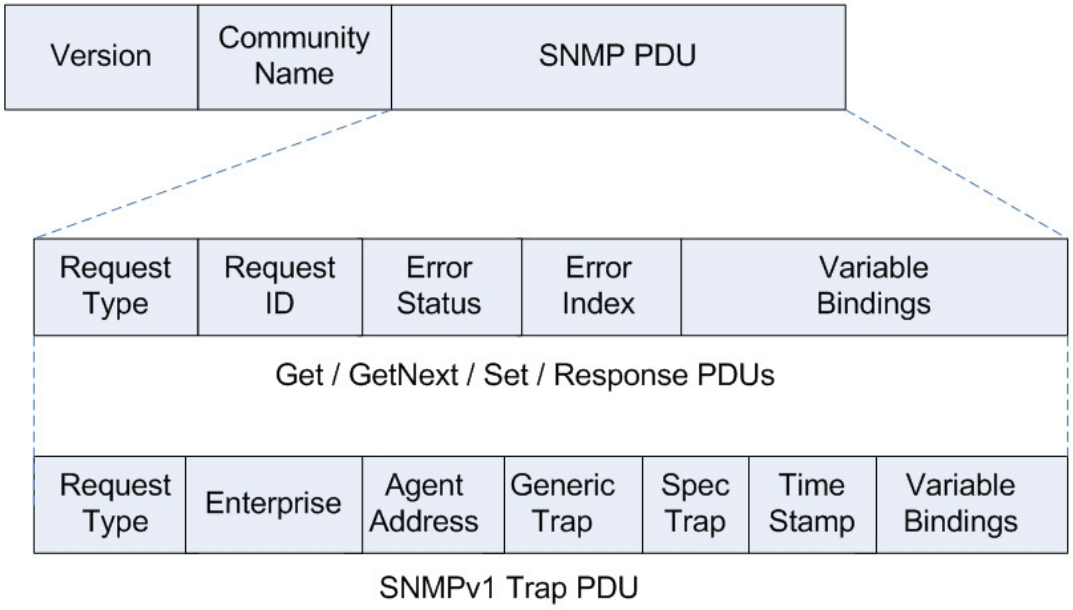
```
Specific: 1
Message reception date: 5/9/2012
Message reception time: 10:07:00.374 AM
Time stamp: 0 days 08h:14m:02s.90th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
Address: 10.33.40.6
Port: 35239
Manager
Address: 10.32.41.21
Port: 162
Community: public
SNMPv1 agent address: 10.33.40.6
Enterprise: wwpLeosFileTransferMIBNotificationPrefix
```


Copyright© 2022 Ciena® Corporation

```
Specific Trap MIB Lookup Results
Name: newRoot, Module: BRIDGE?]MIB, Enterprise: dot1dBridge
Bindings (4)
Binding #1: wwpLeosFTransferRemoteFilename.0 *** (OCTET STRING)
hh
Binding #2: wwpLeosFTransferLocalFilename.0 *** (OCTET STRING)
hh
Binding #3: wwpLeosFTransferNotificationStatus.0 *** (INTEGER)
couldNotGetFile(2)
Binding #4: wwpLeosFTransferNotificationInfo.0 *** (OCTET
STRING) File cannot be downloaded
```

The SNMPv1 message and Protocol Description Unit (PDU) format is shown in Figure 3-1.

Figure 3-1
SNMPv1 message and PDU format



Copyright© 2022 Ciena® Corporation

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.

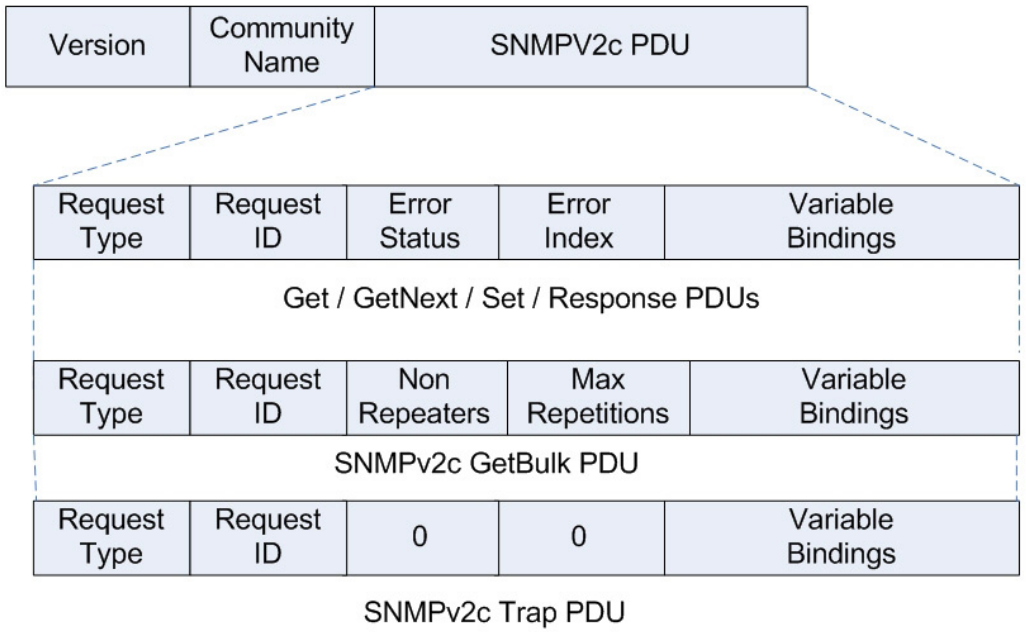
The following is an example of an SNMPv2c trap:

```
wwpLeosFTransferCompletion
Message reception date: 5/9/2012
Message reception time: 10:05:18.238 AM
Time stamp: 0 days 10h:30m:05s.30th
Message type: Notification (Trap)
Protocol version: SNMPv2c
Transport: IP/UDP
Agent
Address: 10.33.40.244
Port: 56827
Manager
Address: 10.32.41.21
Port: 162
Community: public
Bindings (6)
Binding #1: sysUpTime.0 *** (TimeTicks) 0 days 10h:30m:05s.30th
Binding #2: snmpTrapOID.0 *** (OBJECT IDENTIFIER)
wwpLeosFTransferCompletion
Binding #3: wwpLeosFTransferRemoteFilename.0 *** (OCTET STRING)
hh
Binding #4: wwpLeosFTransferLocalFilename.0 *** (OCTET STRING)
hh
Binding #5: wwpLeosFTransferNotificationStatus.0 *** (INTEGER)
couldNotGetFile(2)
Binding #6: wwpLeosFTransferNotificationInfo.0 *** (OCTET
STRING) File cannot be downloaded
```


Copyright© 2022 Ciena® Corporation

The SNMPv2c message and PDU format is shown in Figure 3-2.

Figure 3-2
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.

The devices SMPv3 supports are described in RFCs 3411, 3412, 3413, 3414, 3415, 3416, 3417. Devices are capable of using SNMPv3 for all SNMP sessions. If SNMPv3 response messages are received a timeliness check is done on the SNMPv3 message.

The message processing model used is snmpMessagingProcessingModel=3.

If state altering messages are sent to a managed, authoritative SNMPv3 engine, sending successive message to that managed SNMPv3 engine is delayed until a positive acknowledgment is received from the previous message or until the message expires. Products using SNMPv3 implement the key-localization mechanism.

Copyright© 2022 Ciena® Corporation

Packet format

The SNMPv3 packet format includes a message header, security parameters, and PDU information as shown in Figure 3-3.

Figure 3-3
SNMPv3 packet format

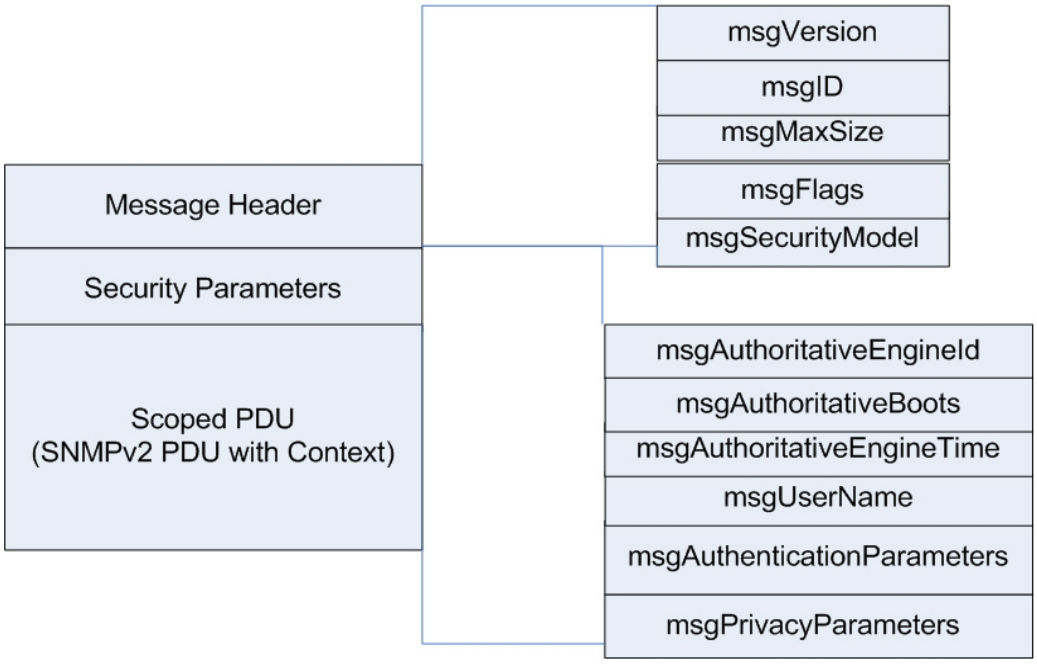


Table 3-3 lists the supported SNMPv3 fields.

Table 3-3
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 *msgID* in a response must be the same as the *msgID* received in the request. Different msgIDs are used in all request messages that are sent out during a 150-second time window. Any SNMPv3 response messages are discarded if they do not correspond to any current outstanding Request messages.
msgMaxSize	Indicates the maximum message size that the sender can support.

Copyright© 2022 Ciena® Corporation

Table 3-3
SNMPv3 packets (continued)

Packet Name	Description
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 *msgSecurityModel*.
scopedPDU	Contains the normal PDU and information for identifying the administratively unique context for processing the PDU. Any SNMPv3 responses are discarded if there is no outstanding Confirmed Class PDU. Different request-IDs are used in all Request PDUs that are sent out during a time window.

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*). The network device can be configured for read-only SNMP access when using SNMPv1, v2c or basic v3 (no authentication or privacy). Write access may be used if authentication is configured using SNMPv3.

> ***Note:*** If a valid security license key is not installed, SNMP will not respond to SNMPv3 requests with an authentication only security or privacy security level setting and will drop packets.

Once a valid security license key is installed, SNMP enables encryption and authentication. It then accepts SNMPv3 packets and allows the user to access the device.

SNMPv3 uses the following privacy encryption protocols, as described in RFC 3826:

- 3DES Symmetric Encryption Protocol
- AES encryption

The entire SNMPv3 message is checked for integrity and uses the HMAC-SHA1-96 with 160-bit key length by default. The security level for SNMPv3 in the DoD VoIP environment is authentication with privacy -

Copyright© 2022 Ciena® Corporation

snmpSecurityLevel=authPriv. The product is set to snmpSecurityLevel=authPriv, as the default security level used during initial configuration.

Data Encryption Standard-Cipher Block Chaining (DES-CBC) (usmDESPrivProtocol) is supported with a 16-octet (128 bit) input key (outlined in RFC 3414), and an encryption cipher for SNMPv3. CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 is supported, as described in RFC 3826 and specify this as the default encryption ciper for SNMPv3.

The security model for SNMPv3 is snmpSecurityModel=3.

> ***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 "snmpSecurityLevel" on page 3-11.

Supported concepts

Table 3-4 lists the supported SNMPv3 concepts.

Table 3-4
SNMPv3 concepts

Concept	Description
snmpEngineID	A unique identifier for an SNMP engine within an administrative domain. The *snmpEngineID* is computed using the chassis MAC address and an administratively assigned string. An administrator can manually configure snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but it must be modifiable.
snmpEngineBoots	Counts the number of times an SNMP engine has rebooted or reinitialized since the *snmpEngineID* was last set. This counter is initially set to zero.
snmpEngineTime	Specifies the number of seconds since the *snmpEngineBoots* counter was last incremented. This counter is initially set to zero. If the *snmpEngineTime* reaches its maximum (2147483647), the *snmpEngineBoots* is incremented by one and the *snmpEngineTime* starts counting again from zero. Time synchronization is done using authenticated messages.

Copyright© 2022 Ciena® Corporation

Table 3-4
SNMPv3 concepts (continued)

Concept	Description
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 *snmpEngineID* of the agent, and then determines the *snmpEngineBoots* and *snmpEngineTime*.

Table entries

Table 3-5 lists the supported default SNMPv3 table entries.

Table 3-5
Default SNMP user table entries

User name	AuthProtocol	PrivProtocol
Public	noAuth	noPriv
Private	noAuth	noPriv

Table 3-6 lists the supported default SNMP security map table entries.

Table 3-6
Default SNMP security map table entries

User name	SecModel	GroupName
Public	v1	Public
Private	v1	Private
Public	v2c	Public
Private	v2c	Private

Copyright© 2022 Ciena® Corporation

Table 3-7 lists default SNMP VACM access table entries.

Table 3-7
Default SNMP VACM access table entries

Group name	SecModel	SecLevel	ReadView	WriteView	NotifyView
Public	v1	noAuth	V12cView	None	V12cView
Public	v2c	noAuth	V12cView	None	V12cView
Private	v1	noAuth	V12cView	V12cView	V12cView
Private	v2c	noAuth	V12cView	V12cView	V12cView

Table 3-8 lists default SNMP VACM view tree table entries.

Table 3-8
Default SNMP VACM view tree table entries

View TreeName	Subtree	Type
V12cView	iso	include
V12cView	snmpResearch	exclude

Copyright© 2022 Ciena® Corporation

Table 3-9 lists the supported SNMPv3 table entries.

Table 3-9
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. *usmUserTable* includes the following information: • usmUserEngineID • usmUserName • usmUserAuthProtocol • usmUserPrivProtocol
vacmSecurityToGroupTable	Attaches a security model to a group that is defined in *usmUserTable*. This table does not, however, validate whether a user ID specified in the table exists in *usmUserTable*. *vacmSecurityToGroupTable* includes the following information: • vacmSecurityModel • vacmSecurityName • vacmGroupName
vacmAccessTable	Specifies either a read view, write view, or notify view access policy for the group specified in *vacmSecurityToGroupTable*. *vacmAccessTable* includes the following information: • vacmGroupName • vacmAccessSecurityModel • vacmAccessSecurityLevel • vacmAccessReadViewName • vacmAccessWriteViewName • vacmAccessNotifyViewName *vacmAccessSecurityLevel* contains three security levels that rank from highest to lowest, respectively: • authPriv • authNoPriv • noAuthNoPriv
vacmViewTreeFamilyTable	Specifies the following three views that are used in *vacmAccessTable*: • vacmViewTreeFamilyViewName • vacmViewTreeFamilySubtree • vacmViewTreeFamilyType

Copyright© 2022 Ciena® Corporation

Table 3-9
SNMPv3 table entries (continued)

Table Name	Description
snmpTargetAddrTable	Specifies the transport addresses that can either be used when generating SNMP traps or allow SNMP requests that come from specified IP addresses. *snmpTargetAddrTable* includes the following information: • snmpTargetAddrName • snmpTargetAddrTAddress • snmpTargetAddrTagList • snmpTargetAddrParams
snmpTargetParamTable	Specifies additional information about the *snmpTargetAddrTable*. This additional information includes what security model, security level, and trap type is to be used when generating SNMP traps. *snmpTargetParamTable* includes the following information: • snmpTargetParamsName • snmpTargetParamsSecurityModel • snmpTargetParamsSecurityName • snmpTargetParamsSecurityLevel
snmpCommunityTable	Used to map earlier SNMPv1 and SNMPv2c communities, notifications, and configurations into the SNMPv3 framework. *snmpCommunityTable* includes the following information: • snmpCommunityIndex • snmpCommunityName • snmpCommunitySecurityName • snmpCommunityTransportTag

Table 3-10 lists the maximum number of SNMPv3 table entries that are supported for each table.

Table 3-10
SNMPv3 maximum number of table entries

Table name	Maximum Entries Supported
usmUserTable	10
vacmSecurityToGroupTable	15
vacmAccessTable	15
vacmViewTreeFamilyTable	20
snmpTargetAddrTable	17

Copyright© 2022 Ciena® Corporation

Table 3-10
SNMPv3 maximum number of table entries (continued)

Table name	Maximum Entries Supported
snmpTargetParamTable	15
snmpCommunityTable	18
snmpNotifyTable	17

Alarm inputs

The 5142 and 5160 platforms support external alarm inputs for monitoring the status of various external sources. When an external alarm is triggered, an informational event is logged, and the wwpLeosChassisExternalAlarmStatusChangeNotification SNMP trap is sent. The trap specifies which alarm input was triggered, and whether the alarm was raised or cleared.

For overview information, including alarm pinouts, refer to *39XX/51XX Service Delivery, Aggregation, and Virtualization Switches Product Fundamentals*.

For more information, refer to the Installation and Startup Manual for the platform:

- *5142 Installation and Startup Manual*
- *5160 Installation and Startup Manual*

SNMP inform notification

SNMP provides a reliable trap mechanism to store traps with sequence numbers to enable ESM to track received SNMP traps. This mechanism sends SNMP notifications in the form of an SNMPv2c Inform Request message in sequence (Inform Request-PDU). When the SNMP manager, such as ESM, receives an Inform Request, it acknowledges by sending the Inform Response message to the SNMP agent on the device. If the agent does not receive the Inform Response in the configured timeout period (snmpTargetAddrTimeout), it re-sends the Inform Request message until it receives an Inform Response message. It does not send the next Inform Request until it receives an acknowledgment.

Any Inform Request message generated at the agent is first enqueued in this buffer. The agent periodically reads this queue and sends the Inform Request starting from the oldest to the most recent to ensure sequential delivery. After the Inform Response is received, the associated Inform Request is dequeued.

Notes

1 The agent is not blocked by the Inform Request message. If two notifications are generated back-to-back within the retry-timeout period, the agent does not wait for the receipt of the Inform Response for the

Copyright© 2022 Ciena® Corporation

previous request before sending the next Inform Request message. This could lead to out-of-sequence Inform Request messages if for some reason, the agent does not receive the Inform Response message to the first Inform Request message in the retry-timeout period.

2 The SNMPv2c Inform message is a “best effort” delivery mechanism.

3 If multiple notifications are generated back-to-back within a second and added to the SNMP inform queue, then after retry-timeout it is quite possible that the agent sends the retry Inform Request for the SNMP inform whose sequence number is higher and added last to the queue within a second interval. This could lead to out-of-sequence Inform Request messages.

For example, suppose that SNMP inform notifications are added to the queue within one-second intervals in order of sequence numbers (request-ids) 1,2,3,4,5,6,7,8. Then, after retry-timeout, it is quite possible that retry requests are sent in order of sequence numbers 8,7,6,5,4,3,2,1, because SNMP inform notifications are expired at same time.

Inform queue per trap server

The “Inform queue per trap server” feature is an enhancement to the standard inform functionality that aims to overcome the limitations faced while using standard informs.

Using standard inform functionality, the agent adds the Inform Request message to the SNMP inform queue after sending it to the SNMP manager. If the agent receives the Inform Response message, then the request message is removed from the SNMP inform queue. If the agent does not receive a response within a configurable timeout, the agent resends the request. After a configurable “retry” count, the agent eventually gives up and the Inform Request message is removed from the SNMP inform queue.

In the current SAOS implementation, there is one SNMP inform queue to store the Inform Request messages sent to configured multiple SNMP targets. A couple of limitations for using a single SNMP inform queue for all configured SNMP targets are:

1 Processing performance is impacted because the queue must be searched linearly. Whenever the agent receives the Inform Response message, the queue must be searched linearly to match the sequence ID from the response message with the sequence ID for sent Inform Request messages. Even when the agent does not receive a response message after a configurable timeout, the queue must be searched linearly to remove the Inform Request message. The linear search approach consumes processing time, especially when the queue size is large.

2 A request-id field in the SNMP packet must be filled when SNMPv2c or SNMPv3 traps and Inform Request messages are sent to SNMP managers. In the current SAOS implementation, there is a single available range (1 to 2147483648) to allocate the request-id for both traps and Inform Request messages. When multiple targets are configured, then the

Copyright© 2022 Ciena® Corporation

request-id field in traps and informs sent to the targets are not in sequence. As a result, the SNMP manager doesn't have any mechanism to know how many traps are missed.

The "Inform queue per trap server" feature addresses the limitations of standard informs by implementing the following:

Multiple queue design approach

The current single SNMP inform queue (horizontal approach) for all configured SNMP targets is changed to multiple queue design (horizontal and vertical) approach:

- A single queue handles multiple SNMP managers, that is, manager queue.
- Another single queue corresponds to every SNMP manager to handle Inform Request messages, that is, inform queue per manager.

Single timer object per configured SNMP managers

The current single timer object to handle timeouts scenarios for Inform Request messages of all configured SNMP targets is changed to a single timer object per manager. The timer object corresponds to each manager and is responsible to handle timeouts for only the respective managers and removes the Inform Request message from the corresponding manager inform queue.

Same range is allocated to all configured SNMP managers

Currently, the NE allows a maximum of 17 SNMP targets to configure for either traps or informs. The initial single available range (1 to 2147483648, according to the SNMP RFCs) is now allocated to every configured target. Initially, it was shared among the configured targets. Now when multiple targets are configured, the request-id field in traps and informs sent to the targets is in sequence. Consequently, the SNMP manager has a mechanism to know how many traps or informs are missed.

Sharing maximum inform queue length equally

In the current SAOS implementation, there is CLI available to configure SNMP inform queue length. The same configured inform queue length is also applicable globally when this feature is enabled. It is *not* applicable to inform queue per manager. The configured maximum value is divided equally among the configured SNMP targets instead.

Inform queue notes

1 The "Inform queue per trap server" feature is enabled by default as soon as a device is upgraded to SAOS 6.18.1 or later. There is no CLI available to disable this feature.

2 When the configured SNMP inform queue length is not divided equally among the number of configured SNMP targets, then the SNMP inform queue length count is divided equally among the number of configured

Copyright© 2022 Ciena® Corporation

targets and remaining nodes are ignored. This table captures possible combinations for SNMP inform queue length, targets configurations, and accordingly, allocated SNMP inform queue length per target:

Table 3-11
SNMP inform queue length possibilities

Sequence number	SNMP inform queue length	Number of configured targets	SNMP inform queue length per target
1	100	3	33
2	150	7	21
3	1716	17	100

Advantages over standard Inform functionality

The “Inform queue per trap server” feature is designed to overcome the limitations for standard informs:

- The multiple queue design approach makes searching faster as only a particular manager inform queue must be searched for handling either Inform Response message or timeouts. Consequently, it helps to achieve better performance when compared with the standard single queue design approach.
- The timer object per manager allows searching only a particular manager inform queue to handle timeouts. Consequently, it helps to achieve better performance and it becomes more visible when the inform queue size is large.
- Allocating the single available range (1 to 2147483648) of request-ids to every configured SNMP manager provides a mechanism to send traps/informs sequentially. It allows every SNMP manager to know how many traps or informs are dropped in case of a communication break. Consequently, SNMP managers can develop a mechanism at their end to handle dropped situations accordingly.

The configured maximum inform queue length is shared equally among the manager inform queues. In cases when any target is unreachable, then the inform queue for that target grows only up to the allocated inform queue length. This does not impact the inform queue for other SNMP managers. This functionality was missing from the standard global SNMP inform queue, where the entire queue was exhausted to store Inform Request messages for unreachable targets, restricting the NE to send informs to reachable targets.

This chapter provides the following procedures for SNMP:

- “Disabling the SNMP agent” on page 3-21
- “Enabling or disabling an SNMP notification” on page 3-22
- “Displaying SNMP notifications” on page 3-23

Copyright© 2022 Ciena® Corporation

- "Configuring a device to send SNMPv1 traps" on page 3-24
- "Configuring a device to send SNMPv2c traps" on page 3-27
- "Configuring a device to send SNMPv3 traps" on page 3-30
- "Configuring global SNMP settings" on page 3-34
- "Creating SNMPv3 users" on page 3-36
- "Configuring SNMP notification entries" on page 3-38
- "Configuring SNMP source address checking" on page 3-39
- "Configuring SNMP reliable traps" on page 3-42
- "Setting or unsetting the maximum SNMP inform queue length" on page 3-50
- "Showing or clearing SNMP inform statistics counters" on page 3-51
- "Troubleshooting SNMP and RMON configuration" on page 3-63

RMON

RMON supports network monitoring features described in RFC 2819. With remote monitoring (RMON), you can enable a device to gather information related to groups defined in RFC 1757 and RFC 2021. Using a network monitoring device, you can probe the network to retrieve this information by sampling SNMP MIB objects.

Table 3-12 lists RMON RFC support.

Table 3-12
RMON support

Group	Description
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.

Copyright© 2022 Ciena® Corporation

Table 3-12
RMON support

Group	Description
Statistics	Ethernet statistics are retrieved and measured by the probes for each of the configured Ethernet ports on the device.
RFC 2021	
User History	Periodic samples of user specified history.

This chapter provides the following procedures for RMON:

- “Configuring alarms” on page 3-53
- “Configuring events” on page 3-58
- “Configuring statistics” on page 3-61
- “Troubleshooting SNMP and RMON configuration” on page 3-63
- “Displaying RMON information” on page 3-64

Copyright© 2022 Ciena® Corporation

Procedure 3-1
Disabling the SNMP agent

When the SNMP agent is disabled, attempts to connect to the SNMP agent time out. By default, the status is enabled.

SNMP packets are dropped by the agent if the SNMP agent is globally disabled.

Step	Action
1	Disable the SNMP agent: `snmp disable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 3-2
Enabling or disabling an SNMP notification

You can enable or disable a specific notification. When the notification is enabled, notifications are generated.

For every notification trap, the default state is enabled.

Notifications are grouped by:

- class (Ciena, standard and WWP)
- MIB name
- notification name

Step	Action
1	Enable or disable an SNMP notification: `snmp notification [ciena|standard|wwp]{<mib-name-object> [enable|disable] <notification-name-object>}`

—end—

Example

The following example enables the notification cienaCesConfigMgmtConfigChangeNotification on CIENA-CES-CONFIG-MGMT-MIB.

```
snmp notification ciena CIENA-CES-CONFIGG-MGMT-MIB enable
notification-name cienaCesConfigMgmtConfigChangeNotification
```


Copyright© 2022 Ciena® Corporation

Procedure 3-3
Displaying SNMP notifications

The following attributes of SNMP notifications can be displayed:

- state (enabled or disabled) of the specific notification
- MIB (the MIB the notification belongs to)
- class (Ciena or WWP)
- notification name

Step	Action
1	Display the SNMP notification: `snmp notification show`

—end—

Example

The following shows the output for the snmp notification show command.

```
snmp notification show
```

```
+------------------------------- SNMP NOTIFICATION CONFIGURATION ----------------------+----------+
| Class    | MIB                       | Notification                                  | State    |
+----------+---------------------------+-----------------------------------------------+----------+
| Ciena    | CIENA-CES-CONFIG-MGMT-MIB | cienaCesConfigMgmtConfigSavedNotification     | Enabled  |
| Ciena    | CIENA-CES-CONFIG-MGMT-MIB | cienaCesConfigMgmtConfigChangeNotification    | Enabled  |
| Standard | ALARM-MIB                 | alarmActiveState                              | Disabled |
| Standard | ALARM-MIB                 | alarmClearState                               | Disabled |
+----------+---------------------------+-----------------------------------------------+----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-4
Configuring a device to send SNMPv1 traps

Configure a device to send SNMPv1 traps when you want to enable the device to send SNMP version 1 (v1) message format traps, including generic traps such as:

- linkUp
- linkDown
- coldStart
- warmStart
- authenticationFailure

SNMPv1 traps are defined in the MIB files using the "TRAP-TYPE" macro.

You can also configure the network element to send all three versions of the trap at the same time by performing the procedure for all three SNMP versions.

When using SNMPv1 with IPv6, note the following:

- The SNMPv1 trap packet itself has the source agent IP which is 32 bytes. The SNMPv1 trap packet can accommodate the IpAddress type parameter only, which is IPv4. If an IPv6 agent sends the SNMPv1 trap packet, then this address is all 0s or the loopback address of the agent. The source IP is only in the SNMP v1 trap.
- The main source IP, that is, from the IP layer, should have the IPv6 address.

Step	Action
1	Create an entry in the snmpTargetAddrTable. `snmp create target <String[1..32]> {addr <IpAddressWithMask>} {param-name <String[1..32]>} [tag <String[32]>] [udp-port <NUMBER: 0-65535>] [transport-domain <snmp-udp|v4-udp|v6-udp>] [retrycount <NUMBER: 0-255>] [retry-timeout <NUMBER: Measured in 0.01 seconds units>]`

Copyright© 2022 Ciena® Corporation

where

target <String[32]>	is a text string of up to 32 characters that represents the name of the target (trap server).
addr <IpAddressWithMask>	is the destination IP address or hostname with mask expressed in CIDR notation.
param-name <String[32]>	is a text string of up to 32 characters that selects a set of entries in the snmpTargetParam table.
tag <String[32]>	is a text string of up to 32 character s that corresponds to the value of the “notify-tag” defined in the SNMP notify table. If this tag does not match any entry in the SNMP notify table, notifications are not sent.
udp-port <NUMBER: 0-65535>	is the UDP trap port.
transport-domain <snmp-udp| v4-udp| v6-udp>	is the transport domain.
retry-count <NUMBER: 0-255>	is the number of times to re-send messages when configured for reliable traps.
retry-timeout <NUMBER: Measured in 0.01 seconds units>	is the amount of time to wait to re-send messages if no response is received when configured for reliable traps.

2 Create a target parameter entry and security name:

```
snmp create target-param <String[32]> {sec-name
<String[32]>}
```

where

target-param <String[32]>	is a text string of up to 32 characters that represents the name of the target parameter (trap).
sec-name <String[32]>	is the security name (access entry).

To validate the configuration

3 Display the target configuration:

```
snmp show target
```

4 Display the target parameter configuration:

```
snmp show targetparams
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example configures a device to send SNMPv1 traps. The address of the SNMP manager is 10.32.41.117.

```
snmp create target v1 param-name v1 addr 10.32.41.117
snmp create target-param v1 sec-name public sec-model v1
```

The following example displays sample output for the snmp show target command.

```
snmp show target
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|TargetName    |IPAddress/Host  |ParamName  |Tags         | Udp Port|Transport| Retry | Retry |
|              |                |           |             |         | Domain  | Count |Timeout|
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|anywhere      |0.0.0.0/0       |none       |anywhereTag  |0        |snmp-udp |0      |0      |
|anywhereIpv6  |::/0            |none       |anywhereTag  |0        |v6-udp   |0      |0      |
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
```

The following example displays sample output for the snmp show targetparams command.

```
snmp show targetparams
+-------------------------------+-------------------------------+-----+------------+-----+
| TargetParamName               | SecurityName                  |Sec  |Sec Level   |MP   |
|                               |                               |Model|            |Model|
+-------------------------------+-------------------------------+-----+------------+-----+
|v1                             |public                         |v1   |noAuth      |0    |
|v2c                            |public                         |v2c  |noAuth      |1    |
|v3                             |public                         |v3   |noAuth      |3    |
+-------------------------------+-------------------------------+-----+------------+-----+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-5
Configuring a device to send SNMPv2c traps

Configure a device to send SNMPv2c traps when you want to enable the device to send SNMP version 2 (v2) message format traps. SNMPv2 traps are defined in the MIB files using the "NOTIFICATION-TYPE" macro.

You can also configure the network element to send all three versions of the trap at the same time by performing the procedure for all three SNMP versions.

Step	Action

1 Create an entry in the snmpTargetAddrTable.

```
snmp create target <String[32]> {addr
<IpAddressWithMask>}{param-name <String[32]>} [tag
<String[32]>] [udp-port <NUMBER: 0-65535>] [transport-
domain <snmp-udp|v4-udp|v6-udp>] [retrycount <NUMBER: 0-
255>] [retry-timeout <NUMBER: Measured in 0.01 second
units>]
```

where

target <String[32]>	is a text string of up to 32 characters that represents the name of the target (trap server).
addr <IpAddressWithMask>	is the destination IP address or hostname with mask expressed in CIDR notation.
param-name <String[32]>	is a text string of up to 32 characters that selects a set of entries in the snmpTargetParam table.
tag <String[32]>	is a text string of up to 32 character s that corresponds to the value of the “notify-tag” defined in the SNMP notify table. If this tag does not match any entry in the SNMP notify table, notifications are not sent.
udp-port <NUMBER: 0-65535>	is the UDP trap port

Copyright© 2022 Ciena® Corporation

where

transport-domain <snmp-udp| v4-udp| v6-udp>	is the transport domain.
retry-count <NUMBER: 0-255>	is the number of times to re-send messages when configured for reliable traps.
retry-timeout <NUMBER: Measured in 0.01 seconds units>	is the amount of time to wait to re-send messages if no response is received when configured for reliable traps.

2 Create a target parameter entry and security name:

```
snmp create target-param <String[32]> {sec-name
<String[32]>}
```

where

target-param <String[32]>	is a text string of up to 32 characters that represents the name of the target parameter (trap).
sec-name <String[32]>	is the security name (access entry).

To validate the configuration

3 Display the target configuration:

```
snmp show target
```

4 Display the target parameter configuration:

```
snmp show targetparams
```

—end—

Example

The following example configures a device to send SNMPv2 traps. The address of the SNMP manager is 10.32.41.117.

```
snmp create target informTarget param-name informParamv2c addr
10.32.41.117
snmp create target-param informParamv2c sec-name public sec-
model v2c
```


Copyright© 2022 Ciena® Corporation

The following example displays sample output for the snmp show target command.

```
snmp show target
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|TargetName    |IPAddress/Host  |ParamName  |Tags         | Udp Port|Transport| Retry | Retry |
|              |                |           |             |         | Domain  | Count |Timeout|
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|anywhere      |0.0.0.0/0       |none       |anywhereTag  |0        |snmp-udp |0      |0      |
|anywhereIpv6  |::/0            |none       |anywhereTag  |0        |v6-udp   |0      |0      |
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
```

The following example displays sample output for the snmp show targetparams command.

```
snmp show targetparams
+------------------------------+--------------------------------+-----+------+-----+
| TargetParamName              |SecurityName                    |Sec  |Sec   |MP   |
|                              |                                |Model|Level |Model|
+------------------------------+--------------------------------+-----+------+-----+
|v1                            |public                          |v1   |noAu  |0    |
|informParamv2c                |public                          |v2c  |noAu  |1    |
|v3                            |public                          |v3   |noAu  |3    |
+------------------------------+--------------------------------+-----+------+-----+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-6
Configuring a device to send SNMPv3 traps

Configure a device to send SNMPv3 traps when you want to enable the device to send SNMP version (v3) message format traps.

You can also configure the network element to send all three versions of the trap at the same time by performing the procedure for all three SNMP versions.

Step	Action

1 Create an entry in the snmpTargetAddrTable.

```
snmp create target <String[32]> {addr
<IpAddressWithMask>} {param-name <String[32]>} [tag
<String[32]>] [udp-port <NUMBER: 0-65535>] [transport-
domain <snmp-udp|v4-udp|v6-udp>] [retrycount <NUMBER: 0-
255>] [retry-timeout <NUMBER: Measured in 0.01 seconds
units>]
```

where

target <String[32]>	is a text string of up to 32 characters that represents the name of the target (trap server).
addr <IpAddressWithMask>	is the destination IP address or hostname with mask expressed in CIDR notation.
param-name <String[32]>	is a text string of up to 32 characters that selects a set of entries in the snmpTargetParam table.
tag <String[32]>	is a text string of up to 32 character s that corresponds to the value of the “notify-tag” defined in the SNMP notify table. If this tag does not match any entry in the SNMP notify table, notifications are not sent.
udp-port <NUMBER: 0-65535>	is the UDP trap port

Copyright© 2022 Ciena® Corporation

where

transport-domain <snmp-udp| v4-udp| v6-udp>	is the transport domain.
retry-count <NUMBER: 0-255>	is the number of times to re-send messages when configured for reliable traps.
retry-timeout <NUMBER: Measured in 0.01 seconds units>	is the amount of time to wait to re-send messages if no response is received when configured for reliable traps.

2 Create a target parameter entry and security name:

```
snmp create target-param <String[32]> {sec-name
<String[32]>}
```

where

target-param <String[32]>	is a text string of up to 32 characters that represents the name of the target parameter (trap).
sec-name <String[32]>	is the security name (access entry).

3 Create an access policy for the specified group name:

```
snmp create access-entry <String[32]> sec-model v3 {sec-
level {sec-level <noAuth|authNoPriv|authWithPriv>}
[read-view <String[64]>] [notify-view <String[64]>]
```

where

<String[32]>	is the group name.
sec-model v3	is the security model for access entry.
sec-level {sec-level <noAuth| authNoPriv| authWithPriv>	is the security level.
read-view <String[64]>	is the read view name. Left unspecified, the default value is '1.3.6.1' which is every object under internet sub tree.
notify-view <String[64]>	is the notify view name. The default value is 'null OID': nothing is included for notify access.

Copyright© 2022 Ciena® Corporation

4 Attach a user to the group:

```
snmp security-to-group attach user <String> sec-model v3
{group <String[32]>}
```

where

user <String>	is the user name.
group <String[32]>	is the group name specified in step 3.

To validate the configuration

5 Display the target configuration:

```
snmp show target
```

6 Display the target parameter configuration:

```
snmp show targetparams
```

7 Display users:

```
snmp show user
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example configures a device to send SNMPv3 traps. The address of the SNMP manager is 10.32.41.117. The group name is public and the user name is public.

```
snmp create target InformTarget1 param-name InformParamv3 addr
10.32.41.117
snmp create target-param InformParamv3 sec-name public sec-
model v3
snmp create access-entry public sec-model v3 sec-level noAuth
read-view V12cView notify-view V12cView
snmp security-to-group attach user public sec-model v3 group
public
```

The following example displays sample output for the snmp show target command.

```
snmp show target
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|TargetName    |IPAddress/Host  |ParamName  |Tags         | Udp Port|Transport| Retry | Retry |
|              |                |           |             |         | Domain  | Count |Timeout|
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
|anywhere      |0.0.0.0/0       |none       |anywhereTag  |0        |snmp-udp |0      |0      |
|anywhereIpv6  |::/0            |none       |anywhereTag  |0        |v6-udp   |0      |0      |
+--------------+----------------+-----------+-------------+---------+---------+-------+-------+
```

The following example displays sample output for the snmp show targetparams command.

```
snmp show targetparams
+------------------------------+--------------------------------+-----+------+-----+
| TargetParamName              |SecurityName                    |Sec  |Sec   |MP   |
|                              |                                |Model|Level |Model|
+------------------------------+--------------------------------+-----+------+-----+
|v1                            |public                          |v1   |noAu  |0    |
|v2                            |public                          |v2c  |noAu  |1    |
|informParamv3                 |public                          |v3   |noAu  |3    |
+------------------------------+--------------------------------+-----+------+-----+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-7
Configuring global SNMP settings

You can configure the following for SNMP:

- contact
- location
- standard link up and down traps
- proprietary link up and down traps
- aggregation port link up and down traps
- CFM fault traps

Note: Special characters are limited on the SNMPv2c string entries. Use other characters or use SNMPv3 if security is an issue.

Step	Action

1 Set SNMP contact, location, trap attributes and CFM fault traps:

```
snmp set {[contact <String[255]>], [location
<String[255]>], [std-link-up-down-trap
<disable|enable>], [enhancement-link-up-down-trap
<disable|enable>], [agg-port-link-up-down-trap
<disable|enable>], [cfm-fault-trap <disable|enable>]}
```

where

contact <String[255]>	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, Ciena”.
location <String[255]>	is 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”.
std-link-up-down-trap <disable|enable>	When enabled, standard link up and down traps are sent by the device. By default, standard link up and link down traps are enabled.
enhancement-link-up-down-trap <disable|enable>	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
agg-port-link-up-down-trap <disable|enable>	When enabled, aggregation port link up and down traps are sent by the device. By default, aggregation port link up and link down traps are disabled.
cfm-fault-trap <disable|enable>	When enabled, CFM faults are sent by the device. By default, the CFM fault traps are enabled.

Copyright© 2022 Ciena® Corporation

To validate the configuration

2 Display the configuration:

```
snmp notification show
```

—end—

Example

The following example sets the contact to “Customer Support, Ciena”, the location to “Spokane Valley, USA”, disables the enhanced link up and link down trap, and enables the standard link up and link down trap.

```
snmp set contact "Customer Support, Ciena" enhancement-link-up-down-trap disable location "Spokane Valley, USA" std-link-up-down-trap enable
```

The following example displays sample output for the snmp notification show command.

```
snmp notification show

+------------------------------------ SNMP NOTIFICATION CONFIGURATION-------------------------+---------+
| Class | MIB                          | Notification                                           | State   |
+-------+------------------------------+--------------------------------------------------------+---------+
| Ciena | CIENA-CES-CONFIG-MGMT-MIB    | cienaCesConfigMgmtconfigSavedNotification              | Enabled |
| Ciena | CIENA-CES-CONFIG-MGMT-MIB    | cienaCesConfigMgmtConfigChangeNotification             | Disabled|
| Ciena | CIENA-CES-TIME-SYNC-MIB      | cienaCesSyncinputPUStateChangeNotification             | Enabled |
| Ciena | CIENA-CES-TIME-SYNC-MIB      | cienaCesSyncinputProtectionGroupstateChangeNotification| Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetMgmtAddrChangeNotification                 | Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetMgmtAddrAddedNotification                  | Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetMgmtAddrRemovedNotification                | Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetGatewayAddrChangeNotification              | Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetGatewayAddedNotification                   | Enabled |
| Ciena | CIENA-CES-MGMT-INTERFACE-MIB | cienaCesInetGatewayRemovedNotification                 | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesMplsTunnelOperStateChgTrap                     | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesMplsEncapTunnelGrpActiveEncapTunnelchange      | Enabled |
| Ciena | CIENA-CES -MPLS-MIB          | cienaCesMplsTransitTunnelOperStateChgTrap              | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesMplsAssociatedTunnelOperStateChgTrap           | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesGmplsEncapUnidirTunnelOperstatechgTrap         | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesGmplsEncapCoroutedTunnelOperStateChgTrap       | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesGmplsDecapcoroutedTunnelOperstatechgTrap       | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesGmplsTransitunidirTunneloperStateChgTrap       | Enabled |
| Ciena | CIENA-CES-MPLS-MIB           | cienaCesGmplsTransitcoroutedTunneloperstateChgTrap     | Enabled |
--More--
```


Copyright© 2022 Ciena® Corporation

Procedure 3-8
Creating SNMPv3 users

Create at least one SNMPv3 user In order for an SNMP engine to send and receive SNMPv3 messages. This procedure describes how to configure User-based Security Model (USM) for SNMPv3.

Step	Action

To create a user

1 Create a user:

```
snmp create username <String[1..32]> {auth-protocol
<noauth|md5|sha>} [echoless-auth-password] [priv-
protocol <aes-128|des|3des|nopriv>] [echoless-priv-
password] [priv-secret <String[40]>] {engine-id <SNMP
EngineID:XX:XX..(5-32 octets)Default:LocalSnmpEngineId>}
```

where

username <String[32]>	is a text string of up to 32 characters that specifies the security identifier.
auth-protocol <noauth|md5|sha>	enables messages sent to or from the user to be authenticated using MD5 or SHA or not at all (noauth).
echoless-auth-password	collects authentication password interactively.
priv-protocol <aes-128|des|3des|nopriv|des>	enables messages sent to or from the user to be protected from disclosure using DES or not at all (nopriv).
echoless-priv-password	collects authentication password interactively.
priv-secret <String[40]>	is a 40-character converted privacy password
engine-id <SNMP EngineID:XX:XX..(5-32 octets)Default:LocalSnmpEngineId>}>	is, by default, the local SNMP engine. To enable SNMPv3 informs, set the engine-id to the engine identifier of the receiving entity.

To delete a user

2 Delete a user:

```
snmp delete user <String[32]>
```

where

user <String[32]>	is a text string of up to 32 characters that specifies the security identifier.

Copyright© 2022 Ciena® Corporation

To validate the user configuration

3 Display users:

```
snmp show user
```

—end—

Example

The following example creates a user with a user identifier of user1, an authentication protocol of md5, des privacy protocol, and an authentication password of mypassword.

```
snmp create user user1 echoless-auth-password echoless-priv-
password auth-protocol md5 priv-protocol des priv-secret
myPassword
```

The following example deletes a user with a user identifier of user1.

```
snmp delete user user1
```

The following example displays sample output for the snmp show user command.

```
snmp show user
+--------------+------------+------------+----------------------------------------+
| UserName     | AuthProt   | PrivProt   |Engine ID                               |
+--------------+------------+------------+----------------------------------------+
| public       | noAuth     | noPriv     |80:00:04:f7:05:00:03:18:6d:a9:60:00     |
| private      | noAuth     | noPriv     |80:00:04:f7:05:00:03:18:6d:a9:60:00     |
+--------------+------------+------------+----------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-9
Configuring SNMP notification entries

You can modify and delete 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.

Step	Action

To modify a notification entry

1 Modify a notification entry:

```
snmp set notify <notify> {[notify-tag <String[32]>],
[notify-type <trap|inform>]}
```

where

notify <notify>	is the SNMP target entry.
notify-tag <String[32]>	is the notify view tag.
notify-type <trap|inform>	is the notification type. A value of 1 means trap; a value of 2 means inform.

To delete a notification entry

2 Delete a notification entry:

```
snmp delete notify <String[32]>
```

where

notify <notify>	is the SNMP target entry.

—end—

Example

The following example modifies a notification entry.

```
snmp set notify myNotifyName notify-tag myNotifyTag notify-type
inform
```

The following example deletes a notification entry.

```
snmp delete notify myNotification
```


Copyright© 2022 Ciena® Corporation

Procedure 3-10
Configuring SNMP source address checking

Configure source address checking to reject incoming SNMPv1 and SNMPv2c messages unless they meet the following criteria:

- Community string matches a configured entry in the community map table.
- Transport tag has a corresponding entry in the target table.
- Subnet-mask indicates bit 0 or 1 and matches the corresponding bit in the “addr” value.

Note: Source address checking for SNMPv3 messages is not supported.

Source address checking can be configured to match:

- A specific source address. If the target IPv4 or IPv6 address in the SNMP target table is a valid IP address and the transport-tag in the SNMP community table matches the tag in the SNMP target table, then SNMP packets from only this specific IPv4 or IPv6 address are accepted.
- A specific source address in a subnet. If the target address in SNMP target table is a valid IPv4 or IPv6 address, the desired subnet mask is set to a valid subnet mask other than the default, and the transport-tag in the SNMP community table matches the tag in the SNMP target table, then only SNMP packets from IP addresses in the specified subnet are accepted.
- Any source address. If the target address in SNMP target table is 0.0.0.0 and subnet mask is 0.0.0.0 for IPv4 or ::0 for IPv6, and the transport-tag in SNMP community table matches tag in the SNMP target table, then SNMP packets from any IP are accepted.

Step	Action
1	Create an SNMP community mapping: `snmp create community-index <community-index> {community <String[64]>} {sec-name <String[32]>} [transport-tag <String[32]>]` where community-index <community-index> is the SNMP community to sec-name mapping.

Copyright© 2022 Ciena® Corporation

where

community <String[64]>	is the community name.
sec-name <String[32]>	is the security name.
transport-tag <String[32]>	is the transport tag.

2 Create an SNMP target entry:

```
snmp create target <target> {addr <IP address with mask>}
{param-name <String[32]>} [tag <String[32]>][udp-port
<NUMBER: 0-65535>] [transport-domain <snmp-udp | v4-udp |
v6-udp>] [retry-count <NUMBER: 0-255>] [retry-timeout
<NUMBER :Measured in 0.01 seconds>]
```

where

target <target>	is the SNMP target entry.
addr <IP address with mask>	is the target IP address.
param-name <String[32]>	is the param name.
tag <String[32]>	is the tag. Transport Tag must be set to TrapTag for V1 Trap. The default value is TrapTag.
udp-port <NUMBER: 0-65535>	is the UDP trap port.
transport-domain <snmp-udp | v4-udp | v6-udp>	is the transport domain.
retry-count <NUMBER: 0-255>	is the number of retries.
retry-timeout <NUMBER :Measured in 0.01 seconds>	is the retry timeout.

—end—

Copyright© 2022 Ciena® Corporation

Example

In this example, the incoming source address must match 192.147.142.35 (as set in the target table) or the incoming SNMP request will be rejected. The subnet-mask is 255.255.255.255 and all the bits have a value of “1.”

```
snmp create community-index target1 community comm1 sec-name
user1 transport-tag TrapTag
snmp create target TRAPS addr 192.147.142.35/32 param-name
TRAPS tag TrapTag
```

In this example, the incoming source address must match 192.147.142.35 and the subnet must match 255.255.128 (as set in the target table) or the incoming SNMP request will be rejected.

```
snmp create community-index target1 community comm1 sec-name
user1 transport-tag TrapTag
snmp create target TRAPS addr 192.147.142.35/25 param-name
TRAPS tag TrapTag
```

The following example shows source address checking configured to match any source address. The target address in the SNMP target table is 0.0.0.0, the subnet mask is 0.0.0.0, and the transport-tag in the SNMP community table matches the tag in the SNMP target table.

```
snmp create community-index target1 community comm1 sec-name
user1 transport-tag TrapTag
snmp create target TRAPS addr 0.0.0.0/0 param-name TRAPS tag
TrapTag
```

In this example, the incoming source address must match 2001:db8:1234:abcd:567:ef::

```
snmp create target TRAP0 addr 2001:db8:1234:abcd:567:ef::
param-name TRAP0
```


Copyright© 2022 Ciena® Corporation

Procedure 3-11
Configuring SNMP reliable traps

Configure reliable traps for SNMPv2c and SNMPv3 when you want a reliable trap mechanism to store traps with sequence numbers to enable ESM to track received SNMP traps.

Note: For the reliable traps feature to work, the SNMP manager needs to be configured to parse the Inform Request message and send Inform Response message back to the SNMP agent correctly.

Step	Action

To configure reliable traps for SNMPv2c

1 Create a notification entry:

```
snmp create notify <notify> {notify-tag <String[32]>}
[notify-type <trap|inform>]
```

where

notify <notify>	is the SNMP target entry.
notify-tag <String[32]>	is the notify view tag.
notify-type <trap|inform>	is the notification type. A value of 1 means trap; a value of 2 means inform.

2 Confirm the configuration of the notification entry:

```
snmp show notify
```

3 Configure a target-parameter with v2c security model to support v2c notification.

```
snmp create target-param <target-param> {sec-name
<String>} [sec-model v2c] [sec-level <noAuth | authNoPriv
| authWithPriv>]
```

where

target-param <target-param>	is the SNMP target parameter.
sec-name <String>	is the security name.
sec-model v2c	sets the security model for the target parameter to v2c.
[sec-level <noAuth | authNoPriv | authWithPriv>]	is the security level for target parameter.

Copyright© 2022 Ciena® Corporation

4 Create an inform receiver.

```
snmp create target <target> {addr <IP address with mask>}
{param-name <String[32]>} [tag <String[32]>] [udp-port
<NUMBER: 0..65535>] [transport-domain <snmp-udp | v4-udp
| v6-udp>] [retry-count <NUMBER: 0..255>] [retry-timeout
<NUMBER :Measured in 0.01 seconds units>]
```

where

target <target>	is the SNMP target entry.
addr <IP address with mask>	is the target IP address.
param-name <String[32]>	is the param name.
tag <String[32]>	is the tag. The Transport Tag must be set to TrapTag for V1 Trap. The default value is TrapTag.
udp-port <NUMBER: 0-65535>	is the UDP trap port.
transport-domain <snmp-udp | v4-udp | v6-udp>	is the transport domain.
retry-count <NUMBER: 0..255>	is the number of retries.
retry-timeout <NUMBER :Measured in 0.01 seconds units>	is the retry timeout.

5 Enable reliable traps.

```
snmp reliable-trap enable
```


Copyright© 2022 Ciena® Corporation

To configure reliable traps for SNMPv3

6 Create an SNMPv3 user.

```
snmp create username <String[1..32]> {auth-protocol
<noauth|md5|sha>} [echoless-auth-password] [priv-
protocol <aes-128|des|3des|nopriv>] [echoless-priv-
password] [priv-secret <String[40]>] {engine-id <SNMP
EngineID:XX:XX..(5-32 octetsDefault:LocalSnmpEngineId>}
```

where

user <user>	is the SNMP user name.
auth-protocol <noauth | md5 | sha>	is the authentication protocol.
echoless-auth-password	collects authentication password interactively.
priv-protocol <aes-128|des|3des|nopriv>	is the privacy protocol.
echoless-priv-password	collects authentication password interactively.
priv-secret <String[40]>	sets the password using a pre-encrypted string.
engine-id <SNMP EngineID:XX:XX..(5-32 octets)Default:LocalSnmpEngineId>	is the SNMP engine ID. The default value is LocalSnmpEngineId.

7 Create a second SNMPv3 user.

```
snmp create user <user> {auth-protocol <noauth | md5 |
sha>} [echoless-auth-password] [priv-protocol <aes-
128|des|3des|nopriv>] [echoless-priv-password] [priv-
secret <String[40]>] {engine-id <SNMP EngineID:XX:XX..(5-
32 octetsDefault:LocalSnmpEngineId>}
```

where

user <user>	is the SNMP user name.
auth-protocol <noauth | md5 | sha>	is the authentication protocol.
echoless-auth-password	collects authentication password interactively.

Copyright© 2022 Ciena® Corporation

where

priv-protocol <aes-128|des|3des|no priv>	is the privacy protocol.
echoless-priv-password	collects authentication password interactively.
priv-secret <String[40]>	sets the password using a pre-encrypted string.
engine-id<SNMP EngineID:XX:XX..(5-32 octets)Default:LocalSnmpEngineId>	is the SNMP engine ID. The default value is LocalSnmpEngineId.

8 Attach the first SNMPv3 user to an SNMPv3 access group.

```
snmp security-to-group attach user <user> sec-model v3
group <String[32]>
```

where

user <user>	is the SNMP user name.
sec-model v3	is the v3 security model for the user
group <String[32]>	is the SNMP group name.

9 Attach the second SNMPv3 user to an SNMPv3 access group.

```
snmp security-to-group attach user <user> sec-model v3
group <String[32]>
```

where

user <user>	is the SNMP user name.
sec-model v3	is the v3 security model for the user
group <String[32]>	is the SNMP group name.

Copyright© 2022 Ciena® Corporation

10 Create a view tree entry with a sub-tree that can be viewed. (Optionally, you can use the default viewtree, V12cView).

```
snmp create viewtree <viewtree> {sub-tree <String[64]>}
{type <include | exclude>}
```

where

viewtree <viewtree>	is the SNMP view tree name.
sub-tree <String[64]>	is the sub-tree MIB OID.
type <include | exclude>	is the tree type, which is one of include or exclude.

11 Create an access policy for the 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 <access-entry> sec-model v3
{sec-level <noAuth | authNoPriv | authWithPriv>} {read-
view <String[64]>} [write-view <String[64]>] [notify-view
<String[64]>]
```

where

access-entry <access-entry>	is the SNMP access entry.
sec-model v3	is the v3 security model for access entry.
sec-level <noAuth | authNoPriv | authWithPriv>	is the security level.
read-view <String[64]>	is the read view name.
write-view <String[64]>	is the write view name.
notify-view <String[64]>	is the write view name.

12 Create a notification tag with notify-type as inform.

```
snmp create notify <notify> {notify-tag <String[32]>}
notify-type <trap | inform>
```

where

notify <notify>	is the SNMP notify entry.
{notify-tag <String[32]>	is the notify view tag.
notify-type <trap | inform>	is the notification type. A value of 1 means trap; a value of 2 means inform.

Copyright© 2022 Ciena® Corporation

13 Create an target SNMP trap server entry.

```
snmp create target <target> {addr <IP address with mask>}
param-name <String[32]> tag <String[32]> [udp-port
<NUMBER: 0..65535>] [transport-domain <snmp-udp | v4-udp
| v6-udp>] retry-count <NUMBER: 0..255> retry-timeout
<NUMBER :Measured in 0.01 seconds units>
```

where

target <target>	is the SNMP target entry.
addr <IP address with mask>	is the target IP address.
param-name <String[32]>	is the param name.
tag <String[32]>	is the transport tag. This attribute must be set to TrapTag for V1 Trap. The default value is TrapTag.
udp-port <NUMBER: 0-65535>	is the UDP trap port.
transport-domain <snmp-udp | v4-udp | v6-udp>	is the transport domain.
retry-count <NUMBER: 0..255>	is the number of retries.
retry-timeout <NUMBER :Measured in 0.01 seconds units>	is the retry-timeout.

14 Configure a target-parameter to support v3 notification.

```
snmp create target-param <target-param> {sec-name
<String>} sec-model v3
```

where

target-param <target-param>	is the SNMP target parameters.
sec-name <String>	is the security name.
sec-model v3	sets the security model for the target parameter to v3.

15 Enable reliable traps.

```
snmp reliable-trap enable
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example configures SNMP reliable traps.

Create a notification entry by entering the following command.

```
snmp create notify <notify> {notify-tag <String[32]>} [notify-
type <trap|inform>]
```

Confirm the configuration of the notification entry:

```
snmp show notify
```

Configure a target-parameter with v2c security model to support v2c notification.

```
snmp create target-param informParamv2c sec-name public sec-
model v2c
```

Create an inform receiver.

```
snmp create target informTarget addr 192.168.1.1 param-name
informParamv2c tag InformTag retry-count 3 retry-timeout 1500
```

Enable reliable traps.

```
snmp reliable-trap enable
```

Create an SNMPv3 user with an auth-protocol and priv-protocol. You will be prompted to input the passwords once the command is entered.

```
snmp create user cienaV3User auth-protocol md5 echoless-auth-
password priv-protocol des echoless-priv-password
```

Create a second SNMPv3 user that uses the same username, auth-protocol, priv-protocol, and passwords as the previous user as well as the engine-id of the SNMPv3 manager.

```
snmp create user cienaV3User auth-protocol md5 echoless-auth-
password priv-protocol des echoless-priv-password engine-id
80:00:55:66:77:88:99:AA:AA
```

Attach the SNMPv3 user to an SNMPv3 access group.

```
snmp security-to-group attach user cienaV3User sec-model v3
group cienaV3Group
```

Create a view tree entry with a sub-tree that can be viewed. (Optionally, you can use the default viewtree, V12cView).

Copyright© 2022 Ciena® Corporation

```
snmp create viewtree cienaViewtree sub-tree iso type include
```

Create an access policy for the 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 cienaV3Group sec-model v3 sec-level
authWithPriv read-view cienaV3Viewtree write-view
cienaV3Viewtree notify-view cienaV3Viewtree
```

Create a notification tag with notify-type as inform.

```
snmp create notify cienaV3Notify notify-tag cienaV3NotifyTag
notify-type inform
```

Create an target SNMP trap server entry.

```
snmp create target cienaV3TrapTarget addr 10.10.10.10 param-
name cienaV3TrapParam tag cienaV3NotifyTag
```

Configure a target-parameter to support v3 notification.

```
snmp create target-param cienaV3TrapParam sec-name cienaV3User
sec-model v3 sec-level authWithPriv
```

Enable reliable traps.

```
snmp reliable-trap enable
```


Copyright© 2022 Ciena® Corporation

Procedure 3-12
Setting or unsetting the maximum SNMP inform queue length

Set or unset the maximum SNMP inform queue length.

The “set” action configures the upper limit on the SNMP inform queue length. By default, there is no upper limit on the SNMP inform queue length and it can grow indefinitely.

The “unset” action resets the SNMP inform queue length to zero. It removes any configured limit on the SNMP inform queue.

Step	Action

To set the maximum SNMP inform queue length

1 Set the maximum SNMP inform queue length:

```
snmp set max-inform-queue-length <max-inform-queue-length>
```

To unset the maximum SNMP inform queue length

2 Unset the maximum SNMP inform queue length:

```
snmp unset max-inform-queue-length
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 3-13
Showing or clearing SNMP inform statistics counters

Show or clear SNMP inform statistics counters.

SNMP inform statistics counters displayed are:

- Max Inform Queue Length
- Current Inform Queue Length
- Inform Sent
- Inform Acks Received
- Inform Dropped Timeout
- Last Timestamp Inform Dropped Timeout
- Inform Dropped Queue Full
- Last Timestamp Inform Dropped Queue Full

Note: The entry in the inform statistics table corresponding to the SNMP target is removed from the table when that target is deleted.

SNMP inform statistics counters cleared are:

- Inform Sent
- Inform Acks Received
- Inform Dropped Timeout
- Last Timestamp Inform Dropped Timeout
- Inform Dropped Queue Full
- Last Timestamp Inform Dropped Queue Full

Step	Action

To display the inform statistics counters table for all configured SNMP inform targets

1 To display the inform statistics counters for all configured SNMP inform targets:

```
snmp show statistics
```

To display the inform statistics counters table for a specific SNMP inform target IP address

2 To display the inform statistics counters for a specific SNMP inform target IP address:

```
snmp show statistics snmp-target <IP-address>
```


Copyright© 2022 Ciena® Corporation

To display the inform statistics counters table for a specific SNMP inform target port

3 To display the inform statistics counters for a specific SNMP inform target port:

```
snmp show statistics snmp-target-port <NUMBER>
```

where

NUMBER is in the range 0 to 65535

To clear the inform statistics counters table for all configured SNMP inform targets

4 To clear the inform statistics counters for all configured inform SNMP targets:

```
snmp clear statistics
```

To clear the inform statistics counters table for a specific SNMP inform target IP address

5 To clear the inform statistics counters for all a specific inform SNMP target IP address:

```
snmp clear statistics snmp-target <IP-address>
```

To clear the inform statistics counters table for a specific SNMP inform target port

6 To clear the inform statistics counters for all a specific inform SNMP target port:

```
snmp clear statistics snmp-target-port <NUMBER>
```

where

NUMBER is in the range 0 to 65535

—end—

Copyright© 2022 Ciena® Corporation

Procedure 3-14
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 are 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 is triggered if the amount of packets going through a port is higher than expected (rising threshold) or below normal (falling threshold).

You can:

- add an alarm entry
- display an alarm entry
- delete an alarm entry

Note: Switches support up to 36 alarm entries.

Step	Action

To add an alarm entry

1 Add an alarm entry:

```
rmon alarm add alarm-index <alarm-index> {data-source
<String[127]>} {falling-event-index <NUMBER:0-65535>}
{falling-threshold <NUMBER:0-999999999>} {interval
<duration: {N[yMwdhms]} *e.g. 1h10m3s>} [owner
<String127]>] {rising-event-index <NUMBER:0-65535>}
{rising-threshold <NUMBER:0-999999999>} {sample-type
<absolute|delta>} {startup-alarm <falling|rising|both>}
```


Copyright© 2022 Ciena® Corporation

where	
alarm-index <alarm-index>	is the index in the alarm table.
data-source <String[127]>	is the interface OID. Note that the ifIndex range is not the same on all devices. Use a MIB browser to determine the OID.
falling-event-index <NUMBER:0-65535>	is the falling event index.
falling-threshold <NUMBER:0-999999999>	is the minimum value (related to the particular interface MIB object being monitored) against which samplings are compared.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s	is the interval to be used for sending alarms, 1sec to 1year (N[yMwdhms]...).
owner <String[127]>	is the name of the owner.
rising-event-index <NUMBER:0-65535>	is the rising event index.
rising-threshold <NUMBER:0-999999999>	is the maximum value (related to the particular interface MIB object being monitored) against which samples are compared.
sample-type <absolute|delta >	is the type of sample.
startup-alarm <falling|rising|both>	defines the condition required to trigger an alarm.

To set RMON alarm attributes

2 Set RMON alarm attributes:

```
rmon alarm set alarm-index <alarm-index> [data-source
<String[127]>] [falling-event-index <NUMBER:0-65535>]
[falling-threshold <NUMBER:0-999999999>] {interval
<duration: {N[yMwdhms]} *e.g. 1h10m3s>} [owner
<String[127]>] [rising-event-index <NUMBER:0-
```


Copyright© 2022 Ciena® Corporation

```
65535>][rising-threshold <NUMBER:0-999999999>] [sample-
type <absolute|delta>] [startup-alarm
<falling|rising|both>]
```

where

alarm-index <NUMBER:1-65535>	is the index in the alarm table.
data-source <String[127]>	is the interface OID. Note that the ifIndex range is not the same on all devices; use a MIB browser to determine the OID.
falling-threshold <NUMBER:0-999999999>	is the minimum value (related to the particular interface MIB object being monitored) against which samplings are compared.
falling-event-index <NUMBER:0-65535>	is the falling event index.
interval <duration: {N[yMwdhms]} *e.g. 1h10m3s	is the interval to be used for sending alarms, 1sec to 1year (N[yMwdhms]...).
owner <String[127]>	is the name of the owner.
rising-threshold <NUMBER:0-999999999>	is the maximum value (related to the particular interface MIB object being monitored) against which samplings are compared.
rising-event-index <NUMBER:0-65535>	is the rising event index.
sample-type <absolute|delta >	is the type of sample.
startup-alarm <falling|rising| both>	defines the condition required to trigger an alarm.

Copyright© 2022 Ciena® Corporation

To unset RMON alarm attributes

3 Unset RMON alarm attributes:

```
rmon alarm unset alarm-index <alarm-index> [interval]
[owner] [sample-type] [startup-alarm]
```

where

alarm-index <alarm-index>	is the index in the alarm table.
interval	is the interval used for monitoring, in seconds.
owner	is the name of the owner.
sample-type	is the type of sample.
startup-alarm	defines the condition required to trigger an alarm.

To delete an alarm entry

4 Delete an alarm entry:

```
rmon alarm remove alarm-index <alarm-index>
```

where

alarm-index <alarm-index>	is the alarm entry to be deleted.

To display the alarm table

5 Display the alarm table:

```
rmon alarm show
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following 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.

> ***Note:*** Ensure that a stat-index has been set up prior to creating the alarm index.

```
rmon statistics add stat-index 5 port 1
```

Then create the alarm index:

```
rmon alarm add alarm-index 1 data-source 1.3.6.1.2.1.16.1.1.1.5 interval 30
owner Admin sample-type absolute startup-alarm both falling-event-index 1
falling-threshold 100 rising-event-index 1 rising-threshold 900
```

The following example shows sample output for the rmon show event command.

```
rmon show event
```

```
WARNING: This CLI output may take few minutes depending on the number of entries


+--------------------------- RMON EVENT STATISTICS -----------------------------+
| Index | Description                      | Event Type   | Community  | Owner    |
+-------+----------------------------------+--------------+------------+----------+
|              No RMON Event Statistics configured                               |
+-------+----------------------------------+--------------+------------+----------+
```

The following example deletes an alarm entry.

```
rmon alarm remove alarm-index 1
```


Copyright© 2022 Ciena® Corporation

Procedure 3-15
Configuring events

An event notifies you when an alarm is triggered.

You can

- add an event entry
- display an event entry
- delete an event entry

Note: Switches support up to 28 event entries.

Step	Action

To add an event entry

1 Add an event entry:

```
rmon event add event-index <event-index> {[community
<String[127]>] [owner <String[127]>] description
<String[127]> type <none|log|snmp-trap|log-and-
snmptrap>}
```

where

event-index <event-index>	is the index for the event in the event table.
community <String[127]>	is the event community to use.
owner <String[127]>	is the name of the owner of the event.
description <String[[127]]>	is a description of the event.
type <none|log|snmp-trap|log-and-snmptrap>	is the type of event created and where the information is sent.

Copyright© 2022 Ciena® Corporation

To set RMON event attributes

2 Set RMON event attributes:

```
rmon event set event-index <event-index> {[community
<String[127]>] [owner <String[127]>] description
<String[127]> type <none|log|snmp-trap|log-and-
snmptrap>}
```

where

event-index <event-index>	is the index for the event in the event table.
community <String[127]>	is the event community to use.
owner <String[127]>	is the name of the owner of the event.
description <String[[127]]>	is a description of the event.
type <none|log|snmp-trap|log-and-snmptrap>	is the type of event created and where the information is sent.

To unset RMON event attributes

3 Unset RMON event attributes:

```
rmon event unset event-index <event-index> {[community
<String[127]>] [owner <String[127]>] description
<String[127]> type <none|log|snmp-trap|log-and-
snmptrap>}
```

where

event-index <event-index>	is the index for the event in the event table.
community <String[127]>	is the event community to use.
owner <String[127]>	is the name of the owner of the event.
description <String[[127]]>	is a description of the event.
type <none|log|snmp-trap|log-and-snmptrap>	is the type of event created and where the information is sent.

To display event entries

4 Display event entries:

```
rmon show event
```


Copyright© 2022 Ciena® Corporation

To delete an event entry

5 Delete an event entry:

```
rmon event remove {event-index <event-index>}
```

where

event-index <event-index> is the event entry to be deleted.

—end—

Example

The following example adds an event entry.

```
rmon event add index 1 description Test type log community
Network1 owner Admin
```

The following example shows sample output for the rmon show event-table command.

```
rmon show event-table

+----------------------RMON EVENT STATISTICS---------------------------+
| Index | Description           | Event Type   | Community  | Owner    |
+-------+-----------------------+--------------+------------+----------+
| 1     | Test                  | log          | Network1   | Admin    |
+-------+-----------------------+--------------+------------+----------+
```

The following example deletes an event entry.

```
rmon event remove index 1
```


Copyright© 2022 Ciena® Corporation

Procedure 3-16
Configuring statistics

The statistics group (defined in RFC1757) provides information about data received over device ports. This information is a list of raw statistics. These statistic counters are either based on frames or bytes passing through the port.

When configuring statistics, you can:

- add a statistics entry
- delete a statistics entry
- display a statistics entry

Step	Action

1 Add an entry for Ethernet statistics:

```
rmon statistics add stat-index <stat-index> {port <Port>
[owner <String[127]>]}
```

where

stat-index <stat-index>	is the index.
port <Port>	is the port.
owner <String[127]>	is the owner of the history entry.

To delete a statistics entry

2 Delete a statistics entry:

```
rmon statistics remove {stat-index <NUMBER: 1..65535>}
```

where

stat-index <NUMBER: 1..65535>	is the statistics entry to remove.

To display a statistics entry

3 Display configured RMON statistics:

```
rmon statistics show
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example adds a statistics entry.

```
rmon statistics add stat-index 1 data-source ifIndex.10001
owner Admin
```

The following example deletes a statistics entry.

```
rmon statistics remove stat-index 1
```


Copyright© 2022 Ciena® Corporation

Procedure 3-17
Troubleshooting SNMP and RMON configuration

SNMP and RMON configuration is saved to the configuration file in the SNMP CONFIG: section.

Step	Action
1	View the configuration file: `configuration show`

—end—

Example

The following example shows sample output for the configuration show command.

```
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 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 usr-index 1 object snmplnPkts.0 control-index 1
sample-type absolute
!
```


Copyright© 2022 Ciena® Corporation

Procedure 3-18
Displaying RMON information

Display RMON information to verify configuration information.

Step	Action
1	Display RMON information: `rmon show {alarm} {auto-configuration} {event} {history} {statistics} {usr-history} {transfer}` where alarm — shows alarm information. auto-configuration — shows auto-configuration information. event — shows event information. history — shows history information. statistics — shows statistics information. usr-history — shows user history information. transfer — shows transfer information.

—end—

Copyright© 2022 Ciena® Corporation

Fault monitoring and analysis

Monitoring of chassis components can provide early warning indications of possible failure to ensure safe and reliable system operation and avoid network interruptions.

System resources are also monitored and available for display. System resource items include CPU and memory usage, as well as aggregations, meter profiles, virtual switches, and MAC tables.

Procedures

This chapter provides the following procedures:

- "Monitoring door status" on page 4-3
- "Monitoring fan speed status" on page 4-4
- "Monitoring temperature and status" on page 4-5
- "Monitoring power supply status" on page 4-9
- "Monitoring device-id status" on page 4-12
- "Enabling and disabling POSTs" on page 4-13
- "Monitoring POSTs" on page 4-14
- "Enabling and disabling dying gasp" on page 4-15
- "Configuring dying gasp informs" on page 4-16
- "Displaying dying-gasp" on page 4-17
- "Set and unset source port for dying gasp" on page 4-18
- "Displaying device archives" on page 4-19
- "Saving device archives to flash" on page 4-20
- "Displaying device identification attributes" on page 4-21
- "Displaying platform capabilities" on page 4-22
- "Displaying the chassis MAC address" on page 4-24
- "Configuring port traps and servers" on page 4-25
- "Displaying an alarm entry" on page 4-26

Copyright© 2022 Ciena® Corporation

- “Monitoring system health and resources” on page 4-27
- “Displaying the event severity to Syslog severity mapping” on page 4-35

Copyright© 2022 Ciena® Corporation

Procedure 4-1
Monitoring door status

For switches that have inner and outer doors for access to ports, you can display the status of the doors to determine if they are open or closed.

Step	Action
1	Display door status: `chassis show door`

—end—

Example

The following example shows output from the chassis show door command.

```
chassis show door

+------------------------- CHASSIS DOOR STATUS --------------------------+
| Parameter               | Value                                        |
+-------------------------+----------------------------------------------+
| OUTER DOOR              | OPEN                                         |
| INNER DOOR              | CLOSED                                       |
+-------------------------+----------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-2
Monitoring fan speed status

The 3903, 3903x, 3904, 3906, 3926, 3928, 5142, and 5160 platforms provide redundant internal fans for cooling internal components. If one of the fans shows a minimum or average fan speed RPM that is significantly lower than the other fan(s), this might indicate a possible fan failure.

Table 4-1 lists the fields in the fan speed status display.

Table 4-1
Fields in the fan speed status display

Field	Description
Fan ID	ID of each fan.
Current	Current speed measured in revolutions per minute RPM.
Average	Fan speed averaged for the device's uptime.
Minimum	Slowest fan speed since the last reboot of the device in revolutions per minute.

Step	Action
1	Check fan status: `chassis show fans`

—end—

Example

The following example shows sample output for the chassis show fans command.

```
+------------ FAN SPEED STATUS ------------+
| FanId | Current    | Average    | Minimum  |
+-------+------------+------------+----------+
| 1     | 5969 rpm   | 5965 rpm   | 5922 rpm |
| 2     | 6110 rpm   | 6118 rpm   | 6063 rpm |
| 3     | 6157 rpm   | 6118 rpm   | 6063 rpm |
+-------+------------+------------+----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-3
Monitoring temperature and status

All platforms are equipped with temperature sensors to measure and report the device's current operating temperature. For rackmount style platforms, the sensor reading is adjusted to provide an approximation of the ambient air temperature outside of the platform. This ambient air is drawn in by the fans and used to cool the device.

The 3905 differs in that in that both are a sealed, weatherproof design and do not employ fans. The temperature sensor reading for the 3905 is not adjusted, and provides the internal temperature within the 3905. The temperature reading for each platform is available by CLI command.

Two fixed temperature alarm thresholds are set on the device, a low temperature threshold and a high temperature threshold. These default thresholds are set based on the platform type and on the environmental operating specification for each platform. Exceeding these temperature thresholds can cause damage to the device and may void the warranty.

Copyright© 2022 Ciena® Corporation

Table 4-2 shows the low and high temperature thresholds for each platform.

Table 4-2
Temperature Sensor Alarm Thresholds

Platform	Low	High
3903	0°C	45°C
3903x	0°C	45°C
3904	0°C	65°C
3905	-40°C	65°C
3906	0°C	40°C
3926	-40°C	65°C
3928 (AC version)	0°C	50°C
3828 (DC version)	-40°C	65°C
3942	-5°C	65°C
5142	-40°C	65°C
5160	-40°C	65°C

The device stores the highest and lowest temperatures. Also, when a high/low temperature violation is detected, a counter is incremented. Separate counters are kept for high and low temperature violations.

> ***Note:*** The temperature status displayed by the `chassis show temperature` command cannot be cleared; however, this data is not persistent across a reboot. The values stored in the device archive (displayed by the `device-archive show` command) are persistent.

Copyright© 2022 Ciena® Corporation

Table 4-3 lists the fields in the chassis show temperature display.

Table 4-3
Fields in the chassis show temperature display

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.

Step Action

To set the temperature thresholds

1 Set the high temperature threshold:

```
chassis set temperature-high-threshold <#>
```

where

temperature-high-threshold <#> is the high temperature threshold in degrees Celsius.

2 Set the low temperature threshold:

```
chassis set temperature-low-threshold <#>
```

where

temperature-low-threshold <#> is the low temperature threshold in degrees Celsius.

To check chassis temperature

3 Check chassis temperature.

```
chassis show temperature
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example sets the high temperature threshold to 50 degrees Celsius.

```
chassis set temperature-high-threshold 50
```

The following example sets the low temperature threshold to 0 degrees Celsius.

```
chassis set temperature-low-threshold 0
```

The following example shows sample output of the chassis show temperature command for a device.

```
chassis show temperature
```

```
+- TEMPERATURE THRESHOLD -+
| Low         | High       |
+-------------+------------+
| -40 C       | 65  C      |
+-------------+------------+

+--- TEMPERATURE STATUS --+
| Current | Low   | High  |
+---------+-------+-------+
| 17  C   | 17  C | 21  C |
+---------+-------+-------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-4
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.

Table 4-4
Power supply status

Field	Description
ID	• ID A— Main power supply • ID B— 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.
PS Fan	• Online — Power supply fan is operational. • Offline — Power supply fan is installed but not turned on. • Faulted — Power supply fan is not functioning.

Step	Action
1	Check the power supply status. `chassis show power`

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows sample output for the chassis show power command when two power supplies are present.

> ***Note:*** This information is only available on systems that have removable power supplies: 5142 and 5160.

```
chassis show power

+---------- POWER SUPPLY STATUS -----------+
| Id      | Type       | State    | PS Fan   |
+---------+------------+----------+----------+
| A       | AC         | Online   | Online   |
| B       | AC         | Online   | Online   |
+---------+------------+----------+----------+

+---------------- POWER SUPPLY ID A ----------------+
| Parameter                  | Value                |
+----------------------------+----------------------+
| Model Number               | 170-0014-900         |
| Serial Number              | M6517510             |
| Revision                   | ;;A                  |
| CLEI Code                  | CMUPAABAAA           |
| Manufactured Date          | 1111                 |
| Input                      | AC                   |
| Input Voltage              | 85-265               |
| Output Voltage             | 12                   |
| Manufacturing Location     | CHINA                |
| Checksum                   | 84                   |
+----------------------------+----------------------+

+---------------- POWER SUPPLY ID B ----------------+
| Parameter                  | Value                |
+----------------------------+----------------------+
| Model Number               | 170-0014-900         |
| Serial Number              | M6517530             |
| Revision                   | ;;A                  |
| CLEI Code                  | CMUPAABAAA           |
| Manufactured Date          | 1111                 |
| Input                      | AC                   |
| Input Voltage              | 85-265               |
| Output Voltage             | 12                   |
| Manufacturing Location     | CHINA                |
| Checksum                   | 86                   |
+----------------------------+----------------------+
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the chassis show power command when one of the power supplies is missing.

```
chassis show power

+---------- POWER SUPPLY STATUS -------------+
| Id      | Part Number| Type      | State   |
+---------+------------+-----------+---------+
| A       | N/A        | Unequipped| Faulted |
| B       | Unequipped | AC        | Offline |
+---------+------------+-----------+---------+

Power Supply ID A is not present

+---------------- POWER SUPPLY ID B ----------------+
| Parameter                  | Value                |
+----------------------------+----------------------+
| Model Number               | 170-0070-900         |
| Serial Number              | M6869210             |
| Revision                   | 001                  |
| CLEI Code                  | NOCLEICODE           |
| Manufactured Date          | 1208                 |
| Input                      | AC                   |
| Input Voltage              | 85-265               |
| Output Voltage             | 12                   |
| Manufacturing Location     | CHINA                |
| Checksum                   | 87                   |
+----------------------------+----------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-5
Monitoring device-id status

Monitor device-id status.

Step	Action
1	Monitor device-id status: `chassis show device-id`

—end—

Example

The following example shows sample output for the chassis show device-id command.

```
chassis show device-id

+---------------- CHASSIS DEVICE ID ----------------+
| Parameter                  |                      |
+----------------------------+----------------------+
| Device Type                | 095                  |
| Part Number/Revision       | 170-3926/001         |
| Serial Number              | 3926-096             |
| Manufactured Date          | 20130111             |
| CLEI Code                  | CMMGS00CRA           |
| Location of Manufacture    | 1                    |
| Chassis MAC Address        | 00:02:5a:01:da:29    |
| Param Version              | 007                  |
+----------------------------+----------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-6
Enabling and disabling POSTs

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 indicate that no errors were detected. To monitor POST results, refer to "Monitoring POSTs" on page 4-14.

Step	Action
To disable POST	
1	Disable POST: `chassis post disable`
To enable POST	
2	Enable POST: `chassis post enable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 4-7
Monitoring POSTs

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.

Step	Action

To check POST state and results

1 Check POST state and results:

```
chassis post show
```

To clear POST results errors:

2 Clear POST results errors:

```
chassis post clear
```

—end—

Example

The following examples show sample output for the chassis port show command.

```
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: SEVERE: 0x8821b00a Port 11:Rx packets
= 0 of 1000 SWITCH: SEVERE: 0x8821b00a Port 11:Tx packets = 0 of 1000
```


Copyright© 2022 Ciena® Corporation

Procedure 4-8
Enabling and disabling dying gasp

Enable and disable dying gasp.

Step	Action
To enable dying gasp	
1	Enable dying gasp: `chassis dying-gasp enable`
To disable dying gasp	
2	Disable dying gasp: `chassis dying-gasp disable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 4-9
Configuring dying gasp informs

Configure dying gasp informs.

Step	Action
1	Configure dying gasp informs: `chassis dying-gasp set informs <on|off>`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 4-10
Displaying dying-gasp

Display dying gasp to see its status and whether informs are on or off.

Step	Action
1	Display dying-gasp: `chassis dying-gasp show`

—end—

Example

The following example shows the output from the chassis dying-gasp show command:

```
chassis dying-gasp show

+------------------------- DYING GASP STATUS -----------------------------+
| Parameter                | Value                                        |
+--------------------------+----------------------------------------------+
| DYING GASP STATUS        | DISABLED                                     |
| DYING GASP INFORMS       | OFF
| DYING GASP SOURCE PORT   | 0
+--------------------------+----------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-11
Set and unset source port for dying gasp

Set and unset source port for dying gasp.

Step	Action

To set source port for dying gasp

1 Set source port for dying gasp:

```
chassis dying-gasp set src-port <src-port-number>
```

where

src-port-number any source port number in range 32768..60999

To unset source port for dying gasp

2 Unset source port for dying gasp, this will set the source port value to default value ‘0’:

```
chassis dying-gasp unset src-port
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 4-12
Displaying 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.

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

> ***Note:*** The maximum and minimum temperatures shown to the right of the Highest Temperature and Lowest Temperature values reflect the platform specific temperature capabilities as listed in Table 4-2.

Step	Action
1	Display device archives: `device-archive show`

—end—

Example

The following example shows sample output for the device-archive show command.

```
device-archive show

+------------------------- DEVICE ARCHIVE -------------------------------+
| Parameter                                    | Value                   |
+----------------------------------------------+-------------------------+
| Cumulative system uptime (seconds)           | 59310918                |
| Cumulative system uptime (days:hh:mm:ss)     | 686:11:15:18            |
| Archived system uptime (seconds)             | 59256558                |
| Archived system uptime (days:hh:mm:ss)       | 685:20:09:18            |
| Highest Temperature (degrees Celsius)        | 63              (50 MAX)|
| Number of High Temperature Violations        | 0                       |
| Lowest Temperature (degrees Celsius)         | 8             (  0 MIN)|
| Number of Low Temperature Violations         | 0                       |
| Number of Soft Resets                        | 68                      |
| Total Number of Resets                       | 133                     |
| Last Reset Reason                            | Upgrade                 |
| Total number of Guardian Reboots             | 0                       |
+----------------------------------------------+-------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-13
Saving device archives to flash

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

Step	Action
1	Save device archives to flash: `device-archive save`

—end—

Example

The following example shows sample output for the device-archive save command.

```
device-archive save
file cd /mnt/sysfs/archive
file ls
-rw-r--r--    1 root     root           167 Jan  1 00:10 default.arc
```


Copyright© 2022 Ciena® Corporation

Procedure 4-14
Displaying device identification attributes

Device identification attributes includes:

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

Step	Action
1	Display device identification attributes: `chassis show attributes`

—end—

Example

The following example shows sample output for the chassis show attributes command.

```
chassis show attributes

+---------------- CHASSIS DEVICE ID ----------------+
| Parameter                 |                      |
+---------------------------+----------------------+
| Chassis Device Type       | 095                  |
| Chassis Hardware Version  | 170-3926/001         |
| Chassis Serial Number     | B6xxxxxx             |
| Chassis MAC Address       | 00:02:5a:01:da:29    |
| Param Version             | 007                  |
+---------------------------+----------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-15
Displaying platform capabilities

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

Step	Action
1	Display platform capabilities: `chassis show capabilities`

—end—

Example

The following example shows sample output for the chassis show capabilities command executed on a 3926 device.

```
chassis show capabilities

+---------------------------------- PLATFORM CAPABILITIES --------------------------+
| Parameter                        | Value                                          |
+----------------------------------+------------------------------------------------+
| Capabilities Class               | 0                                              |
| Platform Type                    | 100                                            |
| Platform Name                    | 3926                                           |
| Platform Description             | 3926 Service Delivery Switch                   |
| No. Slots                        | 1                                              |
| Primary Ctrl Blade               | 1                                              |
| No. Fan Trays                    | 1                                              |
| No. Fans Per Tray                | 2                                              |
| Fixed DC Power                   | No                                             |
| Redundant Power                  | No                                             |
| Max Physical Ports               | 6                                              |
| Max LAG Ports                    | 6                                              |
| Max IP Interfaces                | 64                                             |
| Max VLANs                        | 4094                                           |
| VLAN Translation                 | Supported                                      |
| Max VLAN Cross Connections       | 4096                                           |
| Global Inner TPID Configuration  | Supported                                      |
| Max IGMP Snoop Service Instances | 500                                            |
| Max Mcast Groups                 | 1022                                           |
| Max Mcast Source Addrs           | 2048                                           |
| Max Mcast Source Addrs Per Grp   | 64                                             |
| Max Mcast Logical Interfaces     | 3000                                           |
| Max Mcast Member Interfaces      | 12264                                          |
| Max MSTIs                        | 8                                              |
| Max RSTP Domains                 | 32                                             |
| Max PM Instances                 | 739 (0 auto, 739 user)                         |
| Max PM Bins (Class 0)            | 0 (0 auto, 0 user)                             |
| Max PM Bins (Class 1)            | 23363 (0 auto, 23363 user)                     |
| Max PM Interval Profiles         | 0                                              |
| Protocol Filters                 | Not Supported                                  |
| Max MPLS Ingress Tunnels         | 500                                            |
| Max MPLS Egress Tunnels          | 500                                            |
| Max MPLS Transit Tunnels         | 1000                                           |
| Max MPLS VCs                     | 1000                                           |
| Max MPLS L2VPNs                  | 1000                                           |
| Max MPLS VSs                     | 1000                                           |
|   Max MPLS VPWS VSs              | 1000                                           |
|   Max MPLS VPLS VSs              | 500                                            |
| Max Ethernet VCs                 | 1024                                           |
| Max Default VSs                  | 1024                                           |
| Max VSs                          | 1024                                           |
```


Copyright© 2022 Ciena® Corporation

Max VS Subs	4096
Max L2-CFT Profiles	64
Max Tagged PVST L2PT Instances	6
VC Transforms	Supported
Max VC L2 Transforms	1
Max VCs with L2 Transform	512
Egress Bandwidth Shaping	Not Supported
Multi Subs Per Port	True
Max Redundancy Groups	6
Max Links per Redundancy Group	1
VPLS FPGA Support	False
PBT FPGA Support	False
L2 MAC Table Expansion	Not Supported
Max DYNA-SA Entries	32000
Max FSMT Entries	0
Max SRVC-LVL Entries	0
Max L2-SAC Entries	12
Max SMT Entries	1024
Max EPR Snids	0
Ring Protection	Supported
Max Logical Rings	5
Max Virtual Rings	10
Network Sync	Not Supported
BITS Timing	Not Supported
GPS Timing	Not Supported
PTP Timing	Not Supported
Dying Gasp	Supported
Benchmark	Supported
Max Benchmark Bandwidth (Mbps)	1000
Benchmark Reflector	Supported
Benchmark Generator	Supported
Max Benchmark Concurrent Tests	32
Max Benchmark Profiles Config	128
Max Benchmark Unique Active CVIDs	16
Max ACL Profile Definitions	512
Max ACL Rule Definitions	1024
Max DHCP Relay Agents	512

Copyright© 2022 Ciena® Corporation

Procedure 4-16
Displaying the chassis MAC address

The chassis MAC address is assigned at manufacturing. This MAC address is a base address from which blocks of addresses are allocated. The number of blocks depends upon the platform.

Table 4-5 lists reserved blocks for each platform.

Table 4-5
Reserved blocks for each platform

Platform	Reserved blocks
3903, 3903x, 3904, 3905, 3906	16
3926, 3928, 3942, 5142, 5160	32

Step	Action
1	Display the chassis MAC address: `chassis show mac`

—end—

Example

The following example shows sample output for the chassis show mac command.

```
chassis show mac

+-------------- CHASSIS MAC PARTITIONS --------------+
| Partition         | Base MAC           | Block Size |
+-------------------+--------------------+------------+
| Chassis           | 00:03:18:6d:a9:60  | 16         |
+-------------------+--------------------+------------+
| Local Mgmt        | 00:03:18:6d:a9:60  | 1          |
| L3 Interface      | 00:03:18:6d:a9:61  | 1          |
| Port Base         | 00:03:18:6d:a9:62  | 12         |
| Benchmark         | 00:03:18:6d:a9:6e  | 1          |
| Remote Mgmt       | 00:03:18:6d:a9:6f  | 1          |
+-------------------+--------------------+------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-17
Configuring port traps and servers

When the port trap is disabled, any traps generated by the port are not transmitted to a configured trap server. By default, port traps are enabled for all ports.

Step	Action

To disable port traps

1 Disable port traps:

```
snmp port-traps disable port <port>
```

where

port <port> is the port number.

To display all port traps

2 Display all port traps:

```
snmp show port-traps
```

—end—

Example

The following example disables traps on port 10.

```
snmp port-traps disable port 10
```


Copyright© 2022 Ciena® Corporation

Procedure 4-18
Displaying an alarm entry

Display an alarm entry.

Step	Action

1 Display an alarm entry:

```
rmon show alarm-index <alarm-index>
```

where

alarm-index <alarm-index> is the alarm table object.

—end—

Example

The following example shows sample output for an alarm with an index value of 1.

```
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                          |
+--------+---------------+--------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-19
Monitoring system health and resources

A set of system health and resources are automatically monitored and measured at various intervals. Depending upon the measurements and predefined limits, a monitored item is assigned a state:

- Normal - Operating in normal limits.
- Warning - Minor errors occurred or item is measuring slightly outside of normal limits.
- Degraded - Quantity of errors or measurements exceed normal limits and indicate performance and reliability are adversely affected.
- Faulted - Failed or is measuring beyond safe limits.

When a monitored item changes to Normal, Warning or Degraded states, a system health event is generated with the name of the monitored item, previous state, new state, and information specific to the monitored item.

When a monitored item changes to the Faulted state (if applicable), a system fault is generated, logged, and any action associated with the fault is run.

When the health state of memory utilization changes, the following actions are taken:

- Normal to any other state (Warning/Degraded/Faulted)— Raise an alarm
- Any other state (Warning/Degraded/Faulted) to Normal—Clear an alarm
- Any change in health state (Normal to Warning or Warning to Degraded, and so on)—Generate a notification trap

When the health state of virtual memory utilization changes, the following actions are taken:

- Normal to any other state (Warning/Degraded/Faulted)— Raise an alarm
- Any other state (Warning/Degraded/Faulted) to Normal—Clear an alarm
- Warning to Cleared_warning or Degraded to Cleared_degraded or Fault to Cleared_fault—Clear the alarm
- Any change in health state (Normal to Warning or Warning to Degraded, and so on)—Generate a notification trap

The system observes the pattern of virtual memory utilization for half an hour. If it is constant for the last half-hour, then the system updates the state as follows.

- Normal to Normal (No state change)
- Warning to Cleared_warning

Copyright© 2022 Ciena® Corporation

- Degraded to Cleared_degraded
- Fault to Cleared_fault

The system clears the alarm and generates the trap and syslog events, capturing the newly defined states.

Note 1: For more information on health states and the behavior related to virtual memory utilization, see LEOS process virtual memory utilization.

Note 2: For information on the means by which the system avoids bursts of HRM traps, see Debouncing health resource monitoring traps.

Table 4-6 lists monitored items and the criteria for each state.

Table 4-6
Monitored items and the criteria for each state

Monitored Item	Description	Healthy	Warning	Degraded	Fault
CPU Utilization (cpu-utilization)	CPU activity measured at 5, 10, and 60-second intervals. The CPU utilization minimum and maximum values represent the minimum and maximum values for the interval (x) since the system booted, (where x is equal to 5, 10 and 60 seconds).	Less than 75%	From 75% to 94%	95% or more	Not applicable
CPU Load Average (cpuload) 3903, 3903x, 3904, 3905, 3906, 3926, 3928	Moving average of processes in the operating system's run queue marked running or uninterruptable. Measured at 1, 5, and 15-minute intervals. The CPU load average minimum and maximum values represent the minimum and maximum values for the interval (x) since the system booted, (where x is equal to 1, 5 and 15 minutes).	Less than 6	Between6 and 8	Greater than 8	Not applicable

Copyright© 2022 Ciena® Corporation

Table 4-6
Monitored items and the criteria for each state

Monitored Item	Description	Healthy	Warning	Degraded	Fault
CPU Load Average (cpuload) 5142, and 5160 platforms (four core processors)	Moving average of processes in the operating system's run queue marked running or uninterruptable. Measured at 1, 5, and 15-minute intervals. The CPU load average minimum and maximum values represent the minimum and maximum values for the interval (x) since the system booted, (where x is equal to 1, 5 and 15 minutes).	Less than 8	Between 8 and 10	Greater than 10	Not applicable
File System Utilization (file-system-utilization)	Usage in /tmp and /mnt/sysfs directories	Less than 75%	From 75% to 94%	From 95% to 99%	100%
Memory Utilization (memory-utilization)	Available memory and used memory in megabytes (MB).				
	All SAOS devices	Greater than 130MB	Between 80MB and 130MB	Less than 80MB	Less than or equal to 15MB
Virtual Memory Utilization	SAOS virtual memory available (= Total virtual memory allocated - SAOS virtual memory used)	Less than 85%	From 85% to 89%	From 90% to 94%	Greater than or equal to 95%

Copyright© 2022 Ciena® Corporation

LEOS process virtual memory utilization

Health resource monitoring (HRM) monitors the LEOS process virtual memory usage for the following items:

- SAOS Virtual Memory Available
- SAOS Virtual Memory Used

The item “SAOS Virtual Memory Used” is equal to the “VmSize” parameter extracted from ‘proc/self/status’ file. The “Total virtual memory allocated” is calculated from the stack pointer that stores the address of the stack segment for each thread. The item “SAOS Virtual Memory Available” is the difference between “Total virtual memory allocated” and “SAOS Virtual Memory Used”.

The following table shows how HRM will determine the CPU health state of “SAOS Virtual Memory Available”.

Table 4-7
Formulas for determining virtual memory health states

Normal	Warning	Degraded	Fault
x < 85%	85% <= x < 90%	90% <= x < 95%	x >= 95%
Note 1: The value x is virtual memory utilization in percent. ***Note 2:*** For determining the current health state, values are calculated in terms of percentage using the following formula: (SAOS Virtual Memory Used * 100) / (SAOS Virtual Memory Used + SAOS Virtual Memory Available)			

When the virtual memory health state changes, the following action will be taken:

- If the state changes from normal to warning or degraded or fault, the system **raises an alarm**.
- If the state changes to normal from warning or degraded or fault, the system **clears the alarm**.
- If there is any change in the health state (for example, normal to warning or warning to degraded), the system **generates a notification trap**.

“cleared_” states. The following virtual memory states are introduced: cleared_warning, cleared_degraded, and cleared_fault. Each “cleared_” state indicates the system has observed a constant pattern of virtual memory

Copyright© 2022 Ciena® Corporation

utilization. If the health state is warning or degraded or fault, but the pattern of memory utilization has remained constant for half an hour, the system then updates the health state as shown in the following table.

Table 4-8
Health state update "cleared" state

Health state for the previous half hour	Updated state
warning	cleared_warning
degraded	cleared_degraded
fault	cleared_fault

When the system updates the health state to one of the "cleared_" states, it clears the alarm that was raised when the state changed from normal to warning or degraded or fault.

For example, if the constant pattern for virtual memory utilization was observed at a degraded state, then after half an hour, the system updates the state from degraded to cleared_degraded. This indicates that the last highest reachable state was degraded and now the next time the threshold is crossed, the state will change directly to degraded.

> ***Note:*** These new states are included to provide a workaround to clear virtual memory utilization alarms/traps when the system becomes stable after heavy soak operations. Actually, when soak operations are started, then the LEOS process/threads dynamically allocate memory in large chunks and free it when soak operations are stopped. After that, memory is freed at the heap layer but the process holds kernel pages to be used in the future. This is due to system level optimizations for virtual memory utilizations. Consequently, virtual memory utilization is not decreased. Now when virtual memory utilization crosses a threshold, the SAOS software raises an alarm to indicate the same. But when everything is normal, that is, soak operations are stopped, then this alarm is not getting cleared because the virtual memory utilization is not decreased and still over the threshold values. To override the system optimizations, these intermediate states are introduced to clear an alarm and indicate to the user that the system is working fine, even though virtual memory utilization still shows as high.

Copyright© 2022 Ciena® Corporation

Debouncing health resource monitoring traps

Health resource monitoring (HRM) traps are generated whenever the state of a health item changes. Health states are updated in five-second intervals. To avoid a burst of HRM traps within a short time period, a debouncing mechanism is implemented. After detecting a health state change, it waits for a certain period and re-checks the health state before triggering a trap. If the health state changes back to a previous state during the waiting period, then the debouncing mechanism cancels tracking of the associated state change. The waiting periods differ for various health items.

This table shows the waitings periods for various health items:

Table 4-9
Waiting periods for various health items

Health item	Waiting period
CPU load 1 minute	1 minute
CPU load 5/15 minutes	5 minutes
CPU utilization 1 minute	1 minute
File utilization	20 seconds
Memory utilization	20 seconds
Virtual memory utilization	20 seconds

This table shows the health items for which there is no wait period when the health state changes. Traps are triggered as soon as they are detected.

Table 4-10
States for various health items

Health item	State
CPU load 1/5/15 minutes	Degraded
CPU utilization	Degraded
File utilization	Fault
Memory utilization	Fault
Virtual memory utilization	Fault

Copyright© 2022 Ciena® Corporation

Step	Action

To display health and resources for one or more monitored items

1 Display health and resources for one or more monitored items:

```
system health show cpu-utilization cpu-load-average
memory-utilization file-system-utilization {detail}
```

where

cpu-utilization	shows system CPU usage.
cpu-load-average	shows system CPU load average.
memory-utilization	shows system memory usage.
file-system-utilization	shows file system usage.
file-utilization	shows available and used xFTP space on flash memory.
{detail}	when specified for memory-utilization, enhances the display by showing the detailed usage of system memory and SAOS virtual memory.

To display monitored items in a selected state

2 Display monitored items in a selected state:

```
system health show state <normal|warning|degraded|fault>
```

where

state <normal | warning | degraded | fault | exception>	shows health items currently at certain state.

—end—

Example

The following example shows sample output for the system health show command with cpu-utilization selected as the monitored item.

```
system health show cpu-utilization

+--------------------------- HEALTH MONITORING ---------------------------+
|              Item             | Health    | Current | Min     | Max     |
|                               | State     | Value   | Value   | Value   |
+-------------------------------------------------------------------------+
|Cpu Utilization (%)            |           |         |         |         |
| Last 5 seconds                |    Normal |       3 |       1 |      28 |
| Last 10 seconds               |    Normal |       3 |       1 |      28 |
| Last 60 seconds               |    Normal |       3 |       2 |      11 |
+-------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the system health show state command with a selected state of normal.

```
system health show state normal
+--------------------------- HEALTH MONITORING ---------------------------+
|              Item             | Health    | Current | Min     | Max     |
|                               | State     | Value   | Value   | Value   |
+-------------------------------------------------------------------------+
|Cpu Utilization (%)            |           |         |         |         |
| Last 5 seconds                |    Normal |       3 |       1 |      28 |
| Last 10 seconds               |    Normal |       3 |       1 |      28 |
| Last 60 seconds               |    Normal |       3 |       2 |      11 |
+-------------------------------------------------------------------------+
|Cpu Load Average               |           |         |         |         |
| Last 1 minute                 |    Normal |    0.05 |    0.01 |    2.51 |
| Last 5 minutes                |    Normal |    0.10 |    0.03 |    0.74 |
| Last 15 minutes               |    Normal |    0.09 |    0.05 |    0.26 |
+-------------------------------------------------------------------------+
|Memory Utilization (Kbytes)    |           |         |         |         |
| Used                          |       n/a |  521444 |  513684 |  521972 |
| Available                     |    Normal | 3504356 | 3503828 | 3512116 |
+-------------------------------------------------------------------------+
|File System Utilization (% usage)|        |         |         |         |
| /tmp/                         |    Normal |       1 |       1 |       1 |
| /mnt/sysfs/                   |    Normal |       4 |       4 |       4 |
| /mnt/log/                     |    Normal |       8 |       8 |       8 |
+-------------------------------------------------------------------------+
```

The following example shows sample output for the enhanced memory-utilization show state command:

```
system health show memory-utilization detail

+---------------------------- HEALTH MONITORING ----------------------------+
|              Item             | Health    | Current | Min     | Max     |
|                               | State     | Value   | Value   | Value   |
+-------------------------------------------------------------------------+
|Memory Utilization (Kbytes)    |           |         |         |         |
| System Memory Used            |       n/a | 1147712 | 1132632 | 1154392 |
| System Memory Available       |    Normal |  884688 |  878008 |  920764 |
| SAOS Virtual Memory Used      |       n/a | 1304944 | 1293884 | 1318944 |
| SAOS Virtual Memory Available |    Normal |  747248 |  733248 |  778176 |
+-------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-20
Displaying the event severity to Syslog severity mapping

Display the event severity to Syslog severity mapping.

Step	Action

To display event severities mapped to Syslog severities

1 Display the complete list of event severities and how they map to Syslog severities:

```
syslog show severity-mapping
```

where

severity-mapping shows event/syslog severity map.

To display flash log event severities mapped to Syslog severities

2 Display flash log event severity values and how they map to Syslog severity values:

```
log flash show severity-mapping
```

where

severity-mapping shows event/syslog severity map.

To display ram log event severities mapped to Syslog severities

3 Display ram log event severity values and how they map to Syslog severity values:

```
log ram show severity-mapping
```

where

severity-mapping shows event/syslog severity map.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows sample output for the syslog show severity-mapping command.

```
syslog show severity-mapping

+--- SEVERITY MAPPING ----+
|   Event    |  Syslog    |
+------------+------------+
| critical   | emergency  |
| major      | alert      |
| minor      | error      |
| warning    | warning    |
| config     | notice     |
| info       | info       |
| debug      | debug      |
+------------+------------+
```


Copyright© 2022 Ciena® Corporation

Link flap detection for fault management

This chapter describes link flap detection for fault management and provides procedures for configuring link flap detection for fault management.

Link flap detection

Link flap detection is available on physical ports. Detection consists of monitoring the link state of the port for Up to Down transitions.

If a number of up or down transitions occur within a specified time frame, a link flap event is generated. The port is marked as operationally down for either a period of time or until manual intervention takes place. The user can configure:

- the number of transitions to trigger the event
- the duration of the monitoring timeframe
- the time period during which the port will be marked as down

You can configure traps such that you get various notifications each time the port goes up and each time it goes down. You can check for these notifications and disable the port.

Manual intervention consists of setting the port to administratively disabled, then enabled. If manual intervention occurs during the time the port is being held operationally down by the hold timer, this terminates the link flap event without waiting for the timer to expire.

This chapter provides the following procedure for link flap detection:

- “Configuring link flap detection” on page 5-2

Copyright© 2022 Ciena® Corporation

Procedure 5-1
Configuring link flap detection

Configure link flap detection to automatically disable the port that is going up and down and notify you of the link flap condition.

Step	Action

1 Enable the link flap feature.

```
port set port <PortNameList> link-flag-detect on
```

where

port <PortNameList>	is the port that you want to enable the link flap feature on.
link-flag-detect	Indicates whether link flap detection is enabled.

2 Set the number of port state down transitions that will trigger a link flap event.

```
port set port <PortNameList> link-flap-count <1-64>
```

where

port <PortNameList>	is the port that you want to enable the link flap feature on.
link-flap-count <1-64>	is the number of up or down transitions within a configurable period of time that trigger a link flap event.

3 Set the time frame in which to count port state transitions.

```
port set port <PortNameList> link-flap-detect-time <0-600>
```

where

port <PortNameList>	is the port that you want to enable the link flap feature on.
link-flap-detect-time <0-600>	is the amount of time associated with the link flap count.

4 Set the time interval to mark the port operationally down after a link flap event is triggered.

```
port set port <PortNameList> link-flap-hold-time <0-600>
```

where

port <PortNameList>	is the port that you want to enable the link flap feature on.
link-flap-hold-time <0-600>	is the amount of time that the port is marked operationally down after a a link flap event.

—end—

Copyright© 2022 Ciena® Corporation

Alarm management

Alarms are generated when a failure or fault is detected in the network elements. Events are correlated into alarms based on their significance. Alarms are messages that call for an operator or administrator's attention. When an alarm is created, the problem associated with the alarm may be resolved. This chapter contains the following information on alarm management for the 39XX/51XX Switches and Platforms.

- "Alarm Manager" on page 6-1
- "Alarm classes" on page 6-2
- "Alarm instances" on page 6-2
- "Alarm severity levels" on page 6-2
- "Types of alarms" on page 6-3
- "Alarm tables" on page 6-5
- "Alarm records" on page 6-7
- "External alarms" on page 6-9
- "Alarm differences" on page 6-12
- "Alarm instances" on page 6-12
- "Alarms and corresponding events" on page 6-13
- "World Wide Packet traps and corresponding events" on page 6-18
- "Ciena traps and corresponding events" on page 6-25
- "Standard traps and corresponding events." on page 6-28

Alarm Manager

The Alarm Manager provides carrier-grade alarm management by maintaining the state of each alarm that occurs on the 39XX/51XX Switches and Platforms. It also optionally notifies the management station.

The Alarm Manager draws immediate attention to things that need it. Its controls exist for configuration and for adapting to situations where the originating cause may not be immediately correctable. The Alarm Manager also facilitates operator notification.

Copyright© 2022 Ciena® Corporation

All alarm settings can be configured by the operator. No alarm setting can cause physical harm to befall the system. For example, settings in the Alarm Manager do not affect the thermal management policies of the chassis.

See the following procedures:

- “Deleting an alarm” on page 6-35
- “Acknowledging an alarm” on page 6-36
- “Enabling and disabling visible alarm output by severity” on page 6-37
- “Configuring alarm attributes” on page 6-38
- “Displaying alarms” on page 6-40
- “Clearing alarm history” on page 6-46

Alarm classes

An alarm can be classified into equipment, facility or environmental. There can be more than one active alarm in each class. Alarm configuration information applies across the 39XX/51XX Switches and Platforms. All configuration information applies to the class as a whole it is not possible to have different configuration settings for different potential instances of an alarm class.

Each class of alarm may be enabled. Enabling an alarm after the event has occurred will not result in an alarm. Alarms may have a default state of enabled. Commands are available to change this state, however, alarms may not be disabled.

Due to the alarm system construction, some alarm classes may not apply to some specific hardware units. For example, there may be a fan alarm class on a unit that does not have a fan. This alarm would never go active.

Alarm instances

Each class of alarm can have one or more instances, depending on the nature of the alarm. For example, a Fan Failed (per fan) alarm could exist for every port in the system. There can, however, only be one multiple fans failed alarm. A single event can trigger more than one alarm. For example, a Fan Failed event can cause a Fan Failed alarm, and potentially a Multiple Fan Failed alarm.

Alarm severity levels

All alarms are defined with a severity level. While an alarm class has a level of severity, each alarm instance also has its own severity depending on the circumstances and the severity escalation policy of the alarm class.

Copyright© 2022 Ciena® Corporation

Table 6-1 lists alarm severity levels and provides definitions.

Table 6-1
Alarm severity levels

Alarm severity level	Definition
Critical	indicates a service-affecting condition has failed and an immediate corrective action is required, for example, a managed object is completely out-of-service and capability must be immediately restored.
Major	indicates a service-affecting condition has developed and an urgent corrective action is required, for example, a server degradation condition has occurred and must be immediately corrected.
Minor	indicates a non-service-affecting condition has developed and corrective action is required, for example, a server degradation condition exists, but is not currently degrading the server capacity.
Warning	indicates the detection of a potential or impending service-affecting condition before any significant effects have occurred. Closer examination is required to reduce the potential for the alarm escalating to a higher level.
Cleared	indicates the alarm has been disabled.

See “Enabling and disabling visible alarm output by severity” on page 6-37.

Types of alarms

The Alarm Manager monitors various types of events and generates the corresponding alarms. The alarms vary in their complexity. Alarms such as a redundant power supply going up or down are straightforward. Other alarms may require escalating, such as a fan state or chassis temperature. Alarms, such as Check Security Log require rate information.

Occurrences

You can have an occurrence threshold or an occurrence cap. An occurrence threshold prevents the setting of an alarm until a certain number of triggering events have occurred for that instance. The default threshold of 1 would be a basic alarm. An example of an occurrence threshold is the multiple fan failure alarm which has a threshold of two, which is the adjustable number of failed fans required to set an alarm.

An occurrence cap is a defined limit to the number of set events per instance that will be counted. A cap is used where multiple set events might occur in the system, yet a single clear event is expected to cancel the alarm.

Copyright© 2022 Ciena® Corporation

Timers

Most timers are in the seconds to minutes range. Specific timers can limit their ranges. The user interface method can accommodate a mixed use of common units of time ranging from seconds to years. If no units are specified, seconds are assumed.

The form of a timer is “10m6s”, where the letters used for units are y for years, M for months, w for weeks, d for days, h for hours, m for minutes, and s for seconds. No attempt is made to account for the variability (in seconds) of months or years. Range checking does not occur when timer values are input. Values such as 70m90s or 30s71m are acceptable, and have the same effect as the canonical form of 1h11m30s. The canonical form is used for time value output.

The timer values are configurable from the CLI and the MIB interfaces with one-second granularity and a range of potentially years, the common internal time stamp format of a 32-bit second counter.

The Alarm Manger runs a timer for each active alarm that needs to be monitored for severity. The severity levels transition from Warning to Minor, Minor to Major, or Major to Critical. The Alarm Manager also runs a timer for each rate threshold event.

Escalating severity

An alarm can escalate depending on its severity and how long the alarm condition has existed. Timed escalation progresses from severity to severity. The configuration does not permit skipping a severity level, such as Minor to Critical.

Alarms are escalated via the Alarm Manager. A timer is started when the event is received and the alarm is configured for escalation. The alarm is escalated if the Alarm Manager does not received a “clearing” event before the timer expires. An escalated alarm also has a threshold time. When the escalated alarm is received, the timer is restarted with the new time threshold. If the “clearing” event is not received, the alarm is regenerated with the escalated severity. This process continues until the alarm is at its highest defined severity. It remains at this severity until it is cleared. This de-escalation sequence is not visible to the operator.

If an alarm re-asserts before the severity has been de-escalated back to normal, it will set at the current elevated level, and will resume its escalation cycle with a fresh timer. This alarm becomes inactive when its clearing event is received. The alarm goes away after it uses its de-escalation timer to move back to its original condition.

Copyright© 2022 Ciena® Corporation

Escalated alarms are essentially new alarms. The escalated alarm gets a new sequence number assigned to it, and a clear/set pair is placed into the Alarm History.

Escalating severity with count

An alarm can escalate depending upon how many duplicate (per-instance) alarm setting events are received. This functionality is similar to occurrence thresholds where separate thresholds are specified for each level of severity over the base level.

Severities may be skipped by specifying the same threshold for multiple severities. In this case, the most severe level will be used at that threshold.

Rate threshold

A rate threshold prevents an alarm setting until a certain number of events have occurred within a period of time. A check security log alarm occurs when a rate threshold is exceeded. An event is generated each time something is logged into the security log.

Thresholds with escalating severity

Escalating severities may be used with occurrence or rate alarms. Count and Time escalation cannot be mixed.

Alarm tables

The 39XX/51XX Switches and Platforms has the following alarm tables: active alarm table, alarm history table, and alarm indication table.

Active alarm table

An active alarm table contains all active alarms and selected inactive alarms. When a set event occurs, a corresponding alarm is added to the active alarm table if it is not there already. If the alarm is in the table, its count is incremented unless it has reached its cap value. Visual indications are then set if appropriate, and enabled if the severity is greater than or equal to minor.

Each alarm has a category and instance associated with it which gives details of the alarm. A new unique sequence ID is assigned to each alarm entry when it is added to the active alarm table. Sequencing is restarted at one if there are no active alarms for one minute. If required, sequence numbers can wrap around numerically, though no duplicate numbers can exist concurrently. The Alarm Manager always assigns the next sequence ID even though there might be some previous sequence ID available in the free sequence ID list. The progression of sequence numbers is preserved until it resets due to idleness. When an alarm's severity changes due to escalation or de-escalation, a new sequence ID is assigned.

Copyright© 2022 Ciena® Corporation

Inactive alarms are not visible to the operator. Their presence only affects the observed behavior when or if they become active due to an event.

Table 6-2 lists the fields in the active alarm table.

Table 6-2
Active alarm table fields.

Field	Description
Sequence ID	is the unique ID/index assigned to an alarm entry when an alarm is added to the table or its severity changes.
Instance	is the instance this alarm is triggered for. The Instance includes Port ID, VS ID and slot ID. The instance distinguishes one alarm of a given class from another. It is supplied with the triggering event(s), and used to distinguish one alarm source from another.
Severity	is the alarm's current severity. Severity may transition from Warning ->, Minor -> Major, or Major -> Critical if the alarm has escalation timers.
Time Stamp	is the time the alarm is set in the system. The time stamp is internally recorded in the GMT/UTC time zones. It can be displayed in either GMT/UTC or local time zones.
Acknowledged	is the acknowledgment of the alarm if you want to cancel visual alarms that result from the alarm, The CLI and MIB interfaces also control whether visual alarms should be enabled or disabled globally. By default, they are enabled.
Alarm Description	is a detailed description of the alarm.

Copyright© 2022 Ciena® Corporation

Alarm history table

The Alarm Manager keeps a log of all alarm activity, system-originated or user-originated, in the Alarm History Table. Once the table is at 1250 entries, the Alarm Manager removes the oldest entries in order to make room for new entries.

When an alarm's severity changes it is logged with its own index value as a new history table item. This index number is not related to the index of the alarm in the active alarms table.

Configuration changes, acknowledgment or deletion of alarm instances are logged in the alarm history table.

Note: Alarm log records cannot be manually changed.

Table 6-3 lists the fields in the alarm history table.

Table 6-3
Alarm history table fields

Field	Description
Index	is the unique ID/index assigned to an alarm entry when an alarm is added to the table or its severity changes.
Instance	is the instance this alarm is triggered for. The Instance includes Port ID, VS ID and slot ID. The instance field is not defined or interpreted by the Alarm Manager. It is supplied with the triggering event(s), and used to distinguish one alarm source from another.
Severity	is the alarm's current severity.
Date and Time	is the date and time the alarm was added to the table.
Event Description	is a detailed description of the alarm.

Alarm indication table

The alarm indication table contains the name of the alarm, and whether the indicator is on or disabled. It is unusual for an alarm to be disabled.

Alarm records

Alarm records contain information about the probable causes of an alarm. Table 6-4 lists the fields in the alarm record table.

Copyright© 2022 Ciena® Corporation

Table 6-4
Alarm record table fields

Field	Description
Invoke Identifier	specifies the identifier assigned to the notification, for example, the sequential number of the notification. Each notification (state change, attribute change, object creation/deleting, or alarm of a network element) uses a unique invoke identifier. Network management may use an invoke identifier to request retrieval or synchronization.
Managed Object Class	specifies the class of the managed object in which the event occurred, for example, port.
Managed Object Instance	specifies the instance of the managed object in which the event occurred, for example, port 3/2.
Mode	specifies the mode requested in the operation. The values are confirmed or non-confirmed.
Event Type	specifies the type of event being reported. For general notification purposes, event types can be managed object instance creation or deletion notification, attribute change notification, and state change notification. For alarm notification purposes, the event types include communication alarm, quality of service alarm, processing error alarm, equipment alarm and environment alarm.
Event Time	specifies the time the event was generated.
Event Information	contains information on a detailed list of attributes that includes probable cause and specific problem.

Copyright© 2022 Ciena® Corporation

Field	Description
Probable Cause	contains further information as to the probable cause of the alarm.
Perceived Severity	consists of five security levels which provide an indication of how the managed object has been affected. The perceived severity levels are • Cleared - indicates the clearing of one or more previously reported alarms. • Critical - indicates that a service affecting condition has occurred and an immediate corrective state is required. • Major - indicates that a service-affecting condition has developed and an urgent corrective action is required. • Minor - indicates the existence of a non-service affecting fault condition, and that action should be taken to prevent a more serious fault.
Warning	indicates the detection of a potential or impending service-affecting fault before any significant effects have been felt. Action is required to further diagnose and correct the problem to prevent it from becoming a more serious service-affecting fault.

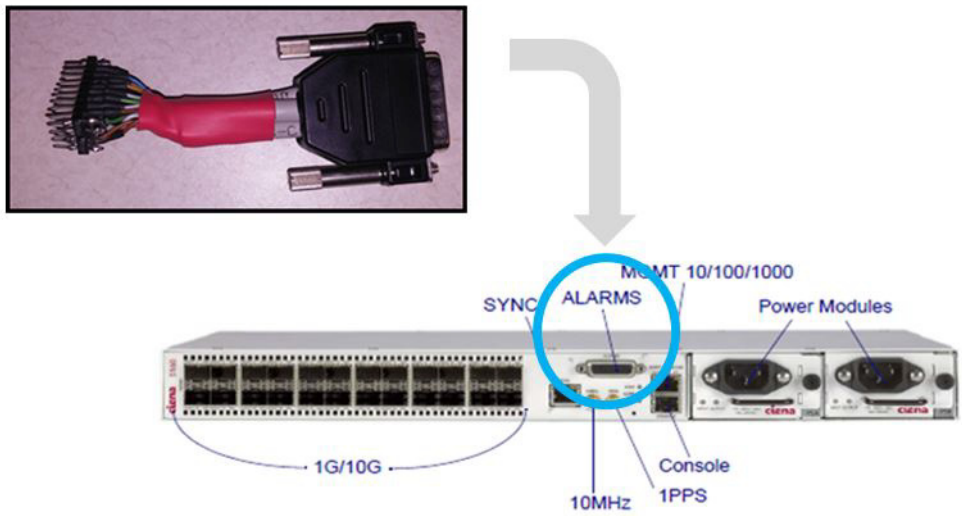
External alarms

Some Service Delivery Switch (SDS) devices have a port that accepts multiple external inputs that can be used to trigger internal alarms to report external events, as shown in Figure 6-1.

Note: Figure 6-1 shows a sample connector. Any other suitable connector works the same way.

Copyright© 2022 Ciena® Corporation

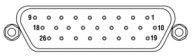
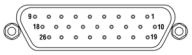
Figure 6-1
External alarm trigger



An operator could, for example, connect an opened door sensor to one of the external inputs of the switch to allow it to report the opening of the casing shelf.

Table 6-5 summarizes the number of alarm inputs available to monitor the status of various external sources such as door and temperature sensors. It also indicates the connectors to use.

Table 6-5
Alarm input summary

Platform	Number of inputs	Connector to use
5142	16	DB26 
5160	16	DB26 

See the following hardware and installation documents for an explanation of the port pin mapping:

- *5142 Hardware Installation and Start-up Manual (009-3206-001)*
- *5160 Hardware Installation and Start-up Manual (009-3207-001)*

The Alarm Manager allows the operator to define the significance and behavior of these alarms. External alarms can indicate minor, major, critical, and less warning severities.

Copyright© 2022 Ciena® Corporation

Use the CLI to view the following:

- pre-defined alarms
- active alarms
- history information for external alarms
- alarm status and statistics information

Each instance is basically a software abstraction managing the source of an external alarm, such as a door sensor.

You can also

- enable or disable the external alarms from the CLI
- assign descriptive labels to the external alarms depending on the type of external source hard-wired to the inputs on the alarm port
- trigger the alarm by an open or closed hardware contact
- trigger the alarm on demand
- escalate the severity of the alarm using the CLI

When an external alarm is triggered, for example, a chassis door opens, the Alarm Manager outputs a system event which may be configured to send an SNMP trap. The Alarm Statistics table is updated with an increment to the corresponding severity count. The rate threshold and other advanced functionality was not intended to be supported for the external class of alarms.

The polarity of an external alarm input is configurable. This means that, depending on the configured sense setting, an open hardware contact can activate the trigger for an external alarm. This is in contrast to the default behavior whereby a closed hardware contact triggers an alarm.

The Alarm Manager's ability to handle external alarm inputs of certain SAOS SDS devices lets you make use of functionality similar to what is supported for other existing alarm classes managed by the Alarm Manager interface.

See these procedures;

- "Configuring alarm attributes" on page 6-38
- "Displaying alarms" on page 6-40

Copyright© 2022 Ciena® Corporation

Alarm differences

Service Delivery, Aggregation and Virtualization platforms support a single front panel alarm LED. This LED is turned on (solid yellow) when there is at least one non-acknowledged active alarm in the system, regardless of its severity. These platforms support a limited set of alarms including the following:

- High/low temperature threshold violations
- POST errors
- Power supply faults
- Fan failures

Users can acknowledge the alarm through the Alarm Manager, and turn off the LED. The LED is turned off when there are no unacknowledged active alarms in the system.

Alarm instances

If the alarm system generates an alarm, it indicates that the alarm system has found something that the operator should correct. Table 6-6 describes the choices the operator has.

Table 6-6
Alarm instances

Action	Description
Correct the underlying problem	If corrected, the alarm goes away by itself. No further action is required to turn off the alarm indications.
Defer the problem	You can defer the problem when you recognize there is a problem, but it cannot be corrected immediately. The alarm indications are suppressed, but the alarm remains available in the active alarm report. This is accomplished by acknowledging the alarm instance.
Ignore the problem	You can ignore the alarm when you have determined that it is not a problem, or is never going to be addressed. The alarm indications are extinguished, and the alarm will not appear in the active alarm report. This is accomplished by deleting the alarm instance.

Copyright© 2022 Ciena® Corporation

Alarms and corresponding events

Table 6-7 outlines the alarms and their corresponding events.

Table 6-7
Alarms and events

Alarm	Event(s) to Raise	Events(s) to Clear	Alarm Type	Alarm Cause
General Health Alarms				
Overtemperature	ChassisEvent_ HighTemperatureThreshold Exceeded	ChassisEvent_ TemperatureNormal	Environment	Cooling Fan Failure
Undertemperature	ChassisEvent_ LowTemperatureThreshold Exceeded	ChassisEvent_ TemperatureNormal	Environment	Low Temperature
Fan Failure	ChassisEvent_ SingleFanFailed	ChassisEvent_ FanSpeedNormalRange	Environment	Cooling Fan Failure
Multiple Fan Failure	ChassisEvent_ SingleFanFailed (multiple)	ChassisEvent_ FanSpeedNormalRange	Environment	Cooling Fan Failure
Blade Post Errors Detected	BladeEvent_ PostErrorsDetected	BladeEvent_ PostErrorsCleared	Equipment	Linecard Problem
Port Post Errors Detected	PortEvent_ PostErrorsDetected	PortEvent_ PostErrorsCleared	Equipment	Linecard Problem
Module Init Failure	ChassisEvent_ ModulePostErrorsDetected	ChassisEvent_ ModulePostErrorsCleared	Equipment	Linecard Problem
Power Supply Failure	ChassisEvent_PowerStatus Failure	ChassisEvent_PowerStatu sFailureCleared	Equipment	Linecard Problem
Redundant Power Removed	ChassisEvent_ RedundantPowerRemove	ChassisEvent_ Redundant Power Inserted	Equipment	Replaceable Unit Missing
Invalid Chassis MAC	ChassisEvent_ InvalidChassisMac	ChassisEvent_ ValidChassisMac	Processing Error	Configuration Error
Unreachable Gateway	InterfaceEvent_ GatewayUnreachable	InterfaceEvent_ Gatewayreachable	Communications	LAN Error
CPU Overloaded	ChassisEvent_ MemoryUtilization	ChassisEvent_ MemoryUtilization	Processing Error	Out of CPU Cycles
Memory Low	ChassisEvent_ MemoryUtilization	ChassisEvent_ MemoryUtilization	Processing Error	Out of Memory
Virtual Memory Low	ChassisEvent_Virtual MemoryUtilization	ChassisEvent_Virtual MemoryUtilization	Processing Error	Out of Virtual Memory
Mount Status Read Only	ChassisEvent_FileSystem SysfsMountStatus	ChassisEvent_FileSystem SysfsMountStatus	Processing Error	Mount Status Read Only
Disk Full	ChassisEvent_ FileSystemTmpUtilization, ChassisEvent_FileSystemS ysfsUtilization, ChassisEvent_FileSystemX tpUtilization	ChassisEvent_FileSystem TmpUtilization, ChassisEvent_FileSystem SysfsUtilization, ChassisEvent_FileSystem XftpUtilization	Processing Error	Resource At/ Near Capacity

Copyright© 2022 Ciena® Corporation

Table 6-7
Alarms and events

Alarm	Event(s) to Raise	Events(s) to Clear	Alarm Type	Alarm Cause
Temp. Sens. Fail	ChassisEvent_TemperatureSensorFailure	ChassisEvent_TemperatureSensorRecovered	Environment	Equipment Malfunction
FRU Failure	TdmEvent_FruFailure	TdmEvent_FruFailureCleared	Equipment	Replaceable Unit Problem
FRU type mismatch	ChassisEvent_FruTypeMismatch	ChassisEvent_FruTypeMismatchCleared	Equipment	Replaceable Unit Type Mismatch
Port Alarms				
Port Link Down	PortEvent_StateChange	PortEvent_StateChange PortEvent_AdminStateChange	Communications	Connection Establishment Error
Port Flapping	PortEvent_StateChange	PortEvent_StateChange	Processor Error	Communications Protocol Error
Port Loopback	PortEvent_ PortSetPhyLoopback	PortEvent_PortSetPhyLoopback	Communications	Communications Protocol Error
Link Failure	TdmEvent_LinkErrors Detected	TdmEvent_LinkErrors Cleared	Equipment	Transmission Error
Data Path Failure	TdmEvent_DataPathErrors Detected	TdmEvent_DataPathErrors Cleared	Equipment	Transmission Error
Port Signal Degraded	PortEvent_SignalDegraded StateChangeSet	PortEvent_SignalDegradedStateChangeClear	Communications	Degraded Signal X733
TDM Port Failure	TdmEvent_TdmPortFailure	TdmEvent_TdmPortFailure Cleared	Equipment	Transceiver Failure
Link Failure	TdmEvent_TdmPortLink ErrorsDetected	TdmEvent_TdmPortLinkErrorsCleared	Equipment	Transmission Error
XCVR Alarms				
XCVR Caps Mismatch	PortEvent_ AdminXcvrIncompatible	PortEvent_AdminXcvrCompatible	Equipment	Replaceable Unit Type Mismatch
XCVR Overtemperature	XcvrEvent_TempHighAlarm, XcvrEvent_TempHighWarning	XcvrEvent_ TempHighAlarmClear	Environment	Cooling Fan Failure
XCVR Undertemperature	XcvrEventTempLowAlarm, XcvrEvent_TempLowWarning	XcvrEvent_ TempHighAlarmClear	Environment	Low Temperature
XCVR Rx Power High	XcvrEvent_ RxPowerHighAlarm, XcvrEvent_ RxPowerHighWarning	XcrEvent_ RxPowerHighAlarmClear	Equipment	Signal Quality Evaluation Failure

Copyright© 2022 Ciena® Corporation

Table 6-7
Alarms and events

Alarm	Event(s) to Raise	Events(s) to Clear	Alarm Type	Alarm Cause
XCVR Rx Power Low	XcvrEvent_ RxPowerLowAlarm, XcrEvent_RxPowerLowWarning	XcvrEvent_ RxPowerHighAlarmClear	Equipment	Signal Quality Evaluation Failure
XCVR_Tx Power High	XcvrEvent_ TxPowerHighAlarm, XcvrEvent_TxPowerHighWarning	XcvrEvent_ TxPowerHighAlarmClear	Equipment	Signal Quality Evaluation Failure
XCVR Tx Power Low	XcvrEvent_TxPowerLowAlarm, XcvrEvent_TxPowerLowWarning	XcvrEvent_ TxPowerHighAlarmClear	Equipment	Signal Quality Evaluation Failure
XCVR Missing	xcvrEvent_XcvrMissing	XcvrEvent_XcvrPresent	Equipment	Replaceable Unit Missing
XCVR Failed	xcrEvent_XcvrFailed	XcvrEvent_XcvrHealthy	Equipment	Transceiver Failure
Transceiver Failure	TdmEvent_XcvrFailure	TdmEvent_XcvrFailureCleared	Equipment	Transceiver Failure
Miscellaneous System Alarms				
NTP Out of Sync	NtpcEvent_NtpSyncChangeNotification	NtpcEvent_ NtpSyncChangeNotification	QoS	Loss of Sync
Check Security Log	LoggingEvent_SecLogEntry	Logging Event_secLogEntry	Communication	Intrusion Detection
Lin Prot Switch Active	LapsEvent_SwitchTo Protection	LapsEvent_SwitchTo Working, LapsEvent_Protection GroupDelete	Communications	Communications Protocol Error
Lin Prot Grp Failure	LapsEvent_Protection GroupFailure	LapsEvent_Protection GroupFailureClear, LapsEvent_Protection GroupDelete	Communications	Communications Protocol Error
Lin Prot Arch Mismatch	LapsEvent_Architecture Mismatch	LapsEvent_Architecture MismatchClear,LapsEvent_ProtectionGroupDelete	Communications	Communications Protocol Error
G.8032 Alarms				
Protection Switch Active	RapsEvent_ ProtectionSwitchActive	RapsEvent_ProtectionSwitchCleared	Communications	Communications Protocol Error
No PDU Received	RapsEvent_NoPduReceived	RapsEvent_NoPduReceivedCleared	Communications	Communications Protocol Error

Copyright© 2022 Ciena® Corporation

Table 6-7
Alarms and events

Alarm	Event(s) to Raise	Events(s) to Clear	Alarm Type	Alarm Cause
Provisioning Mismatch	RapsEvent_ProvisioningMismatch	RapsEvent_ProvisioningMismatchCleared	Communications	Communications Protocol Error
No RPL Owner Detected	RapsEvent_ NoRplOwner	RapsEvent_NoRplOwnerCleared	Communications	Communications Protocol Error
TDM Alarms				
Link Errors Detected	TdmEvent_ LinkErrorsDetected	TdmEvent_ LinkErrorsCleared	Equipment	Transmission Error
Data Path Errors Detected	TdmEvent_ DataPathErrorsDetected	TdmEvent_ DataPathErrorsCleared	Equipment	Transmission Error
Linear MSP 1+1 APS Group Alarms				
Lin Prot Switch Active (raised only when operation type is revertive)	SwitchToProtection	SwitchToWorking	Equipment	Transmission Error
Lin Prot Grp Failure	ProtectionGroupFailure	ProtectionGroupFailureClear	Equipment	Transmission Error
Lin Prot Arch Mismatch	Architecture Mismatch	Architecture Mismatch Clear	Equipment	Transmission Error
Chassis External Alarms				
External Alarm 1	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 2	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 3	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 4	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 5	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 6	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 7	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 8	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 9	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 10	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other

Copyright© 2022 Ciena® Corporation

Table 6-7
Alarms and events

Alarm	Event(s) to Raise	Events(s) to Clear	Alarm Type	Alarm Cause
External Alarm 11	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 12	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 13	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 14	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 15	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other
External Alarm 16	ChassisEvent_ ExternalAlarmRaised	ChassisEvent_ ExternalAlarmCleared	Equipment	Other

Copyright© 2022 Ciena® Corporation

World Wide Packet traps and corresponding events

Table 6-8 describes World Wide Packet (WWP) traps and their corresponding events.

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
WWP-EXT-BRIDGE-TRAP-MIB		
wwpLinkUp	Not supported	No
wwpLinkDown	Not supported	No
WWP-LEOS-8021X-MIB		
wwpLeos8021xAuthAuthenticationEvent	Dot1xEvent_Dot1xPortAuthEapResult	Yes
wwpLeos8021xAuthConfigChangeEvent	Dot1xEvent_Dot1xPortAuthControlSet Dot1xEvent_Dot1xPortAuthEapolVersionSet Dot1xEvent_Dot1xPortAuthMaxReqSet Dot1xEvent_Dot1xPortAuthQuietPeriodSet Dot1xEvent_Dot1xPortAuthReauthPeriodSet Dot1xEvent_Dot1xPortAuthReauthSet Dot1xEvent_Dot1xPortAuthServerTimeoutSet Dot1xEvent_Dot1xPortAuthSuppTimeoutSet Dot1xEvent_Dot1xPaePortControlSet Dot1xEvent_Dot1xPortAuthTxPeriodSet Dot1xEvent_Dot1xPortAuthKeyTxEnableSet	Yes
wwpLeos8021xGlobalStateChangeEvent	Dot1xEvent_Dot1xDisable Dot1xEvent_Dot1xEnable	Yes
wwpLeos8021xSuppAuthenticationEvent	Dot1xEvent_Dot1xPortSuppEapResult	Yes
wwpLeos8021xSuppConfigChangeEvent	Dot1xEvent_Dot1xPortSuppAuthPeriodSet Dot1xEvent_Dot1xPortSuppCheckCertTimeSet Dot1xEvent_Dot1xPortSuppMaxStartSet Dot1xEvent_Dot1xPortSuppPasswordSet Dot1xEvent_Dot1xPortSuppMutualAuthenticationSet Dot1xEvent_Dot1xPortSuppUserNameSet Dot1xEvent_Dot1xPortSuppHeldPeriodSet Dot1xEvent_Dot1xPortSuppEapMethodSet Dot1xEvent_Dot1xPortSuppEapolVersionSet Dot1xEvent_Dot1xPortSuppStartPeriodSet Dot1xEvent_Dot1xPortSuppControlSet	Yes
WWP-LEOS-BENCHMARK-MIB		
wwpLeosBenchmarkProfileTestCompleted	BenchmarkEvent_ProfileTestCompleted	Yes
wwpLeosBenchmarkProfileTestFailedFramelossKpi	BenchmarkEvent_ProfileTestFailedFramelossKpi	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosBenchmarkProfileTestFailedLatencyKpi	BenchmarkEvent_ProfileTestFailedLatencyKpi	Yes
wwpLeosBenchmarkProfileTestFailedPdvKPI	BenchmarkEvent_ProfileTestFailedPdvKpi	Yes
wwpLeosBenchmarkProfileTestFailedThoughputKpi	BenchmarkEvent_ProfileTestFailedThroughputKpi	Yes
wwpLeosBenchmarkProfileTestStarted	BenchmarkEvent_ProfileTestStarted	Yes
wwpLeosBenchmarkProfileTestStopped	BenchmarkEvent_ProfileTestStoppedByUser	Yes
WWP-LEOS-BLADE-MIB		
wwpLeosBladeStateChange	BladeOperState_Unequipped BladeOperState_Disabled BladeOperState_Enabled BladeOperState_Faulted BladeOperState_Init	Yes
WWP-LEOS-BROADCAST-CONTAINMENT-MIB		
wwpLeosBcastThresholdExceed	BcastContainmentEvent_BcastPktStartDrop	Yes
wwpLeosBcastThresholdNormal	BcastContainmentEvent_BcastPktStartDrop BcastContainmentEvent_BcastPktStopDrop	Yes
WWP-LEOS-CFM-MIB		
wwpLeosCfmBlockOppositeMEPSetTrap	CfmEvent_CfmMepBofSet	Yes
wwpLeosCfmBlockOppositeMEPClearTrap	CfmEvent_CfmMepBofClear	Yes
wwpLeosCfmExtDelaySessionAvgDelayFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionAvgDelayFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionMaxDelayFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionMaxDelayFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionAvgJitterFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionAvgJitterFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionMaxJitterFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtDelaySessionMaxJitterFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtFaultTrapSet	CfmEvent_CfmServiceFaultSet	Yes
wwpLeosCfmExtFaultTrapClear	CfmEvent_CfmServiceFaultClear	Yes
wwpLeosCfmExtFrameLossSessionFrameLossFarFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtFrameLossSessionFrameLossFarFaultClearTrap	CfmEvent_CfmTestFault	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosCfmExtFrameLossSessionFrameLossNearFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtFrameLossSessionFrameLossNearFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtSynLossSessionFrameLossFarFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtSynLossSessionFrameLossFarFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtSynLossSessionFrameLossNearFaultSetTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmExtSynLossSessionFrameLossNearFaultClearTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmFaultTrap	CfmEvent_CfmServiceFault	Yes
wwpLeosCfmFrameLossSessionBadSequenceTrap	CfmEvent_CfmTestFault	Yes
wwpLeosCfmPbtFaultTrap	CfmEvent_CfmPbtServiceFault	Yes
WWP-LEOS-CHASSIS-MIB		
wwpLeosChassisPowerSupplyStatusNotification	ChassisEvent_PowerStatusFailure ChassisEvent_PowerStatusOffline ChassisEvent_PowerStatusOnline	Yes
wwpLeosChassisFanModuleNotification	ChassisEvent_MinFanSpeedThresholdExceeded ChassisEvent_SingleFanFailed ChassisEvent_FanSpeedNormalRange	Yes
wwpLeosChassisTempNotification	ChassisEvent_HighTemperatureThresholdExceeded ChassisEvent_LowTemperatureThresholdExceeded ChassisEvent_TemperatureNormal	Yes
wwpLeosChassisBatteryStatusNotification	ChassisEvent_NoBatteryDetected ChassisEvent_BatteryDetected	Yes
wwpLeosChassisBatteryVoltageLevelNotification	ChassisEvent_LowBatteryThresholdExceeded	Yes
wwpLeosChassisBatteryConditionNotification	ChassisEvent_BadBattery	Yes
wwpLeosChassisPowerSourceNotification	ChassisEvent_PowerTransitionToBattery ChassisEvent_PowerTransitionToAc	Yes
wwpLeosChassisPostErrorNotification		Yes
wwpLeosChassisRebootNotification	ChassisEvent_SystemReboot	Yes
wwpLeosChassisSnmpStateNotification	SnmpEvent_AgentAdminSet	Yes
wwpLeosChassisDoorStatusChangeNotification		Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosChassisInnerDoorStatusChangeNotification	EventEvent_DoorStatusChange:	Yes
wwpLeosChassisOuterDoorStatusChangeNotification	EventEvent_DoorStatusChange:	Yes
wwpLeosChassisExternalAlarmStatusChangeNotification	AlarmEvent_ExternalAlarmStatusChange	Yes
wwpLeosChassisDoorAlarmStatusChangeNotification	ChassisEvent_DoorAlarmStatus	Yes
WWP-LEOS-DHCP-CLIENT-MIB		
wwpLeosDhcpClientOptionDisabledNotification	DhcpEvent_InvalidOptionReceived	Yes
WWP-LEOS-EXT-LAG-MIB		
wwpLeosExtLagMclagStateChange	LacpEvent_McLagState	Yes
WWP-LEOS-FEATURE-LICENSE-MIB		
wwpLeosPremiumFeatureLicenseStatusNotification	SwXGradeEvent_FeatureLicenseStatusChanged SwXGradeEvent_PartialLicenseDetected SwXGradeEvent_UnlicensedFeatureConfig	Yes
wwpLeosPremiumFeatureLicenseInstallErrorNotification	SwXGradeEvent_LicenseKeyError	Yes
WWP-LEOS-FILE-TRANSFER-MIB	**The MIB module for the WWP TFTP Operation to download a file**.	
wwpLeosFTransferCompletion	DnldEvent_TransferComplete	Yes
WWP-LEOS-FLOW-MIB	**MIB module for the WWP FLOW specific information.**	Yes
wwpLeosFlowServiceLevelPortOverProvisionedTrap	FlowEvent_FlowPortCirBwExceeded	Yes
wwpLeosFlowServiceLevelPortUnderProvisionedTrap	FlowEvent_FlowPortCirBwNoLongerExceeded	Yes
wwpLeosFlowL2SacHighThreshold	FlowEvent_SACLimitReached	Yes
wwpLeosFlowL2SacNormalThreshold	FlowEvent_SACLimitNotReached	Yes
WWP-LEOS-INFORM-STATUS-MIB	**This MIB module defines managed objects for Reliable Trap Feature on WWP devices.**	
wwpLeosInformDiscardNotification	Not applicable	No
wwpLeosInetTargetInformDiscardNotification	Not supported	No
WWP-LEOS-IP-INTERFACE-MIB	The MIB module for the WWP IpInterface IP interfaces configuration. This MIB provides additional configuration to that provided by the standard IP group.	
wwpLeosIpInterfaceAddrChgNotification	InterfaceEvent_InterfaceIpAdd InterfaceEvent_InterfaceIpRemove	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosIpInterfaceOperationalGatewayChgNotification	InterfaceEvent_InterfaceGatewayDhcpSet InterfaceEvent_InterfaceGatewaySet InterfaceEvent_InterfaceGatewayAdd	Yes
wwpLeosIpInterfaceIPv6AddrAddedNotification	InterfaceEvent_InterfaceIpAdd	Yes
wwpLeosIpInterfaceIPv6AddrRemovedNotification	InterfaceEvent_InterfaceIpRemove	Yes
WWP-LEOS-MSTP-MIB	**The MIB module for the WWP MstpMib specific information.**	
wwpLeosMstpNewRootNotification	MstpEvent_BridgeIsNewRootXst	Yes
wwpLeosMstpTopologyChangeNotification	MstpEvent_TopologyChangeXst	Yes
wwpLeosMstpPortBackupNotification	MstpEvent_BackUpPortRole	Yes
wwpLeosMstpSelfLoopNotification	MstpEvent_LoopBackPortDetected	Yes
wwpLeosMstpPortOperEdgeNotification	MstpEvent_PortOperEdgePortChange	Yes
wwpLeosMstpPortFlapNotification	MstpEvent_BridgePortFlapping	Yes
wwpLeosMstpBridgeRootPortLostNotification	MstpEvent_BridgeXstRootPortLost	Yes
wwpLeosMstpPvstBpduReceiveNotification	MstpEvent_PortRcvdCiscoPvstBpdu	Yes
WWP-LEOS-NTP-CLIENT-MIB		Yes
wwpLeosNtpClientSyncStatusChangeNotification	NtpcEvent_NtpSyncChangeNotification	Yes
WWP-LEOS-OAM-MIB		
wwpLeosOamLinkEventTrap	OamEvent_OamLinkEventLogged	Yes
WWP-LEOS-PORT-MIB		
wwpLeosEthLinkUp	PortEvent_StateChange	Yes
wwpLeosEthLinkDown	PortEvent_StateChange	Yes
wwpLeosEthAdminSpeedIncompatible	PortEvent_AdminXcvrIncompatible	Yes
wwpLeosEthLinkFlap	PortEvent_LinkFlapChange	Yes
wwpLeosAggLinkUpDown	PortEvent_StateChange	Yes
wwpLeosEthRxLowPowerDetect	PortEvent_RxLowPowerDetectChange	Yes
WWP-LEOS-PORT-XCVR-MIB		
wwpLeosPortXcvrLinkStateChangeNotification	XcvrEvent_XcvrDisabled XcvrEvent_XcvrEnabled XcvrEvent_OpticInserted XcvrEvent_OpticRemoved	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosPortXcvrErrorTypeNotification	XcvrEvent_EepromChecksumFailed XcvrEvent_EepromReadFailed	Yes
wwpLeosPortXcvrTempHighNotification	XcvrEvent_TempHighAlarm	Yes
wwpLeosPortXcvrTempLowNotification	XcvrEvent_TempLowAlarm	Yes
wwpLeosPortXcvrTempNormalNotification	XcvrEvent_TempHighAlarmClear XcvrEvent_TempHighWarningClear XcvrEvent_TempLowAlarmClear XcvrEvent_TempLowWarningClear	Yes
wwpLeosPortXcvrVoltageHighNotification	XcvrEvent_VccHighAlarm	Yes
wwpLeosPortXcvrVoltageLowNotification	XcvrEvent_VccLowAlarm	Yes
wwpLeosPortXcvrVoltageNormalNotification	XcvrEvent_VccHighAlarmClear XcvrEvent_VccHighWarningClear XcvrEvent_VccLowAlarmClear XcvrEvent_VccLowWarningClear	Yes
wwpLeosPortXcvrBiasHighNotification	XcvrEvent_BiasHighAlarm	Yes
wwpLeosPortXcvrBiasLowNotification	XcvrEvent_BiasLowAlarm	Yes
wwpLeosPortXcvrBiasNormalNotification	XcvrEvent_BiasHighAlarmClear XcvrEvent_BiasHighWarningClear XcvrEvent_BiasLowAlarmClear XcvrEvent_BiasLowWarningClear	Yes
wwpLeosPortXcvrTxPowerHighNotification	XcvrEvent_TxPowerHighAlarm	Yes
wwpLeosPortXcvrTxPowerLowNotification	XcvrEvent_TxPowerLowAlarm	Yes
wwpLeosPortXcvrTxPowerNormalNotification	XcvrEvent_TxPowerHighAlarmClear XcvrEvent_TxPowerHighWarningClear XcvrEvent_TxPowerLowAlarmClear XcvrEvent_TxPowerLowWarningClear	Yes
wwpLeosPortXcvrRxPowerHighNotification	XcvrEvent_RxPowerHighAlarm	Yes
wwpLeosPortXcvrRxPowerLowNotification	XcvrEvent_RxPowerLowAlarm	Yes
wwpLeosPortXcvrRxPowerNormalNotification	XcvrEvent_RxPowerHighAlarmClear XcvrEvent_RxPowerHighWarningClear XcvrEvent_RxPowerLowAlarmClear XcvrEvent_RxPowerLowWarningClear	Yes
wwpLeosPortXcvrSpeedInfoMissingNotification	XcvrEvent_XcvrSpeedInfoMissing	Yes
wwpLeosPortXcvrBiasHighWarningNotification	XcvrEvent_BiasHighWarning	Yes
wwpLeosPortXcvrBiasLowWarningNotification	XcvrEvent_BiasLowWarning	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosPortXcvrTempHighWarningNotification	XcvrEvent_TempHighWarning	Yes
wwpLeosPortXcvrTempLowWarningNotification	XcvrEvent_TempLowWarning	Yes
wwpLeosPortXcvrVoltageHighWarningNotification	XcvrEvent_VccHighAlarmWarning	Yes
wwpLeosPortXcvrVoltageLowWarningNotification	XcvrEvent_VccLowAlarmWarning	Yes
wwpLeosPortXcvrTxPowerHighWarningNotification	XcvrEvent_TxPowerHighWarning	Yes
wwpLeosPortXcvrTxPowerLowWarningNotification	XcvrEvent_TxPowerLowWarning	Yes
wwpLeosPortXcvrRxPowerHighWarningNotification	XcvrEvent_RxPowerHighWarning	Yes
wwpLeosPortXcvrRxPowerLowWarningNotification	XcvrEvent_RxPowerLowWarning	Yes
WWP-LEOS-RAPS-MIB		
wwpLeosRapsAlarm	RapsEvent_ProvisioningMismatch RapsEvent_ProtectionSwitchActive RapsEvent_FaultClear	Yes
WWP-LEOS-RSTP-MIB		
wwpLeosRstpPortBackupNotification	RstpEvent_BackUpPortRole	Yes
wwpLeosRstpSelfLoopNotification	RstpEvent_LoopBackPortDetected	Yes
wwpLeosRstpPortOperEdgeNotification	RstpEvent_PortOperEdgePortChange	Yes
wwpLeosRstpPortFlapNotification	RstpEvent_BridgePortFlapping	Yes
wwpLeosRstpBridgeRootPortLostNotification	RstpEvent_BridgeRootPortLost	Yes
wwpLeosRstpPvstBpduReceiveNotification	RstpEvent_PortRcvdCiscoPvstBpdu	Yes
WWP-LEOS-SW-XGRADE-MIB		
wwpLeosSwDownloadCompletion	SwXGradeEvent_Complete	Yes
wwpLeosSwXgradeOpCompletion	SwXGradeEvent_Complete	Yes
wwpLeosSwXgradeBladePkgIncorrect	BladeEvent_BladePkgVerIncorrect	Yes
wwpLeosSwXgradeCompletion	Not supported	No
WWP-LEOS-SYSTEM-CONFIG-MIB		
wwpLeosImproperCmdInConfigFile	ConfigEvent_ConfigFileError	
wwpLeosImproperCmdInConfigLineString	ConfigEvent_ConfigApplyCmdError	
wwpLeosSystemServiceModeChange	Not supported	No
wwpLeosSystemMemoryStatusNotification	ChassisEvent_SystemMemoryNormal ChassisEvent_SystemMemoryLowThresholdExceeded	Yes

Copyright© 2022 Ciena® Corporation

Table 6-8
WWP traps and corresponding events

Trap	Event	Enabled / disabled from CLI
wwpLeosSystemMemoryUtilizationStatusTrap	ChassisEvent_MemoryUtilization	Yes
wwpLeosSystemCpuUtilization5SecondStatusTrap	ChassisEvent_CpuUtilization5Seconds	Yes
wwpLeosSystemCpuUtilization10SecondStatusTrap	ChassisEvent_CpuUtilization10Seconds	Yes
wwpLeosSystemCpuUtilization60SecondStatusTrap	ChassisEvent_CpuUtilization60Seconds	Yes
wwpLeosSystemCpu1MinLoadStatusTrap	ChassisEvent_CpuLoadAverage1Minute	Yes
wwpLeosSystemCpu5MinLoadStatusTrap	ChassisEvent_CpuLoadAverage5Minutes	Yes
wwpLeosSystemCpu15MinLoadStatusTrap	ChassisEvent_CpuLoadAverage15Minutes	Yes
wwpLeosSystemFileSystemUtilizationTmpStatusTrap	ChassisEvent_FileSystemTmpUtilization	Yes
wwpLeosSystemFileSystemUtilizationSysfsStatusTrap	ChassisEvent_FileSystemSysfsUtilization	Yes
wwpLeosSystemFileSystemUtilizationXftpStatusTrap	ChassisEvent_FileSystemXftpUtilization	Yes
WWP-LEOS-TABLE-CHG-NOTIF-MIB		
wwpLeosTableChgTrap	Not supported	No
wwpLeosTableRefreshTrap	Not supported	No

Ciena traps and corresponding events

Table 6-9 lists the supported traps.

Table 6-9
Ciena traps and corresponding events

Traps	Events	CLI
CIENA-CES-ALARM-MIB		
No notifications defined		
CIENA-CES_BENCHMARK MIB		
cienaCesBenchmarkTestStarted	TestInstanceStarted	
cienaCesBenchmarkTestStopped	TestInstanceStoppedByUser TestInstanceStoppedDueToError	
cienaCesBenchmarkTestCompleted	TestInstanceCompleted	
cienaCesBenchmarkTestFailedThroughputKpi	TestInstanceFailedThroughputKpi	
cienaCesBenchmarkTestFailedFramelossKpi	TestInstanceFailedFramelossKpi	
cienaCesBenchmarkTestFailedLatencyKpi	TestInstanceFailedLatencyKpi	

Copyright© 2022 Ciena® Corporation

Table 6-9
Ciena traps and corresponding events

Traps	Events	CLI
cienaCesBenchmarkRestFailedPdvKpi	TestInstanceFailedPdvKpi	
cienaCesBenchmarkTestIterationCompleted	TestResultsIterationCompleted	
CIENA-CES-BFD-MIB		
cienaCesBfdSessionOperStateChangeTrap	BfdEvent_BfdSessionOperStateChange	Yes
CIENA-CES-CONFIG-MGMT-MIB		
cienaCesConfigSaveNotification	ConfigEvent_ConfigSave	Yes
cienaCesConfigChangeNotification	ConfigEvent_ConfigChanged	Yes
CIENA-CES-ICL-MIB		
cienaCesIclStateChange	LacpEvent_IclOperStateChange	Yes
CIENA-CES-MCAST-FILTER-MIB		
cienaCesMcastAddrOverlaopNotification	IgmpEvent_IgmpMcastEntryFound	Yes
CIENA-CES-MPLS-MIB		
cienaCesMplsTunnelOperStateChgTrap	MplsEvent_EncapTunlOperStateChange	Yes
cienaCesMplsEncapTunnelGrpActiveEncapTunnelChange	MplsEvent_TunlGrpActiveTunlChange	Yes
cienaCesMplsTransitTunnelOperStateChgTrap	MplsEvent_TransitTunlOperStateChange	Yes
cienaCesMplsAssociatedTunnelOperStateChgTrap	MplsEvent_AssociatedTunlOperStateChange	Yes
cienaCesGmplsEncapUnidirTunnelOperStateChgTrap	MplsEvent_EncapTunlOperStateChange	Yes
cienaCesGmplsEncapCoroutedTunnelOperStateChgTrap	MplsEvent_IngressTpCoroutedTunlAisFaultStateChange	Yes
cienaCesGmplsDecapCoroutedTunnelOperStateChgTrap	MplsEvent_DecapTunlOperStateChange	Yes
cienaCesGmplsTransitUnidirTunnelOperStateChgTrap	MplsEvent_TransitTunlOperStateChange	Yes
cienaCesGmplsTransitCoroutedTunnelOperStateChgTrap	MplsEvent_TransitTunlOperStateChange	Yes
cienaCesGmplsAssociatedTunnelOperStateChgTrap	MplsEvent_AssociatedTunlOperStateChange	Yes
cienaCesGmplsEncapUnidirTunnelGrpActiveEncapTunnelChangeTrap	MplsEvent_EncapTunlOperStateChange	Yes
cienaCesGmplsEncapCoroutedTunnelGrpActiveEncapTunnelChangeTrap	Not supported	No
cienaCesGmplsDecapCoroutedTunnelGrpActiveDecapTunnelChangeTrap	Not supported	No

Copyright© 2022 Ciena® Corporation

Table 6-9
Ciena traps and corresponding events

Traps	Events	CLI
cienaCesGmplsEncapCoroutedTunnelAisFaultStateChgTrap	MplsEvent_IngressTpCoroutedTunlAisFaultStateChange	Yes
cienaCesGmplsDecapCoroutedTunnelAisFaultStateChgTrap	MplsEvent_EgressTpCoroutedTunlAisFaultStateChange	Yes
cienaCesGmplsAssociatedTunnelAisFaultStateChgTrap	MplsEvent_AssocTpTunlAisFaultStateChange	Yes
cienaCesGmplsTunnelAisFaultErrorTrap	MplsEvent_TunlAisUnknownLabelError	Yes
cienaCesMplsPwDown	Not supported (PW-STD-MIB used instead)	No
cienaCesMplsPwUp	Not supported (PW-STD-MIB used instead)	No
cienaCesMplsPwBundleActivePwChange	Not supported (PW-STD-MIB used instead)	No
cienaCesMplsPwGroupSwitchOver	MplsEvent_PwGroupSwitchOver	Yes
cienaCesMplsPwSwitchoverToForwardingState	MplsEvent_VcStateSwitchover	Yes
cienaCesMplsPwSwitchoverToBlockingState	MplsEvent_VcStateSwitchover	Yes
CIENA-CES-PM-MIB		
No notifications defined		
CIENA-CES-TIME-SYNC-MIB		
cienaCesSyncInputPUStateChangeNotification	SyncEvent_SyncReferenceStateChange	Yes
cienaCesSyncInputProtectionGroupStateChangeNotification	SyncEvent_ProtectionGroupStateChange	Yes
CIENA-CES-VLLI-MIB		
cienaCesVlliFaultTrap	VlliEvent_vlliInstanceFault	Yes
cienaCesVlliRecoveryTrap	VlliEvent_vlliInstanceRecovery	Yes

Copyright© 2022 Ciena® Corporation

Standard traps and corresponding events.

Table 6-10 describes the standard traps and corresponding events.

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
ALARM-MIB		
alarmActiveState	Not supported	No
alarmClearState	Not supported	No
BRIDGE_MIB		
newRoot	RstpEvent_BridgeIsNewRoot	Yes
topologyChange	RstpEvent_PortStateUpdated	Yes
DIFFSERV-DSCP-TC		
No notifications defined		
DIFFSERV-MIB		
No notifications defined		
DS1-MIB		
ds1LineStatusChange	TdmEvent_TdmPortAlarmStateChange	Yes
DS3-MIB		
dsx3LineStatusChange	Not supported	No
ESO-CONSORTIUM-MIB		
No notifications defined		
ETHERLIKE-MIB		
No notifications defined		
ETHERLIKE-MIB		
No notifications defined		
HCNUM-TC		
No notifications defined		
HC-PerfHis-TC-MIB		
No notifications defined		
IANA-ADDRESS-FAMILY-NUMBERS-MIB		

Copyright© 2022 Ciena® Corporation

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
No notifications defined		
IANAifType-MIB		
No notifications defined		
IANA-PWE3-MIB		
No notifications defined		
IEEE8021-PAE-MIB		
No notifications defined		
IEEE8021-SECY-MIB		
No notifications defined		
IF-MIB		
linkDown	PortEvent_StateChange	Yes
linkup	PortEvent_StateChange TdmEvent_TdmPortOperStateChange	Yes
INET-ADDRESS-MIB		
No notifications defined		
INTERGRATED-SERVICES-MIB		
No notifications defined		
IP-MIB		
No notifications defined		
ISIS-MIB		
isisDatabaseOverload	Not supported	No
isisManualAddressDrops	Not supported	No
isisCorruptedLSPDetected	Not supported	No
isisAttemptToExceedMaxSequence	Not supported	No
isisIDLenMismatch	Not supported	No
isisMaxAreaAddressesMismatch	Not supported	No

Copyright© 2022 Ciena® Corporation

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
isisOwnLSPPurge	Not supported	No
isisSequenceNumberSkip	Not supported	No
isisAuthenticationTypeFailure	Not supported	No
isisAuthenticationFailure	Not supported	No
isisVersionSkew	Not supported	No
isisAreaMismatch	Not supported	No
isisRejectedAdjacency	Not supported	No
isisLSPTooLargeToPropagate	Not supported	No
isisOrigLSPBuffSizeMismatch	Not supported	No
isisProtocolsSupportedMismatch	Not supported	No
isisAdjacencyChange	Not supported	No
isisLSPErrorDetected	Not supported	No
ITU-ALARM-TC_MIB		
No notifications defined		
LLDP_DOT1-MIB		
No notifications defined		
LLDP_DOT3-MIB		
No notifications defined		
LLDP_DOT3-MIB		
No notifications defined		
LLDP-MIB		
LldpRemTablesChange	LldpEvent_RemTablesChange	Yes
MPLS-LDP-STD-MIB		
mplsLdpInitSessionThresholdExceeded	Not supported	No
mplsLdpPathVectorLimitMismatch	Not supported	No
mplsLdpSessionUp	Not supported	No

Copyright© 2022 Ciena® Corporation

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
mplsLdpSessionDown	Not supported	No
MPLS-LSR-STD-MIB		
mplsXCUp	Not supported	No
mplsXCDown	Not supported	No
MPLS-TC-STD-MIB		
No notifications defined		
MPLS-TE-STD-MIB		
No notifications defined		
OSPF-MIB		
No notifications defined		
P-BRIDGE-MIB		
No notifications defined		
PerfHist-TC-MIB		
No notifications defined		
PW-MPLS-STD-MIB		
No notifications defined		
OSPF-MIB		
No notifications defined		
P-BRIDGE-MIB		
No notifications defined		
PerfHist-TC-MIB		
No notifications defined		
PW-MPLS-STD-MIB		
No notifications defined		
PW-STD-MIB		
pwDown	MplsEvent_VcOperStateChange TdmEvent_TdmPwOperStateChange	Yes

Copyright© 2022 Ciena® Corporation

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
pwUp	MplsEvent_VcOperStateChange TdmEvent_TdmPwOperStateChange	Yes
pwDeleted	MplsEvent_VcDelete	Yes
PW-TC-STD-MIB		
No notifications defined		
Q-BRIDGE-MIB		
No notifications defined		
RFC1155-SMI		
No notifications defined		
Rfc1213.mib		
No notifications defined		
RFC1213-MIB		
No notifications defined		
rfc1215.mib		
No notifications defined		
RFC-1215		
No notifications defined		
RFC1215-TRAP		
No notifications defined		
RMON2-MIB		
Non notifications defined		
RMON-MIB.inc		
No notifications defined		
RMON-MIB		
risingAlarm	Not event based. Sent when RMON requests to send a rising alarm notification.	Yes
falling Alarm	Not event based. Sent when RMON requests to send a falling alarm notification.	Yes

Copyright© 2022 Ciena® Corporation

Table 6-10
Standard traps and corresponding events

Trap	Event(s)	CLI (Enable/ disable control
RSTP-MIB		
No notifications defined		
SNMP-COMMUNITY-MIB		
No notifications defined		
SNMP-FRAMEWORK-MIB		
No notifications defined		
SNMP-MPD-MIB		
No notifications defined		
SNMP-NOTIFICATIONS-MIB		
No notifications defined		
SNMP-TARGET-MIB		
No notifications defined		
SNMP-USER-BASED-SM-MIB		
No notifications defined		
SNMP-USM-AES-MIB		
No notifications defined		
SNMPV2-CONF		
No notifications defined		
SNMPV2-MIB		
coldStart	Not event based. Sent after chassis is operationally enabled and both IPv4 and IPv6 gateways are operational. If the gateways are not operational after three minutes the notification is sent.	Yes
authenticationFailure	SnmpEvent_AuthorizationFailed	Yes
warmStart	Not supported	No
SNMPv2-SNMI		
No notifications defined		

Copyright© 2022 Ciena® Corporation

Procedure 6-1
Enabling and disabling alarms

Alarms can be enabled and disabled. Disabling an alarm means that no future instances of this alarm class will occur, regardless of triggering events, until it is enabled.

Step	Action

To enable an alarm

1 Enable an alarm:

```
alarm enable alarm-table-id {alarm-table-id <NUMBER: 1-9999>}
```

where

alarm-table id <NUMBER: 1-9999> is the alarm object.

To disable an alarm

2 Disable an alarm:

```
alarm disable alarm-table-ID {alarm-table-id <NUMBER: 1-9999>}
```

where

alarm-table id <NUMBER: 1-9999> is the alarm object.

—end—

Example

The following example enables an alarm.

```
alarm enable alarm-table-id 8
```


Copyright© 2022 Ciena® Corporation

Procedure 6-2
Deleting an alarm

You can delete an alarm when there is no intention to fix whatever the alarm is flagging.

Step	Action
1	Delete an alarm: `alarm delete alarm-instance-id <alarm-instance-id>` where alarm-instance-id <alarm-instance-id> is the alarm instance ID(s).

—end—

Example

The following example deletes an alarm.

```
alarm disable alarm-table-id 5000
```


Copyright© 2022 Ciena® Corporation

Procedure 6-3
Acknowledging an alarm

You can acknowledge an alarm if you wish to defer the alarm as it cannot be resolved immediately.

Step	Action
1	Acknowledge an alarm: `alarm acknowledge alarm-instance-id <alarm-instance-id>` where alarm-instance-id <alarm-instance-id> is the alarm instance ID(s).

—end—

Example

The following example acknowledges an alarm instance ID of 10.

```
alarm acknowledge alarm-instance-id 10
```


Copyright© 2022 Ciena® Corporation

Procedure 6-4
Enabling and disabling visible alarm output by severity

You can enable and disable visible alarm output based on severity.

Step	Action

To enable alarm output

1 Enable an alarm's severity:

```
alarm enable [visible-severity <String>] [warning-severity]
```

where

visible-severity <String>	enables visual alarms based on severity.
warning-severity	enables warning alarms

To disable alarm output

2 Disable an alarm's severity:

```
alarm disable [visible-severity <String>] [warning-severity]
```

where

visible-severity <String>	disables visual alarms based on severity.
warning-severity	disables warning alarms.

—end—

Example

The following example enables an visible alarm based on severity.

```
alarm enable visible-severity critical
```


Copyright© 2022 Ciena® Corporation

Procedure 6-5
Configuring alarm attributes

You can set and unset an alarm with various alarm attributes.

Step	Action

To set an alarm's attributes

1 Set an alarm's attributes:

```
alarm set alarm-table-id <1..9999> {[cap <NUMBER: 0-
65535>] {criticalat <NUMBER>} [description
<String[25]>]{every <duration: {N[yMwdhms]} {leak
<NUMBER: 0-655535>} {majorat <NUMBER>} {minorat <NUMBER>}
{severity <String>} {threshold <NUMBER: 1-65535>}
{tocritical <duration: {N[yMwdhms]} {tomajor <duration:
{N[yMwdhms]} {tominor <duration: {N{yMwdhms]} {sense
<open|closed>}{trigger <forced|cleared>}
```

where

alarm-table-id <1..9999>	is the alarm table object(s).
{{cap <NUMBER: 0-9999>}	is the counter cap value.
{{criticalat <NUMBER>}	is the critical escalation threshold.
{{description <String[25]>}	is the alarm description.
{every <duration: {N[yMwdhms]}	is the counter leak rate (N[yMwdhms]...)
{leak <NUMBER: 0-655535>}	is the counter leak value.
{majorat <NUMBER>}	is the major escalation threshold.
{minorat <NUMBER>}	is the minor escalation threshold.
{severity <String>}	is the alarm severity.
{threshold <NUMBER: 1-65535>}	is the activation threshold.
{tocritical <duration: {N[yMwdhms]}	is the escalation time to critical (N[yMwdhms]...)
{tomajor <duration: {N[yMwdhms]}	is the escalation time to major (N[yMwdhms]...)
{tominor <duration: {N{yMwdhms]}	is the escalation time to minor (N[yMwdhms]...)
{sense <open | closed>}	is the trigger polarity of the external alarm input pin.
{trigger <forced | clear>}	puts an alarm into (and brings out of) the forced-trigger state.

Copyright© 2022 Ciena® Corporation

To unset an alarm's attributes

2 Unset an alarm's attributes:

```
alarm unset alarm-table-id <1..9999> {cap} {criticalat}
{description}{every} {leak} {majorat} {minorat}
{severity} {threshold} {tocritical} {tomajor} {tominor}
{sense} {trigger}
```

where

alarm-table-id <1..9999>	is the alarm table object(s)
{cap}	is the counter cap value.
{criticalat}	is the critical escalation threshold.
{description}	is the alarm description.
{every}	is the counter leak rate, for example 1h10m3s.
{leak}	is the counter leak value.
{majorat}	is the major escalation threshold.
{minirat}	is the minor escalation threshold.
{severity}	is the alarm severity.
{threshold}	is the activation threshold.
{tocritical}	is the escalation time to critical, for example 1h10m3s.
{tomajor}	is the escalation time to major, for example 1h10m3s.
{tominor}	is the escalation time to minor, for example 1h10m3s.
{sense}	is the trigger polarity of the external alarm input pin.
{trigger}	puts an alarm into (and brings out of) the forced-trigger state.

—end—

Example

The following example sets an alarm's attributes.

```
alarm set alarm-table-id 8 cap 5000 severity warning
threshold 60 criticalat 300 every 1h10m3s leak 4500
majorat 259 minorat 199 tominor 1h10m3s sense open trigger
forced
```


Copyright© 2022 Ciena® Corporation

Procedure 6-6
Displaying alarms

When displaying alarms, the following options are available:

- active alarm table
- defined alarm table
- defined alarm details
- alarm history
- alarm summary

Step	Action

To display the active alarm table

1 Display the active alarm table:

```
alarm show active-alarms {alarm-table-id <NUMBER: 1-
9999>} {from-date <date: yyyy-mm-dd or yy-mm-dd or mm-
dd>} {from-time <time:hh:mm:ss or hh:mm>} {last
<duration: {N[yMwdhms]} {recent} [severity <String>]
{today} {to-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}
{to-time <time: hh:mm:ss or hh:mm>} {yesterday}
```

where

{alarm-table-id <NUMBER: 1-9999>}	is the specified alarm table ID.
{from-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}	are the alarm entries from a specific date.
{from-time <time:hh:mm:ss or hh:mm>}	are the alarm entries from a specific time.
{last <duration: {N[yMwdhms]}	are the recent entries in the active table.
{recent}	are the recent entries in the active table.
severity <String>]	is the alarm severity.
{today}	are today's entries in the active able.
{to-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}	are the entries to date.
{to-time <time: hh:mm:ss or hh:mm>}	are the entries from a specific time.
{yesterday}	are yesterday's entries in the active table.

Copyright© 2022 Ciena® Corporation

To display the defined alarm table

2 Display the defined alarm table:

```
alarm show defined-alarms [severity <String>]
```

where

[severity <String>]	is the alarm's severity.

To display defined alarm details

3 Display defined alarm details:

```
alarm show alarm-table-id <alarm-table-id>
```

where

alarm-table-id <alarm-table-id>	is the alarm details.

To display alarm history

4 Display alarm history:

```
alarm show history <history> {alarm-table-id <NUMBER: 1-
9999>}{from-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}
{from-time <time: hh:mm:ss or hh:mm>} {last <duration:
{N[yMwdhms]}{recent} [severity <String>] {since-
activated} {tail <NUMBER: 1-4294967295>} {today} {to-date
<date: yyyy-mm-dd or yy-mm-dd or mm-dd>} {to-time <time:
hh:mm:ss or hh:mm>} {yesterday}
```

where

history <history>	is the alarm history log.
{alarm-table-id <NUMBER: 1-9999>}	is the specified alarm table ID only.
{from-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}	are the entries from the specified date.
{from-time <time: hh:mm:ss or hh:mm>}	are the entries from the specified time.
{last <duration: {N[yMwdhms]}	are the recent entries into the history log.
{recent}	are the recent entries into the history log.
[severity <String>]	is the alarm's severity.
{since-activated}	are the alarms from the system start or failover.
{tail <NUMBER: 1-4294967295>}	are the latest entries to show.
{today}	are today's entries in the history log.
{to-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>}	are the entries from the specified date.
{to-time <time: hh:mm:ss or hh:mm>}	are the entries from the specified time.
{yesterday}	are yesterday's entries in the history log.

Copyright© 2022 Ciena® Corporation

To display an alarm summary

5 Display an alarm summary:

```
alarm show [statistics] [status]
```

where

alarm show [statistics]	are the alarm statistics.
alarm show [status]	is the alarm status.

To display alarm sense summary

6 Display alarm sense summary information:

```
alarm show sense
```

To display alarms currently in forced state

7 Display alarms currently in forced state:

```
alarm show forced-alarms
```

—end—

Example

The following example shows output for the alarm show active-alarms command.

```
alarm show active alarms
```

```
+-------------------------------------- ACTIVE ALARMS ---------------------------------------+
| IID |Ack|ATID |Severity| Date & Time (Local)      | Instance         | Description          |
+-----+---+-----+--------+--------------------------+------------------+----------------------+
|   1 |   |   3 |  minor | Tue Nov 10 15:23:15 2015 |                3 | Fan Failed           |
+-----+---+-----+--------+--------------------------+------------------+----------------------+
|  |         \---------> ATID : Alarm Table ID                                                |
|  \-------------------> IID  : Alarm Instance ID                                             |
+-------------------------------------------------------------------------------------------+
```

The following example shows the output from the alarm show statistics status command:

```
alarm show statistics status
```


Copyright© 2022 Ciena® Corporation

```
+------------------- ALARM STATISTICS ----------------------+
| On | Dis | Count | Cumulative | Description               |
+----+-----+-------+------------+---------------------------+
|    |     |     0 |          0 | Warning                   |
|  * |     |     1 |          1 | Minor Visible             |
|    |     |     0 |          0 | Major Visible             |
|    |     |     0 |          0 | Critical Visible          |
+----+-----+-------+------------+---------------------------+

+----------- ALARM STATUS ------------+
| On | Dis | Description              |
+----+-----+--------------------------+
|    |     | Warning                  |
|  * |     | Minor Visible            |
|    |     | Major Visible            |
|    |     | Critical Visible         |
+----+-----+--------------------------+
```

The following example shows the output from the alarm show history command:

```
alarm show history
```

```
+------------------------------------ ALARM HISTORY ------------------------------------------+
| HID | Rsn | IID |ATID |Severity| Date & Time (Local)      | Instance         | Description      |
+-----+-----+-----+-----+--------+--------------------------+------------------+------------------+
|   1 | rst |     |     |   info | Tue Nov 10 12:56:04 2015 |                  |                  |
|   2 | tim |     |     |   info | Tue Nov 10 12:56:29 2015 |             +25s |                  |
|   3 | set |   1 |   3 |  minor | Tue Nov 10 15:23:15 2015 |                3 | Fan Failed       |
+-----+-----+-----+-----+--------+--------------------------+------------------+------------------+
|  |          |     \-----> ATID : Alarm Table ID                                                 |
|  |          \-----------> IID  : Alarm Instance ID                                            |
|  \----------------------> HID  : Alarm History ID                                            |
+-------------------------------------------------------------------------------------------------+
```

The following example shows the output from the alarm show defined-alarms command:

```
alarm show defined-alarms
```

```
+------------------------------ ALARM TABLE -------------------------------+
|ATID |Ena|Act|Thr.|Cap| Severity |  Instance | Description                |
+-----+---+---+----+---+----------+-----------+----------------------------+
|   1 | Y |   |  1 |   |    major |           | Overtemperature            |
|   2 | Y |   |  1 |   |    major |           | Undertemperature           |
|   3 | Y |   |  1 |   |    minor |    Fan ID | Fan Failed                 |
|   4 | Y |   |  2 |   |    major |           | Multiple Fans Failed       |
|   5 | Y |   |  1 |   |    major |   Slot ID | Blade POST Failure         |
|   6 | Y |   |  1 |   |    major |   Port ID | Port POST Failure          |
|   7 | Y |   |  1 |   |    major |     PS ID | Power Supply Failure       |
|   8 |   |   |  6 | 9 |    minor |           | Check Security Log         |
|   9 | Y |   |  1 |   |    major |   Port ID | Transceiver Failure        |
|  10 | Y |   |  1 |   |    major |   Port ID | Link Failure               |
|  11 | Y |   |  1 |   |    major |    PWE ID | Data Path Failure         |
|  12 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  13 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  14 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  15 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  16 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  17 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
|  18 | Y |   |  1 |   |    minor |           | External Alarm Trigger     |
```


Copyright© 2022 Ciena® Corporation

```
|  19 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  20 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  21 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  22 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  23 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  24 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  25 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  26 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
|  27 | Y |   |  1 |   |    minor |           | External Alarm Trigger   |
+-----+---+---+----+---+----------+-----------+--------------------------+
```

The following example shows the output from the alarm show sense command:

```
alarm show sense

+--------------- ALARM SENSE --------------+
| ATID | Sense  | Description               |
+------+--------+---------------------------+
|   43 | Closed | External Alarm 1          |
|   44 | Closed | External Alarm 2          |
|   45 | Closed | External Alarm 3          |
|   46 | Closed | External Alarm 4          |
|   47 | Closed | External Alarm 5          |
|   48 | Closed | External Alarm 6          |
|   49 | Closed | External Alarm 7          |
|   50 | Closed | External Alarm 8          |
|   51 | Closed | External Alarm 9          |
|   52 | Closed | External Alarm 10         |
|   53 | Closed | External Alarm 11         |
|   54 | Closed | External Alarm 12         |
|   55 | Closed | External Alarm 13         |
|   56 | Closed | External Alarm 14         |
|   57 | Closed | External Alarm 15         |
|   58 | Closed | External Alarm 16         |
+------+--------+---------------------------+
```

The following example shows the output from the alarm show forced-alarms command:

```
alarm show forced-alarms

+-------------- FORCED ALARMS -------------+
| ATID | Forced | Description               |
+------+--------+---------------------------+
|   36 |        | External Alarm 1          |
|   37 |        | External Alarm 2          |
|   38 |        | External Alarm 3          |
|   39 |        | External Alarm 4          |
|   40 |        | External Alarm 5          |
|   41 |        | External Alarm 6          |
|   42 |        | External Alarm 7          |
|   43 |        | External Alarm 8          |
|   44 |        | External Alarm 9          |
|   45 |        | External Alarm 10         |
|   46 |        | External Alarm 11         |
|   47 |        | External Alarm 12         |
|   48 |        | External Alarm 13         |
|   49 |        | External Alarm 14         |
|   50 |        | External Alarm 15         |
```


Copyright© 2022 Ciena® Corporation

```
|    51 |         | External Alarm 16         |
+-------+---------+---------------------------+
```

The following example shows output for the alarm show command illustrating the port facility loopback feature.

```
alarm show
```

```
+------------------------------------ ACTIVE ALARMS -------------------------------------+
| IID |Ack|ATID |Severity| Date & Time (Local)       | Instance       | Description          |
+-----+---+-----+--------+--------------------------+----------------+----------------------+
|   1 |   |   7 |  major | Sat Jan  1 00:01:46 2000 |              2 | Power Supply Failure |
|  15 |   |  19 |  minor | Sat Jan  1 17:37:51 2000 |              3 | Port Facility-Loopback |
+-----+---+-----+--------+--------------------------+----------------+----------------------+
|  |        \---------> ATID : Alarm Table ID                                              |
|  \-------------------> IID  : Alarm Instance ID                                          |
+-----------------------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-7
Clearing alarm history

You can clear alarm history.

Step	Action
1	Clear alarm history: `alarm clear history`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-8
Clearing alarms

This procedure provides a list of defined alarms along with the description and clearing action, severity and origin.

Alarm Name	Description and clearing action	Severity	Origin
Blade POST Failure	This alarm is raised when a module fails POST on initialization. The alarm is cleared when the module is removed or shut down.	major	Slot ID
Check Security Log	This alarm is raised when the rate of incoming security log items exceeds the configured threshold (disabled by default). This alarm is useful for intrusion detection.	minor	Chassis
CPU Overloaded	This alarm is raised when the CPU is nearing capacity. This alarm depends on the health state changes on the device. The alarm is cleared when the CPU returns to normal operation.	major	Chassis
Dataplane Table Full	This alarm is raised when a resource in the chassis dataplane table reaches capacity. This alarm is cleared when resources are no longer at capacity.	warning	Chassis
Disk Full	This alarm is raised when disk usage is nearing capacity. This alarm is raised from health state changes on the disk devices. The alarm is cleared when disk usage is reduced to normal levels.	major	chassis
Fan Failed	This alarm is raised when the speed of a cooling fan drops below or climbs above specification. This alarm is raised from health state changes on the fan. The alarm is cleared if the fan returns to normal operational speed.	minor	Fan ID

Copyright© 2022 Ciena® Corporation

Alarm Name	Description and clearing action	Severity	Origin
Invalid MAC Address	This alarm is raised when a MAC address error is detected. This alarm occurs when an error is encountered when reading the MAC address from the hardware IDP,	critical	Chassis
Link Down	This alarm is raised when a port link on an administratively enabled port is lost. The alarm is raised based on the health state changes on the transceiver. The alarm is cleared when port link is restored.	warning major	Port
Memory Low	This alarm is raised when the chassis is nearing capacity. This alarm is cleared when memory usage is returned to normal levels.	major	Chassis
Module Init Failure	This alarm is raised when the module fails to initialize and is not operational. A faulted state powers down the module so that it does not inadvertently affect the other modules. A reset, shutdown or removal of the module clears this alarm. This alarm only applies to devices that have plug-in modules.	major	Slot
Multiple Fans Failed	This alarm is raised when multiple fans have failed within a fan tray.	major	Fan Tray
No PDU Received	This alarm is raised on a major-ring when the ring is not receiving any R-APS messages on a virtual-ring port for 17.5 seconds. This alarm is raised on a sub-ring when the ring is receiving R-APS messages on either virtual-ring port for 17.15 seconds.	warning major	Virtual Ring
No RPL Owner Detected	This alarm is raised when a virtual ring that is not the RPL owner receives no R-APS OK message while it is transmitting R-APS RIM messages for 13 or more minutes.	warning	Virtual Ring
NTP Enabled and Not Synced	This alarm is raised when NTP is enabled and configured, but the time is not synchronized.	warning	Chassis

Copyright© 2022 Ciena® Corporation

Alarm Name	Description and clearing action	Severity	Origin
Port Flapping	This alarm is raised when the link state on a port goes up and down repeatedly over a period of time. This can occur approximately six times during a 30-second interval. The alarm is cleared when the link state becomes stable.	warning minor	Port
Port Loopback	This alarm is raised when loopback is set on a port. This alarm is cleared when the loopback is removed.	minor	Port
Port POST Failure	This alarm is raised when a port fails POST on initialization.	major	Port ID
Power Supply Failure	This alarm occurs when a power supply fails.	major	PS ID
Protection Switch Active	This alarm is raised when there is a failure on a physical ring link or when Force Switch is applied on a logical ring link.	warning minor	Virtual Ring
Provisioning Mismatch	This alarm is raised when there is more than one RPL owner configured in a virtual ring.	warning minor	Virtual ring
Overtemperature	This alarm is raised when any chassis/module is over temperature. An over-temperature alarm is chassis based. The exception is the 51XX switches that have modules.	warning major critical	Chassis Module
Redundant Power Removed	This alarm is raised when a PSU is removed from the chassis. The alarm is cleared when the PSU is replaced.	minor	Chassis
Undertemperature	This alarm is raised when any chassis/module is under temperature. An under-temperature alarm is chassis based. The exception is the 51XX switches that have modules.	warning major	Chassis Module
Unreachable Gateway	This alarm is raised when the gateway cannot be reached. This alarm is cleared when the gateway becomes available.	major	Chassis
XCVR Caps Mismatch	This alarm is raised when the port admin settings are incompatible with the XCVR that has been installed	major	Port
XCVR Failed	This alarm is raised when the XCVR fails.	major	Port
XCVR Missing	This alarm is raised when the port is administratively enabled, but no XCVR is present.	minor	Port

Copyright© 2022 Ciena® Corporation

Alarm Name	Description and clearing action	Severity	Origin
XCVR Overtemperature	This alarm is raised when the transceiver temperature is determined to be above specification. This alarm is lowered when the transceiver temperature returns to normal levels.	major warning	Port
XCVR Rx Power High	This alarm is raised when the transceiver Rx power is above specification. This alarm is lowered when the transceiver Rx power returns to normal levels.	warning major	Port
XCVR Rx Power Low	This alarm is raised when the transceiver Rx power is above specification. This alarm is lowed when the transceiver Rx power returns to normal levels.	warning major	Port
XCVR Tx Power High	This alarm is raised when the transceiver Tx power is above specification. This alarm is lowed when the transceiver Tx power returns to normal levels.	warning major	Port
XCVR Tx Power Low	This alarm is raised when the transceiver Tx power is below specification. This alarm is lowed when the transceiver Tx power returns to normal levels.	warning major	Port
XCVR Undertemperature	This alarm is raised when the transceiver Tx power is below specification. The alarm is lowered when the transceiver temperature returns to normal levels.	major warning	Port

Copyright© 2022 Ciena® Corporation

Logging configuration

An event typically refers to an error condition in the 39XX/51XX Switches and Platforms that has an associated alarm severity; some events may be converted into SNMP traps.



WARNING
Turning on logging can negatively affect performance.

This chapter contains the following sections:

- "Logging of events" on page 7-1
- "Event log formatting" on page 7-4

Logging of events

Table 7-1 list the types of logs supported by the system software.

Table 7-1
Types of logs

Type of log	Description
Syslog	Messages sent to collectors which are added (configured) via the 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 written to flash files.

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 to where they should be logged.

Every event can be written to the logs listed above. An event manager converts events to messages and traps.

Copyright© 2022 Ciena® Corporation

An event log is a series of files stored on the 39XX/51XX Switches and Platforms that contains generated events. These events are stored as a set of log files. Logging can be enabled or disabled. Configurable event filters determine what events are stored or discarded. Table 7-2 lists the event log filter attributes.

Table 7-2
Event log filters attributes

Attribute	Read/Write	Value	Default	Description
Admin State	Read/Write	Enable/disable	Enable	Admin state of the filter.
Oper State	Read	Enable/disable	Operational state is enabled if the global admin state and the log filter admin state are enabled.	Operational state of the filter.
Severity List	Read/Write	Event severity list	None	Defines the event severities that will be included in the log. Users can add or remove severities from the filter.
Destination	Read/Write	FLASH/RAM	Flash	Users can select the destination of the log. Each destination has its own log. Flash is the default storage location for the log.
Origin	Read/Write	chassis-shelf-slot-port or system	Empty	Origin of events that collects all events of every origin.

Copyright© 2022 Ciena® Corporation

See the following procedures:

- “Configuring Syslog” on page 7-6
- “Configuring a flash log filter” on page 7-9
- “Configuring flash log packet filters” on page 7-22
- “Displaying flash log and flash log packet filter configuration” on page 7-27
- “Displaying the flash log” on page 7-29
- “Creating a RAM log filter” on page 7-31
- “Configuring RAM log packet filters” on page 7-34
- “Displaying RAM log and RAM log packet filter configuration” on page 7-36
- “Displaying the RAM log” on page 7-39
- “Clearing the log RAM file” on page 7-41
- “Repeating commands” on page 7-42
- “Enabling and disabling command logging” on page 7-45
- “Displaying the command log” on page 7-46
- “Clearing the command log” on page 7-49
- “Exporting the command log” on page 7-50

Copyright© 2022 Ciena® Corporation

Event log formatting

An event is saved to the log file in the following log message format:

```
<date> <time> [<time zone>] Sev:<severity> <origin>: <id string> :<message
string>
```

Each log has an internal timestamp that is used by the CLI. This timestamp is used by the internal log show commands to allow filtering to work correctly regardless of whether UTC or local time stamping is engaged.

Table 7-3 provides descriptions for the fields in the log message format when a log event is saved to the log files.

Table 7-3
Event log format

Field	Description
<date>	is the date the log event occurred
<time>	is the time the log event occurred.
[<time zone>]	indicates the time zone (UTC or local timestamping) that the event was timestamped in.
Sev:<severity>	is a numerical value that indicates the event severity of the log event.
<origin>:	is the component originating the event
<id string>	provides information on the user responsible for generating the log message. For example, an authentication log message identifies the user who logged into the CLI or the failed username login attempt. This field is always displayed prior to the <message string> field of all log messages using a colon as a separator. ***Note 1:*** The <id string> is blank for system generated events, but the colon is displayed. ***Note 2:*** Event logs also support IPv4 and IPv6 addresses.
:<message string>	is the log event details

Copyright© 2022 Ciena® Corporation

Examples

The following example shows a system generated log message:

```
July 7, 2014  17:11:15.316 [local] Sev:3 chassis(1): :active interface is
operationally enabled
```

where

<date>	`July 7, 2014`
<time>	`17:11:15.316`
[<time zone>]	`[local]`
Sev:<severity>	`Sev:3`
<origin>:	`chassis(1):`
<id string>	
:<message string>	`:active interface is operationally enabled`

The following example shows a user generated log message:

```
August 14, 2014  21:09:07.572 [local] Sev:7 chassis(1): Telnet IP
10.128.233.157 User su:Log Filter Severity Add filter default severity config
```

where

<date>	`August 14, 2014`
<time>	`21:09:07.572`
[<time zone>]	`[local]`
Sev:<severity>	`Sev:7`
<origin>:	`chassis(1):`
<id string>	`Telnet IP 10.128.233.157 User su`
:<message string>	`:Log Filter Severity Add filter default severity config`

The following example shows the <id string> field for a configuration change initiated by a user via a Telnet session:

```
Telnet IP 192.168.1.14 User JohnSmith
```

The following example shows the <id> string> field for a configuration change initiated by a user via the serial port:

```
Local RS-232 User JohnSmith
```

The following example shows the <id string> field for a configuration change initiated via SNMP:

```
SNMP IP 192.168.1.14
```


Copyright© 2022 Ciena® Corporation

Procedure 7-1
Configuring Syslog

When configuring Syslog, the following operations are supported:

- enable Syslog globally
- create a Syslog server
- add a Syslog server
- enable Syslog on a specified server

Step	Action

To enable Syslog globally

1 Enable Syslog globally:

```
syslog enable
```

To create a Syslog server

2 Create a syslog server:

```
syslog create collector <collector> custom-prefix
<String[15]> facility <NUMBER: 0-23> severity
<emergency|alert|error|warning|notice|info|debug|all>
udp-port <NUMBER: 514-65535>
```

where

collector <collector>	is the IP address of syslog collector.
custom-prefix <String[15]>	is the syslog message prefix.
facility <NUMBER: 0-23>	is the syslog facility.
severity <emergency| alert | error| warning | notice | info | debug | all>	is the severity of syslog messages to log.
udp-port <NUMBER: 514-65535>	is the UDP port of collector. The default value is 514.

To add a syslog server

3 Add a syslog server:

```
syslog add collector <collector> custom-prefix
<String[15]> facility <NUMBER: 0-23> max-severity
<emergency | alert | critical | error | warning | notice
```


Copyright© 2022 Ciena® Corporation

```
| info | debug> min-severity <emergency | alert | critical
| error | warning | notice | info | debug> severity
<String List> udp-port <NUMBER: 514-65535>
```

where

collector <collector>	is the IP address of syslog collector.
custom-prefix <String[15]>	is the syslog message prefix.
facility <NUMBER: 0-23>	is the syslog facility.
max-severity <emergency | alert | critical | error | warning | notice | info | debug>	is the maximum severity of syslog messages to log.
min-severity <emergency | alert | critical | error | warning | notice | info | debug>	is the minimum severity of syslog messages to log.
severity <String List>	is the syslog severity value that will be allowed to egress.
udp-port <NUMBER: 514-65535>	is the UDP port of collector. The default value is 514.

To enable Syslog on the specified server

4 Enable Syslog on the specified server:

```
syslog enable collector <collector>
```

where

collector <collector>	is the IP address of syslog collector to enable.

5 Confirm the configuration and status:

```
syslog show collector
syslog show
```

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example enables Syslog and adds an IPv4 syslog server.

```
syslog enable
syslog add collector 192.0.2.1 min-severity error max-severity info udp-port 560
facility 1
syslog enable collector 192.0.2.1
```

The following example shows sample output for the syslog show command for an IPv6 syslog server in enabled state.

```
>syslog show
Syslog Admin State: enabled
+---------------------- SYSLOG SERVER CONFIGURATION -----------------------+
|                      |                 | Config      | Admin     | Oper     |
| IP Address           | HostName        | State       | State     | State    |
+----------------------+-----------------+-------------+-----------+----------+
| 2001:db8::           | dtest           | user        | Enabled   | Enabled  |
+----------------------+-----------------+-------------+-----------+----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-2
Configuring a flash log filter



WARNING
Turning on logging can negatively affect performance.

Configure flash log filters for events based on specific managers and severities.

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.

Configurations that can be performed with a flash log filter include:

- Create a flash log filter
- Add events to an existing flash log filter
- Remove events from an existing flash log filter
- Set the severities for a flash log filter
- Delete a custom flash log filter
- Enable flash logging globally or for a specific flash log filter
- Disable flash logging globally or for a specific flash log filter
- Clear a flash log file

Step	Action

To create a flash log filter

1 Create a flash log filter:

```
log flash create filter <filter> {[all-mgrs] [acl-mgr]
[ais-mgr][alarm-mgr][arp-mgr][bfd-mgr][blade-mgr][bcast-
containment-mgr][cfm-mgr][chassis-mgr][config-mgr][dhcp-
mgr][dhcpv6-mgr][dnld-mgr][dnsc-mgr][dot1x-mgr][event-
mgr][flow-mgr][igmp-mgr][interface-mgr][isis-mgr][l2-
protocol-mgr][lacp-mgr][ldp-mgr][lldp-mgr][logging-
mgr][mpls-ldp-mgr][mpls-mgr][mstp-mgr][ndp-mgr][netconf-
helper-mgr][ntpc-mgr][ntwrk-mgr][oam-mgr][ospf-
mgr][perfmon-mgr][pfg-mgr][port][port-mgr][prtc-
mgr][prtc-mgr][radius-mgr][raps-mgr][rmon-mgr][routing-
domain-mgr][rstp-mgr][rstp-mgr][rstp-mgr][rsvp-mgr][rtm-
```


Copyright© 2022 Ciena® Corporation

```
mgr][security-mgr][severity][ssh-mgr][snmp-
mgr][software-mgr][spidd-mgr][sub-port-mgr][sync-
mgr][tacas-mgr][tdm-mgr][traffic-profiling-mgr][twamp-
mgr][virtual-circuit-mgr][vlli-mgr][xcvr-mgr][xftp-mgr]
```

where

filter <filter>	is the log-filter object.
all-mgrs	is all logging categories.
acl-mgr <String List>	is the list of ACL logging categories.
ais-mgr<String List>	is the list of AIS logging categories.
alarm-mgr	is the list of alarm logging categories.
arp-mgr <String List>	is the list of ARP logging categories.
bfd-mgr <String List>	is the list of BFD logging categories.
blade-mgr <String List>	is the list of blade logging categories.
bcast-containment-mgr <String List>	is the list of broadcast containment logging categories.
cfm-mgr <String List>	is the list of CFM logging categories.
chassis-mgr <String List>	is the list of chassis logging categories.
config-mgr <String List>	is the list of config logging categories.
dhcp-mgr <String List>	is the list of DHCP client logging categories.
dhcpv6-mgr <String List>	is the list of DHCPv6 logging categories.
dnld-mgr <String List>	is the list of download logging categories.
dnsc-mgr <String List>	is the list of DNS client logging categories.
dot1x-mgr <String List>	is the list of dot1x logging categories.
event-mgr <String List>	is the list of event logging categories.
flow-mgr <String List>	is the list of flow logging categories.

Copyright© 2022 Ciena® Corporation

where

igmp-mgr <String List>	is the list of IGMP logging categories.
interface-mgr <String List>	is the list of interface logging categories.
isis-mgr <String List>	is the list of ISIS logging categories.
l2-protocol-mgr <String List>	is the list of l2-protocol logging categories.
lacp-mgr <String List>	is the list of LACP logging categories.
ldp-mgr <String List>	is the list of LDP logging categories.
lldp-mgr <String List>	is the list of LLDP logging categories.
logging-mgr <String List>	is the list of logging categories.
mpls-ldp-mgr <String List>	is the list of MPLS-LDP logging categories.
mpls-mgr <String List>	is the list of MPLS logging categories.
mstp-mgr <String List>	is the list of MSTP logging categories.
ndp-mgr <String List>	is the list of NDP logging categories.
netconf-helper-mgr <String List>	is the list of NETCONF-helper logging categories.
ntpc-mgr <String List> <String List>	is the list of NTPC logging categories.
ntwrk-mgr <String List>	is the list of network logging categories.
oam-mgr <String List>	is the list of OAM logging categories.
perfmon-mgr <String List>	is the list of performance monitoring logging categories.
pfg-mgr <String List>	is the list of PFG logging categories.
port <Port list>	is the port list to add to flash log-filter.
port-mgr <String List>	is the list of port logging categories.

Copyright© 2022 Ciena® Corporation

where

prtc-mgr <String List>	is the list of PRTC logging categories.
radius-mgr <String List>	is the list of RADIUS logging categories.
raps-mgr <String List>	is the list of RAPS logging categories.
rmon-mgr <String List>	is the list of RMON logging categories.
routing-domain-mgr <String List>	is the list of routing-domain logging categories.
rstp-mgr <String List>	is the list of RSTP logging categories.
rsvp-mgr <String List>	is the list of RSVP logging categories.
rtm-mgr <String List>	is the list of RTM logging categories.
security-mgr <String List>	is the list of security logging categories.
severity <String List>	is the list of severity logging categories.
ssh-mgr <String List>	is the list of SSH logging categories.
snmp-mgr <String List>	is the list of SNMP logging categories.
software-mgr <String List>	is the list of software logging categories.
spidd-mgr <String List>	is the list of SPIDD logging categories.
sub-port-mgr <String List>	is the list of sub-port logging categories.
sync-mgr <String List>	is the list of SYNC logging categories.
tacacs-mgr <String List>	is the list of TACACS logging categories.
tdm-mgr <String List>	is the list of TDM logging categories.
traffic-profiling-mgr <String List>	is the list of traffic profiling logging categories.
twamp-mgr <String List>	is the list of TWAMP logging categories..

Copyright© 2022 Ciena® Corporation

where

virtual-circuit-mgr <String List>	is the list of virtual circuit logging categories
vlli-mgr <String List>	is the list of VLLI logging categories.
xcvr-mgr <String List>	is the list of XCVR logging categories.
xftp-mgr <String List>	is the list of xFTP logging categories.

To add events to an existing flash log filter

2 Add events to an existing flash log filter:

```
log flash add [filter <filter>] {[all-mgrs] [acl-mgr]
[ais-mgr][alarm-mgr][arp-mgr][bfd-mgr][blade-mgr][bcast-
containment-mgr][cfm-mgr][chassis-mgr][config-mgr][dhcp-
mgr][dhcpv6-mgr][dnld-mgr][dnsc-mgr][dot1x-mgr][event-
mgr][flow-mgr][igmp-mgr][interface-mgr][isis-mgr][l2-
protocol-mgr][lacp-mgr][ldp-mgr][lldp-mgr][logging-
mgr][mpls-ldp-mgr][mpls-mgr][mstp-mgr][ndp-mgr][netconf-
helper-mgr][ntpc-mgr][ntwrk-mgr][oam-mgr][ospf-
mgr][perfmon-mgr][pfg-mgr][port][port-mgr][prtc-
mgr][prtc-mgr][radius-mgr][raps-mgr][rmon-mgr][routing-
domain-mgr][rstp-mgr][rstp-mgr][rstp-mgr][rsvp-mgr][rtm-
mgr][security-mgr][severity][ssh-mgr][snmp-
mgr][software-mgr][spidd-mgr][sub-port-mgr][sync-
mgr][tacas-mgr][tdm-mgr][traffic-profiling-mgr][twamp-
mgr][virtual-circuit-mgr][vlli-mgr][xcvr-mgr][xftp-mgr]
```

where

filter <filter>	is the log-filter object.
all-mgrs	is all logging categories.
acl-mgr <String List>	is the list of ACL logging categories.
ais-mgr<String List>	is the list of AIS logging categories.
alarm-mgr	is the list of alarm logging categories.
arp-mgr <String List>	is the list of ARP logging categories.
bfd-mgr <String List>	is the list of BFD logging categories.
blade-mgr <String List>	is the list of blade logging categories.
bcast-containment-mgr <String List>	is the list of broadcast containment logging categories.

Copyright© 2022 Ciena® Corporation

where

cfm-mgr <String List>	is the list of CFM logging categories.
chassis-mgr <String List>	is the list of chassis logging categories.
config-mgr <String List>	is the list of config logging categories.
dhcp-mgr <String List>	is the list of DHCP client logging categories.
dhcpv6-mgr <String List>	is the list of DHCPv6 logging categories.
dnld-mgr <String List>	is the list of download logging categories.
dnsc-mgr <String List>	is the list of DNS client logging categories.
dot1x-mgr <String List>	is the list of dot1x logging categories.
event-mgr <String List>	is the list of event logging categories.
flow-mgr <String List>	is the list of flow logging categories.
igmp-mgr <String List>	is the list of IGMP logging categories.
interface-mgr <String List>	is the list of interface logging categories.
isis-mgr <String List>	is the list of ISIS logging categories.
l2-protocol-mgr <String List>	is the list of l2-protocol logging categories.
lacp-mgr <String List>	is the list of LACP logging categories.
ldp-mgr <String List>	is the list of LDP logging categories.
lldp-mgr <String List>	is the list of LLDP logging categories.
logging-mgr <String List>	is the list of logging categories.
mpls-ldp-mgr <String List>	is the list of MPLS-LDP logging categories.
mpls-mgr <String List>	is the list of MPLS logging categories.

Copyright© 2022 Ciena® Corporation

where

mstp-mgr <String List>	is the list of MSTP logging categories.
ndp-mgr <String List>	is the list of NDP logging categories.
netconf-helper-mgr <String List>	is the list of NETCONF-helper logging categories.
ntpc-mgr <String List> <String List>	is the list of NTPC logging categories.
ntwrk-mgr <String List>	is the list of network logging categories.
oam-mgr <String List>	is the list of OAM logging categories.
perfmon-mgr <String List>	is the list of performance monitoring logging categories.
pfg-mgr <String List>	is the list of PFG logging categories.
port <Port list>	is the port list to add to flash log-filter.
port-mgr <String List>	is the list of port logging categories.
prtc-mgr <String List>	is the list of PRTC logging categories.
radius-mgr <String List>	is the list of RADIUS logging categories.
raps-mgr <String List>	is the list of RAPS logging categories.
rmon-mgr <String List>	is the list of RMON logging categories.
routing-domain-mgr <String List>	is the list of routing-domain logging categories.
rstp-mgr <String List>	is the list of RSTP logging categories.
rsvp-mgr <String List>	is the list of RSVP logging categories.
rtm-mgr <String List>	is the list of RTM logging categories.
security-mgr <String List>	is the list of security logging categories.
severity <String List>	is the list of severity logging categories.

Copyright© 2022 Ciena® Corporation

where

ssh-mgr <String List>	is the list of SSH logging categories.
snmp-mgr <String List>	is the list of SNMP logging categories.
software-mgr <String List>	is the list of software logging categories.
spidd-mgr <String List>	is the list of SPIDD logging categories.
sub-port-mgr <String List>	is the list of sub-port logging categories.
sync-mgr <String List>	is the list of SYNC logging categories.
tacacs-mgr <String List>	is the list of TACACS logging categories.
tdm-mgr <String List>	is the list of TDM logging categories.
traffic-profiling-mgr <String List>	is the list of traffic profiling logging categories.
twamp-mgr <String List>	is the list of TWAMP logging categories..
virtual-circuit-mgr <String List>	is the list of virtual circuit logging categories
vlli-mgr <String List>	is the list of VLLI logging categories.
xcvr-mgr <String List>	is the list of XCVR logging categories.
xftp-mgr <String List>	is the list of xFTP logging categories.

Copyright© 2022 Ciena® Corporation

To remove events from an existing flash log filter

3 Remove events from an existing flash log filter:

```
log flash remove [filter <filter>] {[all-mgrs] [acl-mgr]
[ais-mgr][alarm-mgr][arp-mgr][bfd-mgr][blade-mgr][bcast-
containment-mgr][cfm-mgr][chassis-mgr][config-mgr][dhcp-
mgr][dhcpv6-mgr][dnld-mgr][dnsc-mgr][dot1x-mgr][event-
mgr][flow-mgr][igmp-mgr][interface-mgr][isis-mgr][l2-
protocol-mgr][lacp-mgr][ldp-mgr][lldp-mgr][logging-
mgr][mpls-ldp-mgr][mpls-mgr][mstp-mgr][ndp-mgr][netconf-
helper-mgr][ntpc-mgr][ntwrk-mgr][oam-mgr][ospf-
mgr][perfmon-mgr][pfg-mgr][port][port-mgr][prtc-
mgr][prtc-mgr][radius-mgr][raps-mgr][rmon-mgr][routing-
domain-mgr][rstp-mgr][rstp-mgr][rstp-mgr][rsvp-mgr][rtm-
mgr][security-mgr][severity][ssh-mgr][snmp-
mgr][software-mgr][spidd-mgr][sub-port-mgr][sync-
mgr][tacas-mgr][tdm-mgr][traffic-profiling-mgr][twamp-
mgr][virtual-circuit-mgr][vlli-mgr][xcvr-mgr][xftp-mgr]
```

where

filter <filter>	is the log-filter object.
all-mgrs	is all logging categories.
acl-mgr <String List>	is the list of ACL logging categories.
ais-mgr<String List>	is the list of AIS logging categories.
alarm-mgr	is the list of alarm logging categories.
arp-mgr <String List>	is the list of ARP logging categories.
bfd-mgr <String List>	is the list of BFD logging categories.
blade-mgr <String List>	is the list of blade logging categories.
bcast-containment-mgr <String List>	is the list of broadcast containment logging categories.
cfm-mgr <String List>	is the list of CFM logging categories.
chassis-mgr <String List>	is the list of chassis logging categories.
config-mgr <String List>	is the list of config logging categories.
dhcp-mgr <String List>	is the list of DHCP client logging categories.

Copyright© 2022 Ciena® Corporation

where

dhcpv6-mgr <String List>	is the list of DHCPv6 logging categories.
dnld-mgr <String List>	is the list of download logging categories.
dnsc-mgr <String List>	is the list of DNS client logging categories.
dot1x-mgr <String List>	is the list of dot1x logging categories.
event-mgr <String List>	is the list of event logging categories.
flow-mgr <String List>	is the list of flow logging categories.
igmp-mgr <String List>	is the list of IGMP logging categories.
interface-mgr <String List>	is the list of interface logging categories.
isis-mgr <String List>	is the list of ISIS logging categories.
l2-protocol-mgr <String List>	is the list of l2-protocol logging categories.
lacp-mgr <String List>	is the list of LACP logging categories.
ldp-mgr <String List>	is the list of LDP logging categories.
lldp-mgr <String List>	is the list of LLDP logging categories.
logging-mgr <String List>	is the list of logging categories.
mpls-ldp-mgr <String List>	is the list of MPLS-LDP logging categories.
mpls-mgr <String List>	is the list of MPLS logging categories.
mstp-mgr <String List>	is the list of MSTP logging categories.
ndp-mgr <String List>	is the list of NDP logging categories.
netconf-helper-mgr <String List>	is the list of NETCONF-helper logging categories.
ntpc-mgr <String List> <String List>	is the list of NTPC logging categories.

Copyright© 2022 Ciena® Corporation

where

ntwrk-mgr <String List>	is the list of network logging categories.
oam-mgr <String List>	is the list of OAM logging categories.
perfmon-mgr <String List>	is the list of performance monitoring logging categories.
pfg-mgr <String List>	is the list of PFG logging categories.
port <Port list>	is the port list to add to flash log-filter.
port-mgr <String List>	is the list of port logging categories.
prtc-mgr <String List>	is the list of PRTC logging categories.
radius-mgr <String List>	is the list of RADIUS logging categories.
raps-mgr <String List>	is the list of RAPS logging categories.
rmon-mgr <String List>	is the list of RMON logging categories.
routing-domain-mgr <String List>	is the list of routing-domain logging categories.
rstp-mgr <String List>	is the list of RSTP logging categories.
rsvp-mgr <String List>	is the list of RSVP logging categories.
rtm-mgr <String List>	is the list of RTM logging categories.
security-mgr <String List>	is the list of security logging categories.
severity <String List>	is the list of severity logging categories.
ssh-mgr <String List>	is the list of SSH logging categories.
snmp-mgr <String List>	is the list of SNMP logging categories.
software-mgr <String List>	is the list of software logging categories.
spidd-mgr <String List>	is the list of SPIDD logging categories.
sub-port-mgr <String List>	is the list of sub-port logging categories.

Copyright© 2022 Ciena® Corporation

where

sync-mgr <String List>	is the list of SYNC logging categories.
tacacs-mgr <String List>	is the list of TACACS logging categories.
tdm-mgr <String List>	is the list of TDM logging categories.
traffic-profiling-mgr <String List>	is the list of traffic profiling logging categories.
twamp-mgr <String List>	is the list of TWAMP logging categories..
virtual-circuit-mgr <String List>	is the list of virtual circuit logging categories
vlli-mgr <String List>	is the list of VLLI logging categories.
xcvr-mgr <String List>	is the list of XCVR logging categories.
xftp-mgr <String List>	is the list of xFTP logging categories.

To set the severities for a flash log filter

4 Set the severities for a flash log filter:

```
log flash set filter <filter> default severity
<all|critical|major|minor|warning|config|info|debug>]
```

where

filter <filter>	is the log-filter object.
all|critical|major|minor|warning|config|info|debug>	is the message severity.

To delete a custom flash log filter

5 Delete a custom flash log filter:

```
log flash delete filter <filter>
```

where

filter <filter>	is the log filter object to be deleted.

To enable flash logging globally or for a specific flash log filter

6 Enable flash logging globally or for a specific flash log filter:

```
log flash enable [filter <filter>]
```

where

filter <filter>	is the log filter object to be enabled.

Copyright© 2022 Ciena® Corporation

To disable flash logging globally or for a specific flash log filter

7 Disable flash logging globally or for a specific flash log filter:

```
log flash disable [filter <filter>]
```

where

filter <filter> is the log filter object to be disabled.

To clear the log flash file

8 Clear the log flash file:

```
log flash clear
```

—end—

Example

The following 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
```


Copyright© 2022 Ciena® Corporation

Procedure 7-3
Configuring flash log packet filters

Configure flash log packet filters to enable logging based on specific packet types or ports. For each flash log packet filter, you can enable or disable packet decoding. When packet decoding is enabled, only the decoded packet is logged.



WARNING
Creating a packet filter for all, ingress, or egress ip-pkt types can use 100% of the CPU resulting in lockup and reboot. Turning on logging can negatively affect performance.

Table 7-4 provides a description of packet filter attributes.

Table 7-4
Packet Filter Attributes

Field	Default	Range (min. max.)/ Value	Description
Admin State	Enabled	Enable, Disable	The administrative state of this collector
Operational State	Enabled	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 Frame type	0	ICL, IGMP, IP, LACP, LLDP, MSTP, RSTP	Defines the maximum severity of messages to be included in the log
Port List	0	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

Operations for log packet filters include:

- Create a packet filter
- Add a packet type or port to a packet filter
- Remove a packet type from a packet filter

Copyright© 2022 Ciena® Corporation

- Set the packet decoding attribute for a packet filter
- Delete a packet filter
- Enable a packet filter
- Disable a packet filter

Step	Action

To create a packet filter

1 Create a flash log packet filter:

```
log flash create pkt-filter <pkt-filter> {[icl-pkt <all | egress | ingress>][igmp-pkt <all | egress | ingress>][ip-pkt <all | egress | ingress>][lacp-pkt <all | egress | ingress>][lldp-pkt <all | egress | ingress>][mstp-pkt <all | egress | ingress>][pkt-decode <all | egress | ingress>][port <all | egress | ingress>][rstp-pkt <all | egress | ingress>]}
```

where

pkt-filter <pkt-filter>	is the log packet-filter object.
icl-pkt <all | egress | ingress>	is ICL packet types.
igmp-pkt <all | egress | ingress>	is IGMP packet types.
ip-pkt <all | egress | ingress>	is IP packet types.
lacp-pkt <all | egress | ingress>	is LACP packet types.
lldp-pkt <all | egress | ingress>	is LLDP packet types.
mstp-pkt <all | egress | ingress>	is MSTP packet types.
pkt-decode	is the packet decode feature.
port <Port list>	is the port list to add to flash pkt-filter.
rstp-pkt <all | egress | ingress>	is RSTP packet types.

To add a packet type or port to a packet filter

2 Add a packet type or port to a packet filter:

```
log flash add pkt-filter <pkt-filter> {[icl-pkt <all|egress|ingress>] [igmp-pkt <all|egress|ingress>][ip-pkt <all|egress|ingress>]
```


Copyright© 2022 Ciena® Corporation

```
[lacp-pkt <all|egress|ingress>] [lldp-pkt
<all|egress|ingress>] [mstp-pkt <all|egress|ingress>]
[port <PortNameList>] [rstp-pkt <all|egress|ingress>]}
```

where

pkt-filter <pkt-filter>	is the packet filter object.
icl-pkt <all | egress | ingress>	is the ICL packet types.
igmp-pkt <all | egress | ingress>	is IGMP packet types.
ip-pkt <all | egress | ingress>	is IP packet types.
lacp-pkt <all | egress | ingress>	is LACP packet types.
lldp-pkt <all | egress | ingress>	is LLDP packet types.
mstp-pkt <all | egress | ingress>	is MSTP packet types.
port <Port list>	is the port list to add to flash pkt-filter.
rstp-pkt <all | egress | ingress>	is RSTP packet types.

To remove a packet type from a packet filter

3 Remove a packet type from a packet filter:

```
log flash remove pkt-filter <pkt-filter> {[icl-pkt
<all|egress|ingress>] [igmp-pkt <all|egress|ingress>]
[ip-pkt <all|egress|ingress>] [lacp-pkt
<all|egress|ingress>] [lldp-pkt <all|egress|ingress>]
[mstp-pkt <all|egress|ingress>] [port <Port list>] [rstp-
pkt <all|egress|ingress>]}
```

where

pkt-filter <pkt-filter>	is the packet filter object.
icl-pkt <all | egress | ingress>	is the ICL packet types.
igmp-pkt <all | egress | ingress>	is IGMP packet types.
ip-pkt <all | egress | ingress>	is IP packet types.
lacp-pkt <all | egress | ingress>	is LACP packet types.
lldp-pkt <all | egress | ingress>	is LLDP packet types.

Copyright© 2022 Ciena® Corporation

where

mstp-pkt <all | egress | ingress>	is MSTP packet types.
port <Port list>	is the port list to add to flash pkt-filter.
rstp-pkt <all | egress | ingress>	is RSTP packet types.

To set the packet decoding attribute for a packet filter

4 Set the packet decoding attribute for a packet filter:

```
log flash set pkt-filter <pkt-filter> {pkt-decode
<on|off>}
```

where

pkt-filter <pkt-filter>	is the packet filter object.
pkt-decode <on|off>	is the packet decode feature.

To delete a packet filter

5 Delete a packet filter:

```
log flash delete pkt-filter <pkt-filter>
```

where

pkt-filter <pkt-filter>	is the packet filter object.

To enable a packet filter

6 Enable a packet filter:

```
log flash enable pkt-filter <pkt-filter>
```

where

pkt-filter <pkt-filter>	is the packet filter object.

To disable a packet filter

7 Disable a packet filter:

```
log flash disable pkt-filter <pkt-filter>
```

where

pkt-filter <pkt-filter>	is the packet filter object.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following 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
```


Copyright© 2022 Ciena® Corporation

Procedure 7-4
Displaying flash log and flash log packet filter configuration

You can display:

- flash log filter configuration
- flash packet filter configuration
- flash filter summaries

Step	Action

To display flash log-filter configuration

1 Display flash log-filter configuration:

```
log flash show filter <filter>
```

where

filter <filter>	is the log filter object.

To display flash packet -filter configuration

2 Display flash packet filter configuration:

```
log flash show pkt-filter <pkt-filter>
```

where

pkt-filter <pkt-filter>	is the packet filter object.

To display flash log-filter configuration

3 Display flash filter summaries:

```
log flash show log-summary pkt-summary severity-mapping
system-events
```

where

log-summary	displays a summary of log filters.
pkt-summary	displays a summary of packet filters.
severity-mapping	displays event/syslog severity map.
system-events	displays system events.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows 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 ----------------------+
|                   | Admin     | Oper      |         Severity        |            |
| Filter Name       | State     | State     | Maximum   | Minimum     | No. Ports  |
+-------------------+-----------+-----------+-----------+-----------+------------+
| default           | enabled   | enabled   | critical  | critical    | 28         |
| dhcpOptions       | enabled   | enabled   | critical  | debug       | 0          |
+-------------------+-----------+-----------+-----------+-----------+------------+

+---------------------- FLASH PKT FILTER CONFIGURATION ----------------------+
|                   | Admin     | Oper      | Pkt       | No. Frame |            |
| Filter Name       | State     | State     | Decode    | Types     | No. Ports  |
+-------------------+-----------+-----------+-----------+-----------+------------+
| test              | enabled   | enabled   | off       | 0         | 0          |
+-------------------+-----------+-----------+-----------+-----------+------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-5
Displaying the flash log

You can display the entries made to flash based upon the configured flash log and flash log packet filters.

You can also display the log files located in the /mnt/sysfs/log directory.

Step	Action
1	Display the flash log: `log flash view [tail <NUMBER: 1-100>]|[keyword <String[16]>]` where tail <NUMBER: 1-100> displays last x lines. keyword <String[16]> displays last lines that contain keyword. **—end—**

Copyright© 2022 Ciena® Corporation

Example

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.

```
log flash view tail 6
------------ > BOOTING < ------------
January 1, 2000  00:00:44.607 [local] chassis: :AC power supply 1 failure
January 1, 2000  00:00:44.626 [local] interface: :remote interface is operationa
lly enabled
December 31, 1999  17:00:46.974 [local] interface: :remote interface is operatio
nally enabled
December 31, 1999  17:01:30.369 [local] Software: saos-06-05-01-0026 Build 26
December 31, 1999  17:01:33.231 [local] chassis: :AC power supply 1 online
```

The following example shows the time at which the unit was rest and the reason for the reset.

```
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
```


Copyright© 2022 Ciena® Corporation

Procedure 7-6
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.



WARNING
Turning on logging can negatively affect performance.

Step	Action

To create a RAM log filter

1 Create a RAM log filter:

```
log ram create filter <filter> {[all-mgrs] [acl-mgr]
[ais-mgr] [alarm-mgr][arp-mgr][bfd-mgr][blade-
mgr][bcast-containment-mgr][cfm-mgr][chassis-
mgr][config-mgr][dhcp-mgr][dhcpv6-mgr][dnld-mgr][dnsc-
mgr[]dot1x-mgr][event-mgr][flow-mgr][igmp-
mgr][interface-mgr][isis-mgr][l2-protocol-mgr][lacp-
mgr][ldp-mgr][lldp-mgr][logging-mgr][mpls-ldp-mgr][mpls-
mgr][ndp-mgr][netconf-helper-mgr][ntpc-mgr][ntwrk-
mgr][oam-mgr][oam-mgr][ospf-mgr][perfmon-mgr][pgf-
mgr][port][port-mgr][prtc-mgr][radius-mgr][rmon-
mgr][routing-domain-mgr][rstp-mgr][rsvp-mgr][vsvp-
mgr][rtm-mgr][security-mgr][severity][ssh-mgr][snmp-
mgr][software-mgr][spidd-mgr][sub-port-mgr][sync-
mgr][tacacs-mgr][tdm-mgr][traffic-profiling-mgr][twamp-
mgr][virtual-circuit-mgr][vlli-mgr][xcvr-mgr][xftp-mgr]
```

To add events to an existing RAM log filter

2 Add events to an existing RAM log filter:

```
log ram add filter <filter> {[all-mgrs] [acl-mgr
<all|info>][ais-mgr <all|config|info>][alarm-mgr
<all|config|info>][arp-mgr <all|info>][bfd-mgr
<all|config|info>][blade-mgr <all|config|info>] [bcast-
containment-mgr <all|info>] [cfm-mgr <all|info>]
[chassis-mgr <all|info>] [config-mgr <all|info>] [dhcp-
mgr
<all|debug|error|info|options|pkt|sm|timers>][dhcpv6-mgr
<accounting|all||info|options>] [dnld-mgr <all|info>]
[dnsc-mgr all|info] [dot1x <all|info>] [event-mgr
```


Copyright© 2022 Ciena® Corporation

```
<all|info>] [flow-mgr <all|info> [igmp-mgr
<all|events|egress-pkt|info|ingress-pkt>] [interface-mgr
<all|debug|info>][isis-mgr <all|config|info>][l2-
protocol-mgr <all|info>] [lacp-mgr
<all|error|info|notif|mux-sm|ptx-ss-pkt>] [ldp-mgr
<all|info>][lldp-mgr
<all|error|info|notif|other|pdu|sm>] [logging-mgr
<all|config|info>][mpls-ldp-mgr <all|config|info>][mpls-
mgr <all|config|info> [mstp-mgr <all|info> [ndp-mgr
<all|info>][netconf-helper-mgr <all|info>][ntpc-mgr
<all|config|debug|info>] [ntwrk-mgr <all|info>] [oam-mgr
<all|info>][ospf-mgr <all|info>] [perfmon-mgr
<all|config|info>][pfg-mgr <all|info> [port
<PortNameList>] [port-mgr <all|config|info|state-
change>][prtc-mgr <all|info>][radius-mgr <all|info>]
[raps-mgr <all|info>][rmon-mgr <all|info>] [routing-
domain-mgr <all|debug|info>][rstp-mgr <all|info>][rsvp-
mgr <all|info>][rsvp-mgr <all_info>][rtm-mgr
<all|config|info>][security-mgr <all|info>] [ssh-mgr
<all|info>] [snmp-mgr <all|info>] [software-mgr
<all|info>] [spidd-mgr <all|info>][sub-port-mgr
<all|info>][sync-mgr <all|config|info|state-change>]
[tacacs-mgr <all|info>][tdm-mgr <all|info|state-
change>][traffic-profiling-mgr <all|info>] [twamp-mgr
<all|info>] [virtual-circuit-mgr <all|info>][vlli-mgr
<all|error|info|notif>] [xcvr-mgr <all|debug|info>],
[xftp-mgr <all|config|info>]}
```

To remove events from an existing RAM log filter

3 Remove events from an existing RAM log filter:

```
log ram remove filter <filter> {[all-mgrs] [acl-mgr
<all|info>][ais-mgr <all|config|info>][alarm-mgr
<all|config|info>][arp-mgr <all|info>][bfd-mgr
<all|config|info>][blade-mgr <all|config|info>] [bcast-
containment-mgr <all|info>] [cfm-mgr <all|info>]
[chassis-mgr <all|info>] [config-mgr <all|info>] [dhcp-
mgr
<all|debug|error|info|options|pkt|sm|timers>][dhcpv6-mgr
<accounting|all||info|options>] [dnld-mgr <all|info>]
[dnsc-mgr all|info] [dot1x <all|info>] [event-mgr
<all|info>] [flow-mgr <all|info> [igmp-mgr
<all|events|egress-pkt|info|ingress-pkt>] [interface-mgr
<all|debug|info>][isis-mgr <all|config|info>][l2-
protocol-mgr <all|info>] [lacp-mgr
<all|error|info|notif|mux-sm|ptx-ss-pkt>] [ldp-mgr
<all|info>][lldp-mgr
<all|error|info|notif|other|pdu|sm>] [logging-mgr
<all|config|info>][mpls-ldp-mgr <all|config|info>][mpls-
mgr <all|config|info> [mstp-mgr <all|info> [ndp-mgr
<all|info>][netconf-helper-mgr <all|info>][ntpc-mgr
```


Copyright© 2022 Ciena® Corporation

```
<all|config|debug|info>] [ntwrk-mgr <all|info>] [oam-mgr
<all|info>][ospf-mgr <all|info>] [perfmon-mgr
<all|config|info>][pfg-mgr <all|info> [port
<PortNameList>] [port-mgr <all|config|info|state-
change>][prtc-mgr <all|info>][radius-mgr <all|info>]
[raps-mgr <all|info>][rmon-mgr <all|info>] [routing-
domain-mgr <all|debug|info>][rstp-mgr <all|info>][rsvp-
mgr <all|info>][rsvp-mgr <all_info>][rtm-mgr
<all|config|info>][security-mgr <all|info>] [ssh-mgr
<all|info>] [snmp-mgr <all|info>] [software-mgr
<all|info>] [spidd-mgr <all|info>][sub-port-mgr
<all|info>][sync-mgr <all|config|info|state-change>]
[tacacs-mgr <all|info>][tdm-mgr <all|info|state-
change>][traffic-profiling-mgr <all|info>] [twamp-mgr
<all|info>] [virtual-circuit-mgr <all|info>][vlli-mgr
<all|error|info|notif>] [xcvr-mgr <all|debug|info>],
[xftp-mgr <all|config|info>]}
```

To set the severities for a RAM log filter

4 Set the severities for a RAM log filter:

```
log ram set filter <filter> {[severity
<all|critical|major|minor|warning|config|info|debug>]}
```

To delete a custom RAM log filter

5 Delete a custom RAM log filter:

```
log ram delete filter <filter]>
```

To enable flash logging globally or for a specific ram log filter:

6 Enable flash logging globally or for a specific ram log filter:

```
log ram enable [filter <filter>]
```

To disable flash logging globally or for a specific ram log filter

7 Disable flash logging globally or for a specific ram log filter:

```
log ram disable [filter <filter>]
```

—end—

Example

The following 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
```


Copyright© 2022 Ciena® Corporation

Procedure 7-7
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 filter, you can enable or disable packet decoding. When packet decoding is enabled, only the decoded packet is logged.



WARNING
Creating a packet filter for all, ingress, or egress ip-pkt types can use 100% of the CPU resulting in lockup and reboot. Turning on warning can negatively affect performance.

The following operations are supported for RAM log filters:

- Create a packet filter
- Add a packet type or port to a packet filter
- Remove a packet type from a packet filter
- Set the packet decoding attribute for a packet filter

Step	Action

To create a packet filter

1 Create a packet filter:

```
log ram create pkt-filter <pkt-filter> {[icl-pkt
<all|egress|ingress>][igmp-pkt <all|egress|ingress>]
[ip-pkt <all|egress|ingress>][lacp-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

2 Add a packet type or port to a packet filter:

```
log ram add pkt-filter <pkt-filter> {{[icl-pkt
<all|egress|ingress>][igmp-pkt <all|egress|ingress>]
[ip-pkt <all|egress|ingress>][lacp-pkt
<all|egress|ingress>] [lldp-pkt <all|egress|ingress>]
[mstp-pkt <all|egress|ingress>] [port <PortNameList>]
[rstp-pkt <all|egress|ingress>]}
```


Copyright© 2022 Ciena® Corporation

To remove a packet type from a packet filter

3 Remove a packet type from a packet filter:

```
log ram remove pkt-filter <pkt-filter> {{[icl-pkt
<all|egress|ingress>][igmp-pkt <all|egress|ingress>]
[ip-pkt <all|egress|ingress>][lacp-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

4 Set the packet decoding attribute for a packet filter:

```
log ram set pkt-filter <pkt-filter> {pkt-decode <on|off>}
```

To delete a packet filter

5 Delete a packet filter:

```
log ram delete pkt-filter <pkt-filter>
```

To enable a packet filter

6 Enable a packet filter:

```
log ram enable pkt-filter <pkt-filter>
```

To disable a packet filter

7 Disable a packet filter:

```
log ram disable pkt-filter <pkt-filter>
```

—end—

Example

The following 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
```


Copyright© 2022 Ciena® Corporation

Procedure 7-8
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
- a summary of packet filters only
- details for a specific flash log or flash log packet filters

Step	Action
1	Display flash log filter configuration: `log ram show [filter <filter>] | [pkt-filter <pkt-filter>] | [log-summary] | [pkt-summary][severity-mapping] [system-events]`

Example

This example shows 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 -------------------------+
|                   | Admin     | Oper      |         Severity        |            |
| Filter Name       | State     | State     | Maximum   | Minimum     | No. Ports  |
+-------------------+-----------+-----------+-----------+-------------+------------+
| default           | enabled   | enabled   | critical  | info        | 12         |
+-------------------+-----------+-----------+-----------+-------------+------------+

+------------------------ RAM PKT FILTER CONFIGURATION -------------------------+
|                   | Admin     | Oper      | Pkt       | No. Frame   |            |
| Filter Name       | State     | State     | Decode    | Types       | No. Ports  |
+-------------------+-----------+-----------+-----------+-------------+------------+
| No Filters        |           |           |           |             |            |
+-------------------+-----------+-----------+-----------+-------------+------------+
```


Copyright© 2022 Ciena® Corporation

The following example shows the default RAM log filter configuration.

```
log ram show filter default

+---------------------- LOG RAM FILTER CONFIGURATION -----------------------+
| Name               | default                                              |
| Index              | 1                                                    |
| Admin State        | enabled                                              |
| Oper State         | enabled                                              |
| Severity List      | critical                                             |
|                    | major                                                |
+--------------------+------------------------------------------------------+
|  Categories        | ais-mgr                  - config                    |
|                    |                          - info                      |
|                    | alarm-mgr                - config                    |
|                    |                          - info                      |
|                    | bfd-mgr                  - config                    |
|                    |                          - info                      |
|                    | blade-mgr                - config                    |
|                    |                          - info                      |
|                    | chassis-mgr              - info                      |
|                    | config-mgr               - info                      |
|                    | dhcp-mgr                 - debug                     |
|                    |                          - error                     |
|                    |                          - info                      |
|                    |                          - options                   |
|                    |                          - pkt                       |
|                    |                          - sm                        |
|                    |                          - timers                    |
|                    | dnld-mgr                 - info                      |
|                    | dnsc-mgr                 - resolve                   |
|                    |                          - monitor                   |
|                    |                          - info                      |
|                    | event-mgr                - info                      |
|                    | igmp-mgr                 - events                    |
|                    |                          - egress-pkt                |
|                    |                          - ingress-pkt               |
|                    |                          - info                      |
|                    | interface-mgr            - debug                     |
|                    |                          - info                      |
|                    | isis-mgr                 - config                    |
|                    |                          - info                      |
|                    | l2-protocol-mgr          - info                      |
|                    | lacp-mgr                 - error                     |
|                    |                          - info                      |
|                    |                          - notif                     |
|                    |                          - mux-sm                    |
|                    |                          - ptx-sm                    |
|                    |                          - rx-sm                     |
|                    |                          - sl-sm                     |
|                    |                          - tx-sm                     |
|                    | ldp-mgr                  - info                      |
|                    | lldp-mgr                 - error                     |
|                    |                          - notif                     |
|                    |                          - other                     |
|                    |                          - pdu                       |
|                    |                          - sm                        |
|                    |                          - info                      |
|                    | mpls-ldp-mgr             - config                    |
|                    |                          - info                      |
|                    | mpls-mgr                 - config                    |
|                    |                          - info                      |
|                    | mstp-mgr                 - info                      |
|                    | ntpc-mgr                 - config                    |
|                    |                          - debug                     |
|                    |                          - info                      |
```


Copyright© 2022 Ciena® Corporation

```
|                   | ospf-mgr                - info                                |
|                   | perfmon-mgr             - config                              |
|                   |                         - info                                |
|                   | port-mgr                - config                              |
|                   |                         - info                                |
|                   |                         - state-change                        |
|                   | prtc-mgr                - info                                |
|                   | routing-domain-mgr      - debug                               |
|                   |                         - info                                |
|                   | rsvp-mgr                - info                                |
|                   | rtm-mgr                 - config                              |
|                   |                         - info                                |
|                   | snmp-mgr                - info                                |
|                   | software-mgr            - info                                |
|                   | spidd-mgr               - info                                |
|                   | sync-mgr                - config                              |
|                   |                         - info                                |
|                   |                         - state-change                        |
|                   | vlli-mgr                - error                               |
|                   |                         - notif                               |
|                   |                         - info                                |
|                   | xcvr-mgr                - info                                |
|                   |                         - debug                               |
|                   | xftp-mgr                - config                              |
|                   |                         - info                                |
+-------------------+-------------------------------------------------------------+

+-------------------+------------+
|                   |          1 |
|                   |123456789012|
+-------------------+------------+
| Port List         |XXXXXXXXXXXX|
+-------------------+------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-9
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.

Step	Action
1	Activate the RAM trace buffer display: `log ram trace [all]` where all show entire trace buffer.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows sample output for the log ram trace command.

```
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--
```

The following example shows sample output for the log ram trace all command.

```
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: lldpBAdmStateSET() 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
-----------------------------------
```


Copyright© 2022 Ciena® Corporation

Procedure 7-10
Clearing the log RAM file

Clear the log RAM file.

Step	Action
1	Clear the log RAM file: `log ram clear`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-11
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: Commands that run in interactive mode only (such as, all of the commands on the "file" menu and "command-log repeat") and those that contain a clear text password cannot be repeated using the "command-log repeat" command. If you run `command-log repeat my-last-command` and the last command run was an interactive mode only or contains a clear text password, the system will rerun the command you ran prior to it. Also, if you run `command-log repeat` and specify a sequence ID for one of these commands, it will fail with the error message "`Cannot repeat command: <command>`."

Step	Action

1 Repeat a command:

```
command-log repeat [command <String>] [every <duration: {N[yMwdhms]} [my-last-command ] [sequence-id <NUMBER>] [times <NUMBER: 1-4294967295>]
```

where

[command <String>]	is the command.
[every <duration: {N[yMwdhms]}	is the time between repetitions.
[my-last-command]	is the last-executed command in the session.
sequence-id <NUMBER>	is the identifier.
times<NUMBER: 1-4294967295>	is the number of repetitions.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows sample output for the command log repeat 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
```

The following example shows sample output for the command-log repeat sequence-id command.

```
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
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for 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       |
+---------------------+-----------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-12
Enabling and disabling 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.

Step	Action

To disable command logging

1 Disable command logging:

```
command-log disable
```

To enable command logging

2 Enable command logging:

```
command-log enable
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-13
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.

Step	Action
1	Display the command log: `command-log show {containing <String128>} {destination} {exit-status <NUMBER: 0-4294967295>} {from-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd>} {from-time <time: hh:mm:ss or hh:mm>} {last <DurationString>} {mine} {on-terminal <String[32]>} {privilege <limited|admin|super|diag>} {recent} {sequence-id <NUMBER>} {since-activated} {status} {tail <NUMBER: 1-4294967295>} {today} {to-date <<date: yyyy-mm-dd or yy-mm-dd or mm-dd>} {to-time <time: hh:mm:ss or hh:mm>} {user <String[32]>} {verbose} {yesterday}` where containing <String128> — displays entries containing a specific string. destination — displays the location of the command log file. exit-status <NUMBER: 0-4294967295> — displays entries with given exit status. from-date <date: yyyy-mm-dd or yy-mm-dd or mm-dd> — displays entries from specified date (yyyy-mm-dd or yy-mm-dd or mm-dd). from-time <time: hh:mm:ss or hh:mm> — displays entries from specified time (hh:mm or hh:mm:ss) last <DurationString> — displays entries from the specified time interval in the format N[yMwdhms]. If you specify a number only, the interval will be shown in seconds. mine — displays the session entries. on-terminal <String32> — displays entries of commands run from a specific terminal ID. privilege <lmited|admin|super|diag> — displays user access level.

Copyright© 2022 Ciena® Corporation

where	
recent	displays entries into the history log within the last hour
sequence-id <#List>	displays entries with the specified sequence identifier(s).
since-activated	displays from system start or failover.
status	displays command log configuration state.
tail <NUMBER: 1-4294967295>	displays latest entries.
today	displays today's entries in the command log.
to-date <DateString>	displays entries to specified date (yyyy-mm-dd or yy-mm-dd or mm-dd).
to-time <TimeString>	displays entries to specified time (hh:mm or hh:mm:ss).
user <String[16]>	displays entries for the specified user.
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.
yesterday	displays yesterday's entries in the command log.

—end—

Example

The following example shows sample output for the command-log show destination command.

```
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
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the command-log show recent verbose command.

```
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 |                                            |
+-------+--------------------------+--------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-14
Clearing the command log

You can clear the command log.

Step	Action
1	Clear the command log: `command-log clear` **—end—**

Copyright© 2022 Ciena® Corporation

Procedure 7-15
Exporting the command log

You can export the command log to a remote file location for viewing outside of the CLI. Command log files can be exported to a remote xFTP, SFTP, TFTP server by IP address or to an HTTP server using the URL.

The command log consists of a series of up to 5 files. All files must be exported to obtain the complete command log.

Note: Exporting the command log involves exporting multiple files in sequence using separate commands. It is possible that during this process the command log could be written to by the system, resulting in a loss of synchronization amongst the exported command log files. It is recommended that command log exports be performed during times of low system activity

Step	Action

1	Export the first command log file:
	`system xftp putfile {local-filename <String> {remote-filename <String>}`
	`{default-server|default-ftp-server|default-tftp-server|default-sftp-server|`
	`{tftp-server <ip-host-str> [server-port <INTEGER: 1..65535>]}`
	`{ftp-server <ip-host-str> [login-id <username> [<password-attr>|<echoless-password-attr>][server-port <INTEGER: 1..65535>]}|`
	`{sftp-server <ip-host-str> login-id <username> {<password-attr>|<echoless-password-attr>}[server-port <INTEGER: 1..65535>]}}`
	`[url <String>`
	where
	local-filename <String> is the local filename.
	remote-filename <String> is the remote filename.
	default-server uses the default xFTP server.
	default-ftp-server uses the default FTP server.
	default-tftp-server uses the default TFTP server.

Copyright© 2022 Ciena® Corporation

where

default-sftp-server	uses the default SFTP server.
tftp-server <IP-host-str>	is the TFTP server.
server-port <INTEGER: 1..65535>	is the server port number.
ftp-server <IP-host-str>	is the FTP server name.
login-id <username>	is the TFTP/FTP/SFTP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
sftp-server <IP-host-str>	is the SFTP server.
url <String>	is the remote file URL.

2 Repeat the above command for the 4 remaining command log files.

—end—

Example

The following example exports the complete command log file set to a remote TFTP server by specifying its IP address:

```
system xftp putfile tftp-server 10.10.10.10 local-filename /flash1/log/cmdLog.0
remote-filename cmdLog.0
system xftp putfile tftp-server 10.10.10.10 local-filename /flash1/log/cmdLog.1
remote-filename cmdLog.1
system xftp putfile tftp-server 10.10.10.10 local-filename /flash1/log/cmdLog.2
remote-filename cmdLog.2
system xftp putfile tftp-server 10.10.10.10 local-filename /flash1/log/cmdLog.3
remote-filename cmdLog.3
system xftp putfile tftp-server 10.10.10.10 local-filename /flash1/log/cmdLog.4
remote-filename cmdLog.4
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Virtual Link Loss Indicator (VLLI) configuration

VLLI allows network elements at the UNI-N of an EVC to signal to the UNI-C of the customer premise equipment (CPE) if:

- The remote UNI attachment interface has failed or recovered.
- The EVC connection has failed or recovered causing end-to-end client traffic to be transported.

An instance represents an application service, for example, CFM service. It can be either source or destination. The Instance can trigger the action of other Instances in the same instance group. Each Instance links to an action group.

VLLI configuration requires configuring:

- instance groups
- action groups

An instance group represents a VLLI operation group. It contains multiple instances, to a maximum of 256. Since each instance is bound to an action group, source actions can be triggered based on the event type if bidirectional is configured.

VLLI support unidirectional and bidirectional operation on the same instance group.

This chapter provides the following procedures for VLLI:

- “Configuring instance groups” on page 8-2
- “Configuring action groups” on page 8-5
- “Displaying recovery and fault counter information” on page 8-7

Copyright© 2022 Ciena® Corporation

Procedure 8-1
Configuring instance groups

When configuring instance groups, you can:

- create an instance group
- add an instance to an instance group
- configure active direction on an instance group
- enable VLLI on an instance group
- delete an instance group
- remove an instance from an instance group
- set a command for an instance group
- show an instance group

Step	Action

To create an Instance group

1 Create an instance group:

```
virtual-link-loss-indication create instance-group
<String[31]>
```

where

instance-group <String[31]> is a string that identifies the instance group.

To add an instance to an instance group

2 Add an instance to an instance group:

```
virtual-link-loss-indication add instance-group
<instance-group-name> {cfm-instance <instance name>/
port-instance <instance name> /vc-instance <instance
name>} mode <source/destination> [action-group <group-
name>]
```

To configure active direction on an instance group

3 Configure active direction on an instance group:

```
virtual-link-loss-indication set instance-group
<instance-group-name> direction <unidirectional/
bidirectional>
```


Copyright© 2022 Ciena® Corporation

To enable VLLI on an instance group

4 Enable VLLI on an instance group:

```
virtual-link-loss-indication enable [instance-group
<instance-group-name>]
```

where

instance-group <instance-group-name>	is the instance group that VLLI is to be enabled on

To delete an instance group

5 Delete an instance group:

```
virtual-link-loss-indication delete instance-group
<instance-group-name>
```

where

instance-group <instance-group-name>	is the instance group to be deleted

To set an action on an instance

6 Set an action on an instance:

```
virtual-link-loss-indication set instance-group
<instance-group-name> {cfm-instance <instance name>/
port-instance <instance name>/vc-instance <instance
name>} mode <source/destination> action-group <group-
name>
```

To unset an action from an instance

7 Unset an action from an instance:

```
virtual-link-loss-indication unset instance-group
<instance-group-name> {cfm-service-instance <instance
name>/port-instance <instance name>/vc-instance
<instance name>}
```

To remove an instance from an instance group

8 Remove an instance from an instance group:

```
virtual-link-loss-indication remove instance-group
<instance-group-name> {cfm-instance <instance name>/
port-instance <instance name>/vc-instance <instance
name>} mode <source/destination>
```

To set a command for an instance group

9 Configure an active direction for an instance group:

```
virtual-link-loss-indication set instance-group
<instance-group-name> direction <unidirectional/
bidirectional>
```


Copyright© 2022 Ciena® Corporation

10 Configure instance attributes:

```
virtual-link-loss-indication set instance-group
<instance-group-name> [force-fault/force-recovery]
```

11 Configure the action trigger:

```
virtual-link-loss-indication set instance-group
<instance-group-name> [trigger <all | any>]
```

where

instance-group <instance-group-name>	is the instance group that the trigger condition is to be set for
trigger <all | any>	is the trigger condition for an instance group. • all: the switch detects all the same events from the source instance before triggering the target's action. • any: the target's action is triggered if any source's event is detected.

To show an instance group

12 Show an instance group:

```
virtual-link-loss-indication show [instance-group
<instance-group-name>]
```

where

instance-group <instance-group-name>	is the instance group to be displayed

—end—

Copyright© 2022 Ciena® Corporation

Procedure 8-2
Configuring action groups

When configuring action groups, you can:

- Create an action group
- Delete an action group
- Add an action to an action group:
- Remove an action from an action group
- Display an action group

Step	Action

To create an action group

1 Create an action group:

```
virtual-link-loss-indication create action-group
<action-group-name> [direction <unidirectional/
bidirectional>] [trigger <any/all>]
```

To delete an action group

2 Delete an action group:

```
virtual-link-loss-indication delete action-group
<action-group-name>
```

where

action-group <action-group-name>	identifies the action group to be deleted

To add an action to an action group

3 Add an action to an action group:

```
virtual-link-loss-indication add action-group <action-
group-name> type <fault/recovery> action <port-shut/
port-unshut/ccm-stop/ccm-resume/mac-flush/vc-mac-
withdraw/pw-status-fault/pw-status-clear> precedence <1-
8>
```

To remove an action from an action group

4 Remove an action from an action group:

```
virtual-link-loss-indication remove action-group
<action-group-name> action < port-shut/port-unshut/ccm-
stop/ccm-resume/mac-flush/vc-mac-withdraw/pw-status-
fault/pw-status-clear>]
```


Copyright© 2022 Ciena® Corporation

To display an action group

5 Display an action group:

```
virtual-link-loss-indication show [action-group <action-group-name>]
```

where

action-group <action-group-name>	identifies the action group to be displayed

—end—

Copyright© 2022 Ciena® Corporation

Procedure 8-3
Displaying recovery and fault counter information

Display recovery and fault counter information when troubleshooting.

Step	Action
1	Display recovery and fault counter information: `virtual-link-loss-indication show counter`

—end—

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Fault management troubleshooting

This chapter provides the following fault management troubleshooting procedures:

- “Sending log test messages” on page 9-2
- “Resetting log file configuration to defaults” on page 9-3

Copyright© 2022 Ciena® Corporation

Procedure 9-1
Sending log test messages

Send a test message to test the configuration of log flash and RAM filters.

Step	Action
1	Send a test message: `log send msg <String[127]> severity <critical|major|minor|warning|config|info|debug>`

—end—

Example

The following example sends the message “This is a test message” with severity of critical.

```
log send msg “This is a test message.” severity critical
```


Copyright© 2022 Ciena® Corporation

Procedure 9-2
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.

Step	Action
1	Reset the configuration and clear the log files: `log reset-to-factory-defaults` **—end—**

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Performance monitoring configuration

This chapter describes how to configure performance monitoring (PM). PM is an in-service, non-intrusive method of statistical data collection used for fault detection and troubleshooting.

PM is designed to monitor TDM statistics on the 3904, 3905, 3926, 3928, 5142, and 5160 systems. The number of PM instances depends on the device. These statistics are based on time intervals and data counts to determine transmission quality.

PM instances

Performance monitoring is established by creating PM instances. A PM instance is a configured measurement for monitoring an entity on an SAOS device. A PM instance can be auto-created or user-created. Auto-created PM instances are configured for monitoring logical ports, which can be physical or aggregated. User-created PM instances can be configured for the monitored entities listed in the Monitored entity mapped to PM profile table on page 10-2.

Monitored entities are associated with PM profiles. PM profiles define which statistics a particular PM instance collects.

Copyright© 2022 Ciena® Corporation

The Monitored entity mapped to PM profile table maps monitored entities to the PM profiles that each monitored entity supports.

Table 10-1
Monitored entity mapped to PM profile

Monitored entity	PM profile	Description
tdm-t1-port	tdmT1PortStats	May be associated with any PM instance with a monitored entity of TDM module port or TPoP T1 SFP, while the system is configured to be in ANSI mode.
tdm-e1-port	tdmE1PortStats	May be associated with any PM instance with a monitored entity of TDM module port or TPoP E1 SFP, while the system is configured to be in ETSI mode.
tdm-e3-port	tdmE3PortStats	May be associated with any PM instance with a monitored entity of a Combo TDM OC48 FRU E3 port, while the system is configured to be in ETSI mode.
tdm-pw	tdmPwStats	May be associated with a PM instance with a monitored entity of a tdm-pw.
tdm-ds3-port	tdmDs3PortStats	May be associated with a PM instance with a monitored entity of TDM DS3 SFP.
tdm-ocn-port	tdmOcnPortStats	May be associated with a PM instance with a monitored entity of TDM OC3/OC12, when the system is configured to be in ANSI mode.
tdm-stmn-port	tdmStmnPortStats	Maybe be associated with a PM instance with a monitored entity of STM1/STM4 SFP, when the system is in ETSI mode.
port	ExtendedTxRx	Provides counters to fulfill remote network monitoring (RMON) statistics requirements. Used by alert TCA and CRC discard-based alert TCA.
egress port queue group	QueueGroup	Counts packets for each queue of the default queue group which is instantiated on every egress port. Used by alert TCA and queue-based alert TCA.
queue group profile	QueueGroup	Counts packets for each queue of a custom queue group. Custom queue groups are defined by the network operator. Used by alert TCA and queue-based alert TCA.
rsvp-ingress	BasicTx	Counts total packets transmitted.

Copyright© 2022 Ciena® Corporation

Table 10-1
Monitored entity mapped to PM profile

Monitored entity	PM profile	Description
rsvp-ingress-unidir	BasicTx	Counts total packets transmitted. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-ingress-corout	BasicTxRx	Counts total packets transmitted, received, and dropped. Supported only on 3926, 3928, 3938vi, 3942, 5142 and 5160 platforms.
rsvp-egress	BasicRx	Counts total packets received and dropped. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-egress-unidir	BasicRx	Counts total packets received and dropped. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-egress-corout	BasicTxRx	Counts total packets transmitted, received, and dropped. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-transit	BasicTxRx	Counts total packets transmitted, received, and dropped. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-transit-unidir	BasicTxRx	Counts total packets transmitted, received, and dropped. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
rsvp-transit-corout	BasicTxRxBiDir	Counts total packets transmitted, received, and dropped on the forward and reverse paths of an MPLS corouted transit tunnel. Supported only on 3926, 3928, 3942, 5142 and 5160 platforms.
mpls-bgp-ingress	BasicTx	Counts total packets transmitted. Supported only on 3926 and 3928 platforms.
mpls-bgp-egress	BasicRx	Counts total packets received and dropped. Supported only on 3926 and 3928 platforms.
mpls-bgp-transit	BasicTxRx	Counts total packets transmitted, received, and dropped. Supported only on 3926 and 3928 platforms.

The counters and statistics in the PM profiles are held in PM bins, which are the counter holders for a specific time interval. For more information about PM bins, refer to “PM bins” on page 10-23.

Copyright© 2022 Ciena® Corporation

PM profiles

This section provides details for each PM profile. PM profiles are:

- "ExtendedTxRx" on page 10-4
- "QueueGroup" on page 10-5
- "BasicTxRx" on page 10-6
- "BasicTx" on page 10-7
- "BasicRx" on page 10-7
- "BasicTxRxBiDir" on page 10-8
- "TdmPortOpticalStats" on page 10-9

ExtendedTxRx

The ExtendedTxRx PM profile provides counters to fulfill RMON statistics requirements.

> ***Note:*** The ExtendedTxRx PM profile collects statistics based on ingress meters. if packets are dropped due to flood containment, they do not appear in the bin. The Rx bytes do not reflect dropped packets due to flood containment.

Statistics in the ExtendedTxRx PM profile are:

- RxPkts
- RxCrcErrorPkts
  - — Dropped frames due to CRC errors are monitored on a per port basis.
  - — Drops are monitored on a preconfigured absolute value
- RxLOutRangePkts
- RxMcastPkts
- RxBcastPkts
- UndersizePkts
- OversizePkts
- FragmentsPkts
- JabbersPkts
- RxPausePkts
- RxDiscardPkts
- 64OctsPkts
- 65To127OctsPkts
- 128To255OctsPkts

Copyright© 2022 Ciena® Corporation

- 256To511OctsPkts
- 512To1023OctsPkts
- 1024To1518OctsPkts
- TxBytes
- TxPkts
- TxBcastPkts
- TxMcastPkts
- TxUCastPkts
- TxExDeferPkts
- TxGiantPkts
- TxUnderRunPkts
- TxCrcErrorPkts
- TxLCheckErrorPkts
- TxLOutRangePkts
- TxPausePkts
- TX Bytes per Second
- TX Frames per Second
- RX Bytes per Second
- RX Frames per Second

QueueGroup

The QueueGroup PM profile statistics are collected for each queue of a queue group. There are 16 queues in a queue group.

Statistics in the QueueGroup PM profile are:

- Frames Enqueued
- Bytes Enqueued
- Frames Dropped
  - — Monitored per queue within a queue group.
  - — Absolute value is monitored (no differentiation between unicast and multicast packet drops).
- Bytes Dropped

Copyright© 2022 Ciena® Corporation

BasicTxRx

The BasicTxRx PM profile counts total packets transmitted, received, and dropped.

Note: The BasicTxRx PM profile collects statistics based on ingress meters. if packets are dropped due to flood containment, they do not appear in the bin.

This table lists statistics in the BasicTxRx PM profile.

Table 10-2
BasicTxRx PM profile

Counter	Notes
Total Tx Forwarded bytes	
Total Tx Forwarded frames	
Total Rx Accepted bytes	Ingress meter accepted
Total Rx Accepted frames	Ingress meter accepted
Total Rx Remarked bytes	Ingress meter remarked
Total Rx Remarked frames	Ingress meter remarked
Total Rx dropping bytes	Ingress meter dropped
Total Rx dropping frames	Ingress meter dropped
Tx Forwarded byte per second	Based on the time the bin was opened up to the current time
Tx Forwarded frame per second	Based on the time the bin was opened up to the current time
Rx Accepted byte per second	Based on the time the bin was opened up to the current time. This counter does not reflect dropped packets due to flood containment.
Rx Accepted frames per second	Based on the time the bin was opened up to the current time

Copyright© 2022 Ciena® Corporation

BasicTx

The BasicTx PM profile counts total packets transmitted. This applies to logical interfaces that support Tx only.

This table lists counters in the BasicTx PM profile.

Table 10-3
BasicTx PM profile

Counter	Size	Notes
Total Tx Forwarded bytes	U64	Ingress meter forwarded
Total Tx Forwarded frames	U64	Ingress meter forwarded
Tx Forwarded byte per second	U64	Based on the time the bin was opened up to the current time
Tx Forwarded frames per second	U64	Based on the time the bin was opened up to the current time

BasicRx

The BasicRx PM profile counts total packets received and dropped. The BasicRx PM profile applies only to ingress logical interfaces that support both Rx.

This table lists counters in the BasicRx PM profile.

Table 10-4
BasicRx PM profile

Counter	Size	Notes
Total Rx Accepted bytes	U64	Ingress meter accepted
Total Rx Accepted frames	U64	Ingress meter accepted
Total Rx Yellow bytes	U64	Ingress yellow (remarked yellow via ingress metering or rcos-mapped to yellow)
Total Rx Yellow frames	U64	Ingress yellow (remarked yellow via ingress metering or rcos-mapped to yellow)
Total Rx dropping bytes	U64	Ingress meter dropped
Total Rx dropping frames	U64	Ingress meter dropped
Rx Accepted byte per second	U64	Based on the time the bin was opened up to the current time
Rx Accepted frames per second	U64	Based on the time the bin was opened up to the current time

Copyright© 2022 Ciena® Corporation

BasicTxRxBiDir

The BasicTxRxBiDir PM profile counts total packets transmitted, received, and dropped on the forward and reverse paths of an MPLS corouted transit tunnel.

Statistics in the BasicTxRxBiDir PM profile are:

- FwdRxAcceptedBytes
- FwdRxAcceptedFrames
- FwdRxYellowBytes
- FwdRxYellowFrames
- FwdRxDroppedBytes
- FwdRxDroppedFrames
- FwdTxForwardedBytes
- FwdTxForwardedFrames
- FwdRxBytesPerSec
- FwdRxFramesPerSec
- FwdTxBytesPerSec
- FwdTxFramesPerSec
- RevRxAcceptedBytes
- RevRxAcceptedFrames
- RevRxYellowBytes
- RevRxYellowFrames
- RevRxDroppedBytes
- RevRxDroppedFrames
- RevTxForwardedBytes
- RevTxForwardedFrames
- RevRxBytesPerSec
- RevRxFramesPerSec
- RevTxBytesPerSec
- RevTxFramesPerSec

Copyright© 2022 Ciena® Corporation

TdmPortOpticalStats

The TdmPortOpticalStats PM profile can be associated with any PM Instance to monitor physical (optical) measurements of a Tdm port.

This table lists counters in the TdmPortOpticalStats PM profile.

Table 10-5
TdmPortOpticalStats PM profile

Counter	Size	Notes
laserBiasCurrent	float	Laser Bias Current value (uA)
laserBiasMin	float	Laser Bias Min value (uA)
laserBiasMax	float	Laser Bias Max value (uA)
laserBiasAvg	float	Laser Bias Average value (uA)
oprCurrent	float	Optical Power Receiver Current value (dbm)
oprNormalize	signed int16	Optical Power Receiver Normalize value (%)
oprMin	float	Optical Power Receiver Min value (dbm)
oprMax	float	Optical Power Receiver Max value (dbm)
oprAvg	float	Optical Power Receiver Average value (dbm)
optCurrent	float	Optical Power Transmitter Current value (dbm)
optNormalize	signed int16	Optical Power Transmitter Normalize value (%)
optMin	float	Optical Power Transmitter Min value (dbm)
optMax	float	Optical Power Transmitter Max value (dbm)
optAvg	float	Optical Power Transmitter Average value (dbm)

Copyright© 2022 Ciena® Corporation

This table lists the information that comprises a PM instance.

Table 10-6
Information for PM instances

Attribute		Description
PM Instance Name	pm-instance <pm-instance>	Specifies the name of the PM instance.
Monitored Entity	Valid monitored entities are listed in Table 10-1.	Specifies the physical or logical entity being monitored. ***Note:*** Required field. Cannot be changed after the PM instance is created.
PM Instance Type	instance-type <on-demand | proactive>	Specified during PM Instance creation. Valid values are: • Proactive: the PM instance runs for infinite duration • On-demand: the PM instance runs for infinite duration or runs within a specified period of time. The default value is on-demand.
PM Profile	profile-type <TdmPWStats>	Specifies the PM profile type associated with the PM instance. The profile type depends on the monitored entity. • For tdm-ansi-port, the profile-type is TdmAnsiPortStats. • For tdm-etsi-port, the profile-type is TdmEtsiPortStats. • For tdm-pw, the profile type is TdmPWStats. • For tdm-ocn-port, the profile type is tdmOcnPortStats. • For tdm-stmn-port, the profile type is tdmStmnPortStats. • For tdm-ds3-port, the profile type is tdmDs3PortStats.
Start Time	start-date <YYYY-MM-DD> start-time <HH:MM:SS>	Specifies the date and time to start collecting statistics. If no start time is specified, then the start time defaults to the current time. The time is referenced to the system timestamp and is either local or UTC.

Copyright© 2022 Ciena® Corporation

Table 10-6
Information for PM instances

Attribute		Description
Stop Time	end-date <YYY-MM-DD> end-time <HH:MM:SS>	Specifies the date and time to stop collecting statistics. If no end time is specified, then the PM instance is assumed to have an infinite duration. The time is referenced to the system timestamp and is either local or UTC.
Bin Count	bin-count <NUMBER: 0-96>	***Note:*** Required field. Cannot be changed after the PM instance is created. The number of history bins that are collected before rolling over. This field accepts a number between 0 and 96. A bin count of 0 implies a single collection bin for the specified duration.
Bin Duration	bin-duration <15m>	Specifies the duration of the bin. Currently only one 15-minute bin is supported.
Bin Alignment	alignment <local-clock | start time>	Specifies the bin time alignment, which defines the times at which the PM Mgr will populate the PM bins. Valid values are: • local-clock — The system aligns the measurement start time for each bin to the time-of-day, for example, for 15min, bins at :00, :15, :30, :45. The first PM bin may be marked 'partial'. Subsequent PM bins will be aligned to the system clock. For example, if the bin duration is 15 minutes and the PM instance is created at 4:11, the first PM bin will be marked as 'partial' and will last from 4:11 to 4:15. The remaining PM bins will measure 15-minutes and have timestamps aligned to every quarter hour. • start-time — The system will not attempt to align bins to the time-of-day. Bins start whenever the start-time engages the PM Instance. The default value is local-clock.

Copyright© 2022 Ciena® Corporation

Table 10-6
Information for PM instances

Attribute		Description
Monitored Entity Oper State	Not user-configured	Indicates the operational state of the monitored entity. This is a read-only field. The value of this field can be different from the operational state of the PM instance.
PM Instance Admin State	Not user-configured	Indicates the configured administrative state for the PM instance, which is one of enabled or disabled. Auto-created PM instances are created as Admin-enabled. User-created PM instances are created as Admin-enabled. You can set the administrative state of a PM Instance regardless of whether it is a user-created or an auto-created PM Instance.
PM Instance Oper State	Not user-configured	Indicates the operational state of the PM instance. This state depends on the configured state of PM globally, as well as the state of the PM instance. If PM is administratively enabled, the PM bins will continue to roll over, even if the monitored entity associated with the instance is disabled. If the entity being monitored goes down, PM remains enabled. However, PM will not poll statistics if the monitored entity state is down. PM will retrieve the statistics upon notification of a monitored entity being disabled so that those statistics are placed in the correct bin.

Copyright© 2022 Ciena® Corporation

Port performance management statistics

The tables in the following sections list telemetry:

- Table 10-7 lists port statistics collected for ANSI-mode ports on the 3926 16xT1/E1 FRU and on the 3926 3Gb TDM Combo FRU.
- Table 10-8 lists port statistics collected for ANSI-mode ports on TSOP and CEP transceivers.
- Table 10-9 lists port statistics collected for TPoP DS1 and CSoP OC3 ports in ANSI mode.
- Table 10-10 lists port statistics collected for ETSI-mode ports on the 3926 16xT1/E1 FRU and on the 3926 3Gb TDM Combo FRU.
- Table 10-11 lists port statistics collected for collected for ETSI-mode ports on TSOP and CEP transceivers
- Table 10-12 lists port statistics port statistics collected for TPoP DS1 and CSoP OC3 ports in ETSI mode.
- Table 10-13 lists the port statistics collected for E3 ports in ETSI mode.
- Table 10-14 lists telemetry for TDM CEM pseudowire/EVCs.

Port statistics

The following table lists the port statistics collected for ANSI-mode ports on the 3926 16xT1/E1 FRU and on the 3926 3Gb TDM Combo FRU.

Copyright© 2022 Ciena® Corporation

Table 10-7
Port statistics for ANSI-mode ports on 3926 16xT1/E1 FRU and on 3926 3Gb TDM Combo FRU

Statistics	Name	Trigger	3926 16xT1/E1 FRU	3926 3Gb TDM Combo FRU				
				DS1	DS3	OC3	OC12	OC48
ES	Line errored seconds	AIS-L, RDI, Line CV, DNR (See Note 1.)	Y	Y	Y	Y	Y	Y
	Section errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)				Y	Y	Y
	Path errored seconds	LOS, LOF, DNR (See Note 1.)		Y	Y			
SES	Line severely errored seconds	LOS, LOF, Line CV, DNR (See Note 1.)	Y	Y	Y	Y	Y	Y
	Section severely errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)				Y	Y	Y
	Path severely errored seconds	LOS, LOF, DNR (See Note 1.)		Y	Y			
LOSS	LOS seconds	LOS	Y	Y	Y	Y	Y	Y
AIS	AIS seconds	AIS				Y	Y	Y
SEFS	Severely errored frame seconds	LOF		Y		Y	Y	Y
SEF/AIS	Severely errored frame/ AIS seconds	AIS, SEF			Y			
UAS	Unavailable seconds	Consecutive ES/ SES for 10 sec. Also triggered by certain port alarms. (See Note 2.)	Y	Y	Y	Y	Y	Y
AS	Available seconds	Consecutive no ES/SES for 10 seconds	Y	Y	Y			
TT	Total time	UAS + AS	Y	Y	Y			
FC	Failure count	Number of switches between AS and UAS		Y	Y			
CV	Section code violation	Section CV count				Y	Y	Y
	Line code violation	Line CV count	Y	Y	Y	Y	Y	Y

Note 1: DNR stands for near-end device not reachable.

Note 2: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for ANSI-mode ports on CEP transceivers and TSOP transceivers.

Table 10-8
Port statistics for ANSI-mode ports on TSOP and CEP transceivers

Statistics	Name	Trigger	XCVR-CEP001/002/003			XCVR-TSOP01/02/03		
			OC3	OC12	DS3	OC3	OC12	OC48
ES	Line errored seconds	AIS (AIS-L,) RDI-L, Line CV, DNR (See Note 1.)	Y	Y	Y			
	P-bit errored seconds	LOS, LOF, DNR (See Note 1.)			Y			
	Section errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)	Y	Y				
SES	Line severely errored seconds	LOS, LOF, Line CV, DNR (See Note 1.)	Y	Y	Y			
	P-bit severely errored seconds	LOS, LOF, DNR (See Note 1.)			Y			
	Section severely errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)	Y	Y				
LOSS	LOS seconds	LOS	Y	Y	Y			
AIS	AIS seconds	AIS (AIS-L)	Y	Y				
SEFS	Severely errored frame seconds	LOF	Y	Y				
SEF/AIS	Severely errored frame/ AIS seconds	AIS, SEF			Y			
UAS	Unavailable seconds	Consecutive ES/ SES for 10 sec. Also triggered by certain port alarms. (See Note 2.)	Y	Y	Y			
UAS	Unavailable seconds	Consecutive LOS, LOF, AIS, or DNR for 10 seconds. Also triggered by certain port alarms. (See Note 2.)				Y	Y	Y
P-bit UAS	P-bit unavailable seconds	P-bit UAS count			Y			

Copyright© 2022 Ciena® Corporation

Table 10-8
Port statistics for ANSI-mode ports on TSOP and CEP transceivers

Statistics	Name	Trigger	XCVR-CEP001/002/003			XCVR-TSOP01/02/03		
			OC3	OC12	DS3	OC3	OC12	OC48
AS	Available seconds	Absence of 10 consecutive LOS, LOF, AIS, or DNR seconds				Y	Y	Y
TT	Total time	UAS + AS				Y	Y	Y
CV	Section code violation	Section CV count	Y	Y				
	Line code violation	Line CV count	Y	Y	Y			
	P-bit code violation	P-bit CV count			Y			

Note 1: DNR stands for near-end device not reachable.

Note 2: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for TPoP DS1 and CSoP OC3 ports in ANSI mode.

Table 10-9
Port statistics for ANSI-mode TPoP DS1 CSoP DS3 ports

Statistics	Name	Trigger	TPoP DS1 using XCVR-TDM4GE	CSoP OC3 using XCVR-GES101
ES	Line errored seconds	AIS (AIS-L), RDI-L, Line CV, DNR (See Note 1.)	Y	Y
	Section errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)		Y
SES	Line severely errored seconds	LOS, LOF, Line CV, DNR (See Note 1.)	Y	Y
	Section severely errored seconds	LOS, LOF, Section CV, DNR (See Note 1.)		Y
LOSS	LOS seconds	LOS	Y	Y
AIS	AIS seconds	AIS (AIS-L)		Y
SEFS	Severely errored frame seconds	LOF		Y
UAS	Unavailable seconds	Consecutive ES/SES for 10 sec. Also triggered by certain port alarms. (See Note 2.)	Y	Y
AS	Available seconds	Consecutive no ES/SES for 10 seconds	Y	
TT	Total time	UAS + AS	Y	
CV	Section code violation	Section CV count		Y
	Line code violation	Line CV count		Y

Note 1: DNR stands for near-end device not reachable.

Note 2: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for ETSI-mode ports on the 3926 16xT1/E1 FRU and on the 3926 3Gb TDM Combo FRU.

Table 10-10
Port statistics for ETSI-mode ports on 3926 16xT1/E1 FRU and on 3926 3Gb TDM Combo FRU

Statistics	Name	Trigger	3926 16xT1/E1 FRU	3926 3Gb TDM Combo FRU				
				E1	E3	STM1	STM4	STM16
EB	Errored blocks	Count of EBs above threshold	Y					
BBE	Background block errors	Count of EBs below threshold	Y					
ES	Errored seconds MS	LOS, LOF, AIS-MS, RDI-MS, DNR	Y	Y	Y	Y	Y	Y
SES	Severely errored seconds MS		Y	Y	Y	Y	Y	Y
UAS	Unavailable seconds MS	Amount of time ES or SES >= 10 consecutive seconds. Also triggered by certain port alarms. (See Note.)	Y	Y	Y	Y	Y	Y
AS	Available seconds MS	Amount of time ES or SES < 10 consecutive seconds	Y	Y	Y	Y	Y	Y
TT	Total time MS	UAS + AS	Y	Y	Y	Y	Y	Y
Note: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).								

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for collected for ETSI-mode ports on CEP transceivers and TSOP transceivers.

Table 10-11
Port statistics for ETSI-mode ports on TSOP and CEP transceivers

Statistics	Name	Trigger	XCVR-CEP001/002		XCVR-TSOP01/02/03		
			STM1	STM4	STM1	STM4	STM16
ES	Errored seconds MS	LOS, LOF, AIS-MS, RDI-MS, DNR	Y	Y			
SES	Severely errored seconds MS		Y	Y			
UAS	Unavailable seconds MS	Amount of time ES or SES >= 10 consecutive seconds. Also triggered by certain port alarms. (See Note.)	Y	Y			
UAS	Unavailable seconds MS	Consecutive LOS, LOF, AIS, or DNR for 10 seconds. Also triggered by certain port alarms. (See Note.)			Y	Y	Y
AS	Available seconds MS	Amount of time ES or SES < 10 consecutive seconds	Y	Y			
AS	Available seconds MS	Absence of 10 consecutive LOS, LOF, AIS, or DNR seconds			Y	Y	Y
TT	Total time MS	UAS + AS	Y	Y	Y	Y	Y
Note: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).							

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for TPoP E1 ports and for CSoP STM1 ports in ETSI mode.

Table 10-12
Port statistics for ETSI-mode TPoP E1 CSoP TM1 ports

Statistics	Name	Trigger	TPoP E1 using XCVR-TDM2GE	CSop STM1 using XCVR-GES101
ES	Errored seconds MS	LOS, LOF, AIS-MS, RDI-MS, DNR	Y	Y
SES	Severely errored seconds MS		Y	Y
UAS	Unavailable seconds MS	Amount of time ES or SES >= 10 consecutive seconds. Also triggered by certain port alarms. (See Note.)	Y	Y
AS	Available seconds MS	Amount of time ES or SES < 10 consecutive seconds	Y	Y
TT	Total time MS	UAS + AS	Y	Y
Note: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).				

Copyright© 2022 Ciena® Corporation

The following table lists the port statistics collected for E3 ports in ETSI mode.

Table 10-13
Port statistics for ETSI-mode E3 ports

Statistics	Name	Trigger	E3
L, ES	Errored seconds, line	LOS, LOF, AIS-L, RDI-L, DNR	Y
L, SES	Severely errored seconds line		Y
L, UAS	Unavailable seconds line	Amount of time ES or SES >= 10 consecutive seconds	Y
L, AS	Available seconds line	Amount of time ES or SES < 10 consecutive seconds	Y
L, TT	Total time line	L, UAS + L, AS	Y

Statistics for TDM CEM pseudowire/EVCs

The following statistics are supported on a TDM CEM pseudowire/EVC. Due to hardware differences, not all statistics are available on all hardware. TDM CEM pseudowire/EVC statistics are not dependent on ANSI or ETSI mode.

Copyright© 2022 Ciena® Corporation

Table 10-14
TDM CEM pseudowire/EVC statistics

Statistics	Name	Trigger	All TDM CEM pseudowire/EVCs
Missing	Count of missing packets	Detected by hardware based on sequence number.	Y
Reordered	Count of reordered packets	Detected by hardware based on sequence number.	Y
Misordered	Count of misordered packets	Detected by hardware based on sequence number.	Y
Malformed	Count of malformed packets	Detected by hardware based on packet header info./size of packet.	Y
Underrun	Count of jitter buffer underrun occurrences	Detected by hardware once jitter buffer becomes empty.	Y
Overrun	Count of jitter buffer overrun occurrences	Detected by hardware once jitter buffer becomes full.	Y
ES	Errored seconds		Y
SES	Severely errored seconds		Y
UAS	Unavailable seconds	Triggered by certain port alarms. (See Note 1.)	Y
LOPS	Loss of packets seconds		Y
L-bit	Count of L-bit packets	Count of packets received with L bit set in TDM CEM header.	Y (See Note 2.)
R-bit	Count of R-bit packets	Count of packets received with R bit set in TDM CEM header.	Y (See Note 2.)
Rx	Count of [ackets received	Counted byhardware.	Y
Tx	Count of packets transmitted	Counted by hardware.	Y

Note 1: UAS is triggered when any of the following port alarms is in effect: DINIT (Device Initialization), HT (High Temperature), DF (Device Failure), WDP (Wrong Device Present), NDF (No Device Found), MDF (Multiple Devices Found).

Note 2: The L-bit and R-bit statistics are supported only on the 3926 3Gb TDM Combo FRU. They are not supported on any other TDM CEM products.

Copyright© 2022 Ciena® Corporation

PM bins

PM bins are the counter holders for a specific time period (typically 15-minute intervals). This time interval is referred to as a sliding window because there is always a current bin that transitions to a historical bin.

Topics for PM bins are:

- "PM bin types" on page 10-23
- "PM bin states and PM bin state priority" on page 10-24

PM bin types

Statistics for the current interval are stored in the Current Bin. When the interval ends, the Current Bin is moved in to the first History Bin. This transition results in the following changes:

- The oldest History Bin is deleted.
- The identifier of all History Bins shift by one, that is, History Bin #1 becomes History Bin #2, and History Bin #2 becomes History Bin #3.
- The end-time of the Current Bin is set to the current time. However, if the reason for the bin expiration is due to a large system time change, the end time of the Current Bin is set to the system time immediately prior to the time change event.
- The Current Bin is placed into the latest History Bin (History Bin #1).
- If the PM instance is still in effect (end-time value has not been reached), a new Current Bin is started. The expected end time of the new bin will be the time configured by the bin-duration setting (default is 15 minutes).

Table 10-15 summarizes the PM bin types.

Table 10-15
PM bin types

Bin Type	Description
Current	Stores the statistics for the current statistics interval.
History	Store the statistics history. When the current bin duration time expires, the statistics from the current bin are placed in the next available history bin.
24HrCurrent	In a single bin that has a duration of 24 hours. When each Current bin is complete, the statistics from the Current bin are used to update the 24HrCurrent bin.

Copyright© 2022 Ciena® Corporation

Table 10-15
PM bin types (continued)

Bin Type	Description
24HrHistory	Is the rollover from the 24HrCurrent bin. When the 24-hour duration is up on the 24HrCurrent bin, the bin rolls over to the 24HrHistory bin and a new 24HrCurrent bin is started. There is only one 24HrHistory bin. For PM instances with bin alignment of local-clock, the rollover of 24HrCurrent into 24HrHistory happens at UTC midnight, regardless of any user-configured time-offset. For PM instances with bin-alignment of start-time, the rollover of 24HrCurrent into 24HrHistory happens every 24 hours after the initial start-time of the PM instance.
Statistics	Is a free-running PM bin which stores the running total of the statistics for the PM Instance for the entire time the PM Instance has been enabled, and since the PM Instance's statistics were last cleared. There is no particular period associated with the Statistics Bin as it continuously collects (and accumulates) the statistics for the PM Instance for as long as the PM Instance is operational. Every PM Instance has one Statistics Bin. You can clear this bin which will cause it to restart at zero (along with the Current Bin for the PM Instance).
Total Statistics	Records all statistics on the PM Instance regardless of whether the statistics have been cleared. This PM Bin may be useful for certain debugging or by other system calls which need to know about statistics of a monitored entity over its lifetime, without concern of whether a user had cleared the statistics. The user does not have the ability to clear this bin. Every PM Instance has one Total Statistics bin. This bin is used by RMON as the history bin.

PM bin states and PM bin state priority

Every PM bin that is collected will report a PM Bin State. The PM Bin State indicates the status of the PM bin and allows the user to determine the integrity of the bin data.

PM bin state priority provides a predictable and defined behavior when multiple events occur which would otherwise result in multiple possible states for a single PM Bin. PM bin state priority is one of the following:

- Not Valid state has the lowest priority and overwrites any other state.
- IDF has the highest priority and overwrites any other state.
- When multiple bin states occur, the state with the highest priority number overwrites the lower priority state.

Table 10-16 summarizes the PM bin states and provides the bin state priority.

Copyright© 2022 Ciena® Corporation

Table 10-16
PM bin states

PM Bin State	Priority	Description
Not Valid	1	The bin does not contain meaningful data. The PM bin has not yet been initialized. Examples include: • The Current Bin of a PM Instance when the PM Instance is operationally disabled or has not yet started collecting statistics • The 24HrCurrent Bin of a PM Instance which has not yet become operationally enabled • The 24HrHistory Bin of a PM Instance which has yet to receive the 24HrCurrent bin data • History Bins which have yet to receive data from Current Bin expirations
Valid	2	The bin contains valid data with no detected irregularities. For the Current Bin this state means the bin is presently accumulating statistics and no irregularities have been detected which would warrant a bin state other than Valid. For the 24HrCurrent Bin this state means that the bin contains a continuous set of collected data from the bin's start-time to present (if the PM Instance is operationally enabled) or from the bin's start time to the indicated end-time (if the PM instance had once gathered statistics but has now transitioned to operationally disabled). No irregularities were detected during the bins duration. For History Bins and for the 24HrHistory Bin this state indicates that the bin contains a continuous collection of statistics from the PM Instance's monitored entity for the period of time as indicated by the bin's start-time and end-time values. No irregularities were detected during the bins duration.
Time Change	3	The system time was changed after the bin had finished gathering statistics. See "Time changes" on page 10-29 for more information. This state is only applied to History Bins. When a History Bin has this state, it means that the start-time and end-time associated with the bin are not with respect to the current system time. The times are representative of a system time that was previously maintained on the device. As such, the actual times cannot be trusted since they are not representative of the actual moment in time which the data was collected, with respect to the current system time. ***Note:*** Time change can result from syncing with an NTP server or by user configuration of system time.

Copyright© 2022 Ciena® Corporation

Table 10-16
PM bin states (continued)

PM Bin State	Priority	Description
Overflow	4	PM detected that one or more statistics contained within the PM bin has experienced a rollover during the period of time that the PM bin represents. PM stores all counters in the form of unsigned 64-bit integers. This bin means that one of the statistics has increased past the decimal number 18,446,744,073,709,551,615. When this happens, the counter rolls back to 0 and continues to accumulate. This PM Bin state can occur on bins with duration of 24-hours since they periodically accumulate statistics during the course of the 24-hour period. As a result, the 24HrCurrent and 24HrHistory bins could report this overflow state.
Cleared	5	The bin represents data which was cleared (by the user) during the period that the bin represents. This state is applied to the Current Bin and the 24HrCurrent Bin when the user directs the system to clear that statistics for a particular PM Instance. As these bins are moved into their respective History Bin and 24HrHistory Bin then those bins will also reflect this state.

Copyright© 2022 Ciena® Corporation

Table 10-16
PM bin states (continued)

PM Bin State	Priority	Description
Partial	6	The bin contains incomplete or non-continuous measurement. Examples include: • The Current Bin is marked partial due to a time-change event. See "Time changes" on page 10-29 for more information. • The Current Bin is marked partial when its PM Instance is using local-clock bin alignment and the start-time applied to the bin is not that of an aligned moment in time. • The History Bins of a PM Instance will have a partial bin state for any Current Bins which had a partial state at the moment they were placed into History Bins. This will happen when, at the end of a measurement period, the total time of the Current Bin is found to be less than its PM Instance's configured bin-duration. For example, this could occur when a time-change event causes the Current Bin to be prematurely terminated. Another example is when a PM Instance is started which is configured to be aligned to the local-clock, and where the first Current Bin started in the middle of an aligned period and therefore has a duration less than expected. • The 24HrCurrent Bin will be marked partial when its PM Instance is using local-clock bin-alignment and the start-time applied to the bin is not that of a time aligned with midnight. • The 24HrHistory Bin will receive a partial state when it receives a 24HrCurrent Bin that was marked partial. • The Current Bin and 24HrCurrent Bins may be marked as partial when the underlying system experiences an error while attempting to retrieve the statistics. For example, immediately after bootup the system could try to retrieve TDM statistics, however that portion of the system is still being initialized and is unable to provide statistics. As a result the current bins will be marked partial. This partial PM bin state is the expected bin state for the Current and 24HrCurrent bins immediately after a system start. ***Note:*** If the bin-duration is less than 5 seconds short, the bin will be considered complete. If the bin-duration is greater than 5 seconds short, the bin will be marked as partial. This allows a small time buffer to account for factors such as CPU loading, clock accuracy and clock drift. Therefore, a 15-minute bin must be at least 14 minutes and 55 seconds in duration to be considered complete. A bin 14 minutes and 54 seconds in duration or shorter, will be marked as partial.

Copyright© 2022 Ciena® Corporation

Table 10-16
PM bin states (continued)

PM Bin State	Priority	Description
IDF	7	PM detected that the Invalid Data Flag (IDF) was set during the period of time which the PM Bin represents. The IDF has a specific meaning for the particular monitored entity. Typically this means that the monitored entity detected an abnormality with the monitored entity during the statistic collection interval. When PM Mgr receives statistics from a PM Instance's monitored entity, the monitored entity may also pass along an indicator if it had detected an IDF during the period of time which the requested statistics represent. If this indicator is received, then PM will set the Current Bins state to IDF. IDF can occur for PM Instances with the following PM Profiles: • tdmE1PortStats • tdmT1PortStats • tdmPwStats • tdmOcnPortStats • tdmStmnPortStats • tdmDs3PortStats

System time

The system displays the date/time based on the system setting 'timestamp'. The global setting allows the user to specify how time is displayed and can be one of:

- Local time — All time is displayed as local time.
- UTC — All time is displayed as UTC time.

  Note: When UTC time is configured, the displayed time will have a Z appended to the date/time. For example: Wed Jul 10 06:36:53 2013Z.

When you set the start-time, end-time, start-date and end-date of PM instances, the system interprets the time specified in the command based global timestamp setting. Therefore, if the system is set to local time, it is assumed that the time and date information specified in the PM instance creation is also in local time.

Internally the system keeps the time as UTC time. Therefore, switching from UTC to local time does not generally impact the bin collection.

Copyright© 2022 Ciena® Corporation

Note: If users retrieve a history bin with a 'Time Change' bin state, they should be aware that there was a time change. The time change may have modified the length of the bin, making it longer or shorter than the typical bin duration. Determining the actual bin duration will assist you with interpreting the data collected.

Time changes

Adjustments to system time can have an impact on the statistics process and may result in PM Bins being marked as Partial or Time Change. This section will discuss the various time change scenarios and the resulting impact on the PM Bin state.

Table 10-17
Time change scenarios

Time Change Event	System Behavior
Time adjusted forward by less than 60 seconds	Time was adjusted slightly but not enough to trigger the PM time-change logic. The bin duration is shorter than the specified interval and one of the following occurs: • If the bin is 14 minutes and 55 seconds or longer, the bin is considered complete and is marked Valid. • If the bin is 14 minutes and 54 seconds or shorter, the bin is marked Partial.
Time adjusted backward by less than 60 seconds	Time was adjusted slightly but not enough to trigger the PM time-change logic. The bin duration is slightly longer than the specified interval. The bin is considered complete and is marked Valid.
Time adjusted forward by more than 60 seconds	Time is adjusted forward by more than 60 seconds which is enough to trigger the time-change logic in the system. See Table 10-18 on page 10-30 for a summary of the changes that will occur.
Time adjusted backward by more than 60 seconds	Time is adjusted backward by more than 60 seconds which is enough to trigger the time-change logic in the system. See Table 10-18 on page 10-30 for a summary of the changes that will occur.

The time change logic is triggered when the system time is adjusted by more than 60 seconds. Table 10-18 on page 10-30 contains a summary of the adjustments that are made to the PM Instance when this occurs.

Copyright© 2022 Ciena® Corporation

Table 10-18
Time change logic

Parameter Being Adjusted	System Behavior
Adjustments to the PM Instance's start-time and end-time	If the start-time of the PM Instance was a time in the past, prior to the moment of the time-change event then: • The PM Instance's start-time is increased or decreased by the amount of the time change • The PM Instance's end-time is increased or decreased by the amount of the time change. Note that if the end-time is infinite, then no adjustment is required.
Adjustments to the PM Instance's 24HrCurrent PM Bin	The 24HrCurrent bin is updated as follows: • The start-time for the bin is increased or decreased by the amount of the time change • If the end-time is configured to be a specific end-time (such as when the PM Instance is operationally disabled, and as a result the PM Instance is ended), the end-time is increased or decreased by the amount of the time change. • If the 24HrCurrent Bin's cleared-time represents a particular time in which the 24HrCurrent bin had been cleared, then the cleared-time value is also increased or decreased by the amount of the time change.
Adjustments to the PM Instance's History Bins	The bin state of every History bin associated with the PM Instance is set to Time Change.
Adjustments to the PM Instance's Current Bin	If the PM instance is operationally enabled then the state of the Current bin is set to Partial. If the time was adjusted forward, and to a time after which the Current bin was expected to expire, or the time was adjusted backward, and to a time prior to the start-time of the Current bin then the following occurs: • The end-time of the Current bin is set to the system time immediately prior to the time-change event • The Current bin is moved into the History Bins of the PM Instance. • A new Current bin is started with a start-time of the new system time (after the time change event).

Copyright© 2022 Ciena® Corporation

Maximum PM instances

Table 10-19 describes the maximum number of PM instances supported on each device.

Table 10-19
Maximum PM instance summary

	Platforms			
Maximum PM instance summary	**5142 5160**	**3942**	**3903 3903x 3904 3905 3906**	**3926 3928**
Max PM Instances for auto-created with Class0 bins	48	52	20	24
Max PM Instances for auto-created with Class1 bins	23	0	3	23
Max PM Instances for user-created with Class0 bins	374	359	237	280
Max PM Instances for user-created with Class1 bins	5987	4032	287	3179
Max PM Instances Total with Class0 bins	422	411	257	304
Max PM Instances Total with Class1 bins	6010	4032	290	3202
PM Instances reserved for auto-created instances	71	52	23	47
PM instances available for user-created instances	6361	4391	524	3459
Max PM Instances Total	6432	4443	547	3506

PM configuration at system level

Performance Monitoring can be globally enabled/disabled. Table 10-20 summarizes the available PM global attributes.

Copyright© 2022 Ciena® Corporation

Table 10-20
PM global attributes

Attribute	RW	Value	Description
Admin State	RW	• Enable (default) • Disable	The administrative state of the PM service.
Oper State	R	• Enable • Disable	The operational state of the PM service.
persistence-interval	RW	<Seconds: 60-86400> Default = 900 seconds (15 min)	This value dictates how often the data is persisted to flash.

See "Configuring PM at the system level" on page 10-41 for a procedure.

PM Mgr persistence file

The PM Mgr will periodically save the PM History and 24HrHistory Bins to non-volatile memory at a user-configurable rate. This is the persistence-interval. When the persistence-interval expires, a binary data file is saved. The system saves this file to the on-board flash at /flash0/pm/pmHist.bin.

When the system reboots, the PM History binary data file is loaded, thus retaining PM history across reboots.

NTP

To ensure accurate time-stamping for performance monitoring, 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 1: For additional information regarding NTP, see *39XX/51XX Switches and Platforms Administration and Security*.

Note 2: Time changes resulting from NTP may impact the bin state of the PM Instances. See "System time" on page 10-28 for more information.

BulkStats collection

Statistics are collected in bulk format and transferred to a server for processing. These statistics are collected at a specified interval and stored in a file. Periodically, the file is securely transferred off the device by configuring bulkstats-instances and bulkstats-collectors. Bulkstats-instances define the actual statistics collections, and bulkstats-collectors define the nature of the statistics offloading.

Copyright© 2022 Ciena® Corporation

This type of data collection is analyzed for trends based on the collected statistical data. The data does not provide information on events, as these are provided by using events, syslog, traps, and alarms.

BulkStats-instance configuration

A bulkstats-instance is similar to a pm-instance as both contain a specific set of attributes defining the period of stats collection and the types of stats that are being collected at the end of each period. Unlike pm-instances, you can specify the desired statistics to be collected dynamically after the bulkstats-instances is created. The bulkstats-instance can then be associated with bulkstats-collector(s).

You can specify up to 16 bulkstats-instances. Each instance is configured to collect a set of statistics at a desired interval. Bulkstats-instances are aligned to the system clock.

Table 10-21 describes the attributes maintained by a bulkstats-instance.

Table 10-21
Bulkstats-instance attributes

Attribute	Format	Default	Description
Instance Name	String[1..31]	N/A	The bulkstats-instance name must be unique amongst all pm instances, bulkstats-instances, and bulkstats-collectors.
Instance ID	U32	N/A	Instance ID is a unique identifier used to identify the instance numerically. It is assigned by the system upon creation or it can be loaded in configuration by logical ID and may be represented with this number in the MIB. The Instance ID must be unique among all pm instances, bullkstats instances, and bulkstats-collectors.
Admin State	<enable | disable>	enable	Defines whether the bulkstats-instance is administratively enabled or disabled.
Oper State	<enable | disable>	N/A	Defines whether the bulkstats-instance is operationally enabled or disabled.

Copyright© 2022 Ciena® Corporation

Table 10-21
Bulkstats-instance attributes

Attribute	Format	Default	Description
Interval	<5m | 15m | 30m | 60m | 3h | 12h | 24h>	15m	Interval is a statistics collection period which allows you to choose the frequency of gathering statistics.
Duration	<DurationString> Allowing up to 1M (30 days)	8h	Duration defines the entire period of statistics history that is saved for this bulkstats-instance. A bulkstats-instance can define a duration of up to 1 month (30 days). This defines the amount of file history that the system retains for the bulkstats-instance. The system does not allow the configured duration to be less than the configured interval.
Statistics	<cpu | memory | fan | temp | power | logical-port | egress-port--queue-group | virtual-circuit | qos-flow | mpls-vc | mpls-lsp>	None, empty list	Defines the statistics that are gathered for this instance. The statistics can be any mix of supported statistics. The CLI supports comma-separated listing where you can specify any mix of statistics to add to the bulkstats-instance.

When you create a bulkstats-instance, you can specify all necessary configuration in a single command and define the entire instance. Certain attributes can be subsequently modified to allow you to change the bulkstats-instance after it is created. These attributes are described in Table 10-22.

Table 10-22
Adjustable attributes after bulkstats-instance creation

Attribute	Description
Admin State	Administratively enable or disable the bulkstats-instance. This is similar to enabling or disabling a pm instance.
Statistics	Add or remove statistics to a bulkstats-instance which allows you to refine the data that is collected in subsequent statistics collections on behalf of the bulkstats-instance.

Copyright© 2022 Ciena® Corporation

BulkStats-collector configuration

A bullkstats-collector is a set of attributes that defines where to send statistics, and an interval to define the frequency that the statistics are sent. You can specify up to 16 bulkstats-collectors. Each bulkstats-collector saves the data to a file. The file contains total statistics values for each statistics collected. It does not contain delta information. This file is saved in binary format and compressed so that the transfer time is minimized and the storage is small. The bulkstats-collector can be associated with multiple bulkstats-instances which define the particular set(s) of statistics that are sent to the specified destination at the specified frequency.

A bulkstats-instance can define a duration period of up to 1 M (30 days). This defines the amount of file history that the system retains for the bulkstats-instance.

You can configure the device to automatically push the statistics files using SFTP. These files are pushed immediately after collection based on their collection interval. You can specify where and how the file gets transferred through the xftpParams settings of the bulkstats-collector. The transfer occurs when the bulkstats-collector's upload-interval elapses. The applicable statistics are then sent in a file. The file transfer does not occur immediately after the bulkstats-instances have gathered their statistics.

File transfers are not aligned to the system clock to reduce network congestion. You cannot configure the alignment.

Copyright© 2022 Ciena® Corporation

A bulkstats-collector maintains the following attributes as shown in Table 10-23.

Table 10-23
BulkStats-collector attributes

Attribute	Format	Default	Description
Collector Name	String[1..31]	N/A	The bulkstats-collector name must be unique amongst all pm instances, bulkstats-instances, and bulkstats-collectors.
Instance ID	U32	N/A	Instance ID is a unique identifier used to identify the instance numerically. It is assigned by the system upon creation or it can be loaded in configuration by logical ID and may be represented with this number in the MIB. The Instance ID must be unique among all pm instances, bullkstats instances, and bulkstats-collectors.
Admin State	<enable | disable>	enable	Defines whether the bulkstats-collector is administratively enabled or disabled.
Oper State	<enable | disable>	N/A	Defines whether the bulkstats-collector is operationally enabled or disabled.
Push Interval	<DurationString> Allowing 1 hour to 365d	1h	Defines the stats-transmission period and allows you to choose how often frequency the statistics file is transmitted.
bulkstats-instance(s)	<bulkstatsInstance List>	None, empty list	Defines the bulkstats-instances that are included with each file transmission.
Xftp Parameters	Standard xfp configuration	None, no server specified.	Includes tftp-server, ftp-server, sftp-server, xftp-server ipv4/ipv6/hostname, default-tftp-server, default-ftp-server, default-sfp-server, default-server, and login-id/password entry for ftp and sftp server.

Copyright© 2022 Ciena® Corporation

When you create a bulkstats-collector, you can specify all necessary configuration in a single command and define the entire instance. Certain attributes can be subsequently modified to allow you to change the bulkstats-instance after it is created. These attributes are described in Table 10-24.

Table 10-24
Adjustable attributes after bulkstats-collector creation

Attribute	Description
Admin State	Administratively enable or disable the bulkstats-instance. This is similar to enabling or disabling a pm instance.
bulkstats-instance(s)	Add or remove bulkstats-instances from the bulkstats-collector, affecting the next file transfer that occurs on behalf of the bulkstats-collector.
Xftp Parameters	Set the destination file server information after the bulkstats-collector is created. The next regularly scheduled file transfer will use the new settings.
Remote File Prefix	Set the remote file prefix string after the bulkstats-collector has been created. The next regularly scheduled file transfer will use the new settings.

BulkStats file

Bulkstats files are written to the RAM disk. The file format is a Ciena proprietary binary file and it will need to be decoded by another Ciena provided application. The bulkstats manager performs checks to ensure that there is space on the RAM disk, and that the current bulkstats files do not take up more room than a predetermined percentage. When either of these conditions occurs, the device generates an event and removes the oldest files from each bulkstats-instance until the device is no longer in this condition. When the file is transfered to the server, all requested files (instances) that have not been sent to the server are sent.

IP address selection rules

To populate the IP address in the remote BulkStats file and name the file, the following cases are taken into consideration:

- If a preferred-source-ip is set in the XFTP manager (module), the preferred-source-ip interface has priority and its IP address is populated in the remote file.

Copyright© 2022 Ciena® Corporation

- If a preferred-source-ip is not set, check the device for a management interface. The management interface can be either a local or a remote interface and the IP address of the management interface should be populated in the remote file. When both local and remote interfaces are present, the local interface has priority.
- If both of the previous cases fail, the routing table is used to get the interface IP connected to the network of the configured XFTP server.
- If all of the previous cases fail, the IP address is populated as 0.0.0.0 in the file.

PM threshold crossing alerts

Performance monitoring (PM) threshold crossing alerts are used by service providers to set thresholds for, and to report performance data for early detection of problems. Using interval profiles, PM thresholds are configured PM on an LSP tunnel to support automatic bandwidth adjustment for MPLS-TE LSP tunnels.

Table 10-25 lists PM threshold attributes.

Table 10-25
PM threshold attributes

Attributes	Description
Sample interval	The period of time when statistics are sampled.
Sample or Current Sample	A collection of statistics taken at the end of each Sample Interval.
Adjustment TCA	A threshold has been crossed and an adjustment should be made.
Remote File Prefix	The remote file prefix is set after the bulkstats-collector is created. The next regularly scheduled file transfer will use the new settings.
Adjustment Interval	Time interval at which it is determined whether to adjust the LSP bandwidth.
Adjustment Threshold	A percentage or an actual value. The formula is: DIFF (Maximum Average Bandwidth, current LSP BW) >= Adjustment-Threshold then LSP is resized to Adjusted Bandwidth. Value used to derive the Sample values that are subject to causing an Adjustment TCA.

Copyright© 2022 Ciena® Corporation

Table 10-25
PM threshold attributes

Attributes	Description
Adjustment Basis	Base value against which the Adjustment Threshold is applied to determine values that trigger Adjustment TCA.
Adjustment High Watermark	Largest sample value found during an Adjustment Interval.
Adjustment Basis Minimum	Lowest value the Adjustment Basis will reach.
Adjustment Basis Maximum	Highest value the Adjustment Basis will reach.
Overflow Threshold	Value compared to Adjustment Basis triggering an overflow condition. User configurable and used to check if bandwidth usage is rapidly increasing.
Overflow Count	Number of consecutive overflow conditions to trigger an Adjustment TCA.
Overflow Current Count	Current number of consecutive overflow conditions that have occurred.
Overflow High Watermark	Highest sample value recorded during a set of Overflow Count samples.
Underflow Threshold	Value compared to Adjustment Basis triggering an underflow condition.
Underflow Count	Number of consecutive underflow conditions to trigger an Adjustment TCA.
Underflow Current Count	Current number of consecutive underflow conditions that have occurred.
Underflow High Watermark	Highest sample value recorded during a set of Underflow Count samples.
Alert TCA	A threshold has been crossed.
Alert Interval	Period of time consisting of one or more Sample Intervals at which an Alert TCA might be generated.

Copyright© 2022 Ciena® Corporation

Table 10-25
PM threshold attributes

Attributes	Description
Alert Threshold	Value used to derive the Sample values that are subject to causing an Alert TCA.
Alert Basis	Base value against which the Alert Threshold is applied to determine values that trigger Alert TCA.
Alert High Watermark	Largest sample value found during an Alert Interval.
Queue	The queue within a queue group. The queue index can only be configured by the “pm interval-profile set” command and can only be associated with the queue-drop TCA profile.
Alert Boundary	The boundary value per queue within a queue group. Can only be configured in the “pm interval-profile set” command and can only be associated with the queue-drop TCA profile.
CRC Alert Boundary	Boundary value for drop frames due to CRC errors. Can only be associated with the crc-drop TCA profile.
Profile	The basic profile is used for monitoring thresholds. The queue-drop profile monitors packet drops per queue of the egress port queue group. The crc-drop profile monitors Rx frames dropped due to CRC errors on a port. Cannot be changed after the PM instance is created. Default is basic.

Copyright© 2022 Ciena® Corporation

Procedure 10-1
Configuring PM at the system level

PM can be enabled or disabled at the system level. See “PM configuration at system level” on page 10-31 for more information.

If PM is enabled globally, the user also has the ability to enable or disable a specific PM instance. See “Enabling/disabling PM for a specific PM instance” on page 10-46 for a procedure.

> ***Note:*** See “Displaying PM instances” on page 10-49 for assistance displaying the PM configuration and data.

Step	Action

To enable PM globally - Enable PM

```
pm enable
```

To disable PM globally

1 Disable PM:

```
pm disable
```

To set the persistence interval at which PM instance history bins are saved to the designated flash location

2 Set the persistence interval (in seconds):

```
pm set persistence-interval <60-86400>
```

To set the persistence interval to the system default value of 900 seconds

3 Set the persistence interval to the system default:

```
pm unset persistence-interval
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-2
Creating a PM instance

You can create PM instances for many different types of SAOS monitored entities. See Table 10-1 for the complete list. See "Information for PM instances" on page 10-10 for an overview of the items that can be specified when you create a PM instance.

Note: See "Displaying PM instances" on page 10-49 for assistance displaying the PM configuration and data.

Step	Action

To create a PM Instance for a TDM port

1 Create a PM instance for a TDM port:

```
pm create tdm-port <port name> pm-instance <pm-instance>
[alignment <local-clock>][bin-count <0-96>] [bin-
duration <15m>][end-date <YYYY-MM-DD>][end-time
<HH:MM:SS>][instance-type <proactive | on-
demand>][profile-type <TdmAnsiPortStats |
TdmEtsiPortStats>] [start-date <YYYY-MM-DD>][start-time
<HH:MM:SS>]
```

where

tdm-port <port name>	Specifies the name of the port being monitored.
pm-instance <pm-instance>	Specifies the name of the PM instance
alignment <local-clock>	Defines how the start times of the measurement bins will be aligned. Defaults to local-clock and cannot be changed.
bin-count <0-96>	Defines the number of history bins used by the PM instance.
bin-duration <15m>	Sets the bin-duration. Defaults to 15 minutes. The default setting is the only value supported at this time.
end-date <YYYY-MM-DD>	Used for on-demand PM instances to set the end-date. ***Note:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.

Copyright© 2022 Ciena® Corporation

where

end-time <HH:MM:SS>	Used for on-demand PM instances to set the end-time. ***Note 1:*** If an end-date is entered but no end-time is specified, the default value of 23:59:59 will be used. ***Note 2:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.
instance-type <proactive | on-demand>	Defines the PM instance as proactive or on-demand. ***Note:*** When proactive is selected, the PM instance is of infinite duration. Any start/end time and start/end date specified in the creation command will be ignored.
profile-type <TdmAnsiPortStats | TdmEtsiPortStats>	Allows you to create either an ANSI or ETSI profile. ***Note:*** The system will block the creation of profiles that do not match the configured global ANSI/ETSI mode configuration. For example, if the system is in ANSI mode, then ETSI profiles will be blocked.
start-date <YYYY-MM-DD>	Used for on-demand PM instances to set the start-date. ***Note:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.
start-time <HH:MM:SS>	Used for on-demand PM instances to set the start time. ***Note 1:*** If a start-date is entered but no start-time is specified, the default value of 00:00:00 will be used. ***Note 2:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.

To create a PM Instance for a TDM VC

2 Create a PM instance for a TDM VC:

```
pm create tdm-vc <tdm-vc> pm-instance <pm-instance>
[alignment <local-clock>][bin-count <0-96>][bin-duration
<15m>][end-date <YYYY-MM-DD>][end-time
<HH:MM:SS>][instance-type <proactive|on-
demand>][profile-type <TdmPwStats>] [start-date <YYYY-
MM-DD>][start-time <HH:MM:SS>]
```


Copyright© 2022 Ciena® Corporation

where

tdm-vc <tdm-vc>	Specifies the name of the TDM VC being monitored.
pm-instance <pm-instance>	Specifies the name of the PM instance
alignment <local-clock>	Defines how the start times of the measurement bins will be aligned. Defaults to local-clock and cannot be changed.
bin-count <0-96>	Defines the number of history bins used by the PM instance. Default is 32.
bin-duration <15m>	Sets the bin-duration. Defaults to 15 minutes. The default setting is the only value supported at this time.
end-date <YYYY-MM-DD>	Used for on-demand PM instances to set the end-date. ***Note:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.
end-time <HH:MM:SS>	Used for on-demand PM instances to set the end-time. ***Note 1:*** If an end-date is entered but no end-time is specified, the default value of 23:59:59 will be used. ***Note 2:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.
instance-type <proactive | on-demand>	Defines the PM instance as proactive or on-demand. Default setting is on-demand. ***Note:*** When proactive is selected, the PM instance is of infinite duration. Any start/end time and start/end date specified in the creation command will be ignored.
profile-type <TdmPwStats>	Creates a profile to monitor a TDM pseudowire connection.
start-date <YYYY-MM-DD>	Used for on-demand PM instances to set the start-date. ***Note:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.
start-time <HH:MM:SS>	Used for on-demand PM instances to set the start time. ***Note 1:*** If a start-date is entered but no start-time is specified, the default value of 00:00:00 will be used. ***Note 2:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example creates a PM instance called pm01 to monitor port tdm01. The PM instance is on-demand, with start and end times specified.

```
pm create tdm-port tdm01 pm-instance pm01 end-time 7:38
instance-type on-demand profile-type TdmAnsiPortStats start-
time 7:35
```

The following example creates a PM instance called pm04 to monitor port tdm01. The PM instance is proactive and therefore is infinite in duration. The PM instance has 96 bins, 15 minutes each defined and the bins will be aligned to the local clock.

```
> pm create tdm-port tdm01 pm-instance pm04 alignment local-
clock bin-count 96 bin-duration 15m profile-type
TdmAnsiPortStats instance-type proactive
```


Copyright© 2022 Ciena® Corporation

Procedure 10-3
Enabling/disabling PM for a specific PM instance

PM can be enabled or disabled at the system level and at the PM instance level. For PM to be collected, both the system level and instance level must be enabled. See "Configuring PM at the system level" on page 10-41 for more information.

Note: See "Displaying PM instances" on page 10-49 for assistance displaying the PM configuration and data.

Step	Action

To enable PM for a particular instance

1 Enable PM for a specified instance:

```
pm enable pm-instance <instance-name>
```

where

pm-instance <instance-name>	Specifies the name of the PM instance

To disable PM for a particular instance

2 Disable PM for a specified instance:

```
pm disable pm-instance <instance-name>
```

where

pm-instance <instance-name>	Specifies the name of the PM instance

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-4
Deleting a specific PM instance

You can delete a PM instance. Alternatively, you can disable the PM instance. See “Enabling/disabling PM for a specific PM instance” on page 10-46 for more information.

Note: See “Displaying PM instances” on page 10-49 for assistance displaying the PM configuration and data.

Step	Action
1	Delete a specified PM instance: `pm delete pm-instance <instance-name>` where pm-instance <instance-name> Specifies the name of the PM instance

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-5
Clearing the statistics for a specific PM instance

You can clear the statistics for a PM instance.

Note: See "Displaying PM instances" on page 10-49 for assistance displaying the PM configuration and data.

Step	Action
1	Clear the statistics of a specified PM instance: `pm clear pm-instance <pm-instance>` where pm-instance <pm-instance> Specifies the name of the PM instance

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-6
Displaying PM instances

There are a number of different show commands available to display the PM instances and configuration information in the system.

Step	Action

To display all the configured PM instances

1 Display all the PM instances:

```
pm show
```

To display only user-created PM instances

2 Display user-created PM instances:

```
pm show user-created
```

To display only auto-created PM instances

3 Display auto-created PM instances:

```
pm show auto-created
```

To display the persistence settings related to PM

4 Display persistence settings for PM:

```
pm show persistence
```

To display all the details of a specific PM instance

5 Display details of a PM instance, including the current bins:

```
pm show pm-instance <pm-instance>
```

where

pm-instance <pm-instance> — Specifies the name of the PM instance

To display a filtered view of a specific PM instance

6 Display a filtered view of a PM instance, including the current bins:

```
pm show [pm-instance <pm-instance>] [24hr-history]
[active] [count <number>] [delay < 1-86400 >] [display
<clear|scroll> [scale <tera|giga| mega|kilo|none>]
[throughput | total-statistics | history | bin-number <1-
96>] [from-date <YYYY-MM-DD> | to-date <YYYY-MM-DD> |
from-time <HH:MM:SS> | to-time <HH:MM:SS>]
```


Copyright© 2022 Ciena® Corporation

where	
pm-instance <instance-name>	Specifies the name of the PM instance
24hr-history	Displays the last 24hr statistics.
[active]	Displays only statistics that are non-zero over the given interval.
count <number>	Specifies the number of times to repeat the show command. Default count number is 1. A count setting of 0 sets an infinite display and must be broken with 'ctrl-c'.
delay <1-86400>	Sets the delay interval between count repeats. The delay is specified in seconds and defaults to 5. Delay is only configurable when a count has been specified.
display < clear | scroll >	Specifies whether the console will clear the display prior to showing PM instance data. The default value is scroll.
scale < tera | giga | mega | kilo | none >	Specifies the scale of the statistics. Defaults are as follows: none for non-throughput statistics and mega for throughput statistics.
throughput | total-statistics | history | bin-number <1-96>	Throughput shows the PM instances throughput for each statistic since the last query. Total-statistics shows the total statistics for PM instances since system boot-up or statistic creation. History shows the details of a PM instance, including current and history bins. Bin-number shows the specified history bin for the PM instance.
from-date <date> | to-date <date> | from-time <time> | to-time <time>	Shows the PM instance plus all history bins collected in the specified date/time range specified. If a from-date is entered, but no from-time is specified, the from-time defaults to 00:00:00. If a to-date is entered, but no to-time is specified, the to-time defaults to 23:59:59. ***Note:*** Date/time entered are interpreted based on the system timestamp setting. If timestamp is set to local, then the time entered is assumed to be local time. If it is set to UTC, then the time entered is assumed to be UTC.

To display the details of a specific PM instance, including the current bins

7 Display the details of a PM instance, including the current bins:

```
pm monitor [pm-instance <pm-instance>] [active] [count
<number>] [delay < 1-86400 >] [display < clear|scroll >
[scale <tera|giga|mega|kilo|none>] [throughput | total-
statistics]
```


Copyright© 2022 Ciena® Corporation

where	
pm-instance <pm-instance>	Specifies the name of the PM instance
[active]	Displays only statistics that are non-zero over the given interval.
count <number>	Specifies the number of times to repeat the show command. Default count number is 0 and sets an infinite display and must be broken with 'ctrl-c'.
delay <1-86400>	Sets the delay interval between count repeats. The delay is specified in seconds and defaults to 5.
display < clear | scroll >	Specifies whether the console will clear the display prior to showing PM instance data. The default value is clear.
scale < tera | giga | mega | kilo | none >	Specifies the scale of the statistics. Defaults are as follows: none for non-throughput statistics and mega for throughput statistics.
throughput | total-statistics	Throughput shows the PM instances throughput for each statistic since the last query. Total-statistics shows the total statistics for PM instances since system boot-up or statistic creation.

—end—

Example

This example shows the user created instances in the system.

```
pm show user-created
```

```
+--------------------------------- USER CREATED PM INSTANCES ----------------------------------+
|                        |  Admin   |  Oper    | Instance  |Attached Interface        |Bin   |Bin      |
| Instance Name          |  State   |  State   | Type      | Type             | Name  |Count |Duration |
+------------------------+----------+----------+-----------+------------------+-------+------+---------+
| pm01                   | Enabled  | Enabled  | On Demand | tdm-port         | tdm01 | 32   | 15 min  |
| pm02                   | Enabled  | Enabled  | On Demand | tdm-port         | tdm01 | 32   | 15 min  |
| pm03                   | Enabled  | Enabled  | On Demand | tdm-port         | tdm01 | 5    | 15 min  |
| pm04                   | Enabled  | Enabled  | Proactive | tdm-port         | tdm01 | 96   | 15 min  |
| pm05                   | Enabled  | Enabled  | On Demand | tdm-port         | tdm01 | 32   | 15 min  |
+------------------------+----------+----------+-----------+------------------+-------+------+---------+
```

This example shows the auto-created instance for TDM port tdm01.

```
pm show pm-instance tdm01
```

```
+---------------------- PERFORMANCE MONITORING INSTANCE -------------------------+
| Parameter                       | Value                                       |
+---------------------------------+---------------------------------------------+
| Instance Name                   | tdm01                                       |
| Instance ID                     | 201                                         |
| Configuration Mode              | auto-created                                |
| Alignment                       | local-clock                                 |
| Instance Type                   | Proactive                                   |
| Attached Interface Type         | tdm-port                                    |
| Attached Interface Name         | tdm01                                       |
| Attached Interface Oper State   | Disabled                                    |
| Profile Type                    | TdmAnsiPortStats                            |
```


Copyright© 2022 Ciena® Corporation

```
| Current Bin ID                  | 28                                          |
| Collection Start Date/Time      | Thu Jan 28 21:06:20 2016                    |
| Collection End Date/Time        | No end time                                 |
| Configured Bin Count            | 32                                          |
| Configured Bin Duration         | 15 min                                      |
| Admin State                     | Enabled                                     |
| Oper State                      | Enabled                                     |
+---------------------------------+---------------------------------------------+

+---------------------------------+---------------------------------------------+
| Parameter                       | Value                                       |
+---------------------------------+---------------------------------------------+
| Instance Name                   | tdm01                                       |
| Profile Type                    | TdmAnsiPortStats                            |
| Bin                             | Current bin                                 |
| Collection Start Date/Time      | Wed Feb 03 15:45:03 2016                    |
| Bin State                       | IDF                                         |
+---------------------------------+---------------------------------------------+
| Statistic                       | Value                                       |
+---------------------------------+---------------------------------------------+
|    Line, Code Violations        |                                           0 |
|    Line, Errored Seconds        |                                           0 |
|    Line, Severely Errored Secs  |                                           0 |
|    Line, Loss of Signal Secs    |                                           0 |
|    Path, Code Violations        |                                           0 |
|    Path, Errored Seconds        |                                           0 |
|    Path, Severely Errored Secs  |                                           0 |
|    Path, Unavailable Seconds    |                                           0 |
|    Path, SES/AIS Seconds        |                                           0 |
|    Path, Failure Count          |                                           0 |
|    Path, Available Seconds      |                                           0 |
|    Path, Total Time Seconds     |                                           0 |
+---------------------------------+---------------------------------------------+

+---------------------------------+---------------------------------------------+
| Parameter                       | Value                                       |
+---------------------------------+---------------------------------------------+
| Instance Name                   | tdm01                                       |
| Profile Type                    | TdmAnsiPortStats                            |
| Bin                             | Current 24 hour bin                         |
| Collection Start Date/Time      | Wed Feb 03 00:00:02 2016                    |
| Bin State                       | IDF                                         |
+---------------------------------+---------------------------------------------+
| Statistic                       | Value                                       |
+---------------------------------+---------------------------------------------+
|    Line, Code Violations        |                                           0 |
|    Line, Errored Seconds        |                                           0 |
|    Line, Severely Errored Secs  |                                           0 |
|    Line, Loss of Signal Secs    |                                           0 |
|    Path, Code Violations        |                                           0 |
|    Path, Errored Seconds        |                                           0 |
|    Path, Severely Errored Secs  |                                           0 |
|    Path, Unavailable Seconds    |                                           0 |
|    Path, SES/AIS Seconds        |                                           0 |
|    Path, Failure Count          |                                           0 |
|    Path, Available Seconds      |                                           0 |
|    Path, Total Time Seconds     |                                           0 |
+---------------------------------+---------------------------------------------+
```

This example shows the auto-created instance for SFP TDM port po4.

```
pm show pm-instance po4

+--------------------- PERFORMANCE MONITORING INSTANCE -------------------------+
| Parameter                       | Value                                       |
+---------------------------------+---------------------------------------------+
| Instance Name                   | po4                                         |
| Instance ID                     | 220                                         |
| Configuration Mode              | auto-created                                |
| Alignment                       | local-clock                                 |
| Instance Type                   | Proactive                                   |
| Attached Interface Type         | tdm-port                                    |
| Attached Interface Name         | po4                                         |
```


Copyright© 2022 Ciena® Corporation

```
| Attached Interface Oper State   | Disabled                                  |
| Profile Type                    | TdmAnsiPortStats                          |
| Current Bin ID                  | 16                                        |
| Collection Start Date/Time      | Thu Jan 28 23:24:07 2016                  |
| Collection End Date/Time        | No end time                               |
| Configured Bin Count            | 32                                        |
| Configured Bin Duration         | 15 min                                    |
| Admin State                     | Enabled                                   |
| Oper State                      | Enabled                                   |
+---------------------------------+-------------------------------------------+

+---------------------------------+-------------------------------------------+
| Parameter                       | Value                                     |
+---------------------------------+-------------------------------------------+
| Instance Name                   | po4                                       |
| Profile Type                    | TdmAnsiPortStats                          |
| Bin                             | Current bin                               |
| Collection Start Date/Time      | Wed Feb 03 15:00:03 2016                  |
| Bin State                       | Valid                                     |
+---------------------------------+-------------------------------------------+
| Statistic                       | Value                                     |
+---------------------------------+-------------------------------------------+
|    Section, Code Violations     |                                         0 |
|    Section, LOS Seconds         |                                         0 |
|    Section, Errored Seconds     |                                       423 |
|    Section, SES                 |                                       423 |
|    Section, SEFS                |                                         0 |
|    Line, Code Violations        |                                         0 |
|    Line, AIS Seconds            |                                         0 |
|    Line, Errored Seconds        |                                       423 |
|    Line, Severely Errored Secs  |                                       423 |
|    Line, Unavailable Seconds    |                                       423 |
+---------------------------------+-------------------------------------------+

+---------------------------------+-------------------------------------------+
| Parameter                       | Value                                     |
+---------------------------------+-------------------------------------------+
| Instance Name                   | po4                                       |
| Profile Type                    | TdmAnsiPortStats                          |
| Bin                             | Current 24 hour bin                       |
| Collection Start Date/Time      | Wed Feb 03 00:00:04 2016                  |
| Bin State                       | Valid                                     |
+---------------------------------+-------------------------------------------+
| Statistic                       | Value                                     |
+---------------------------------+-------------------------------------------+
|    Section, Code Violations     |                                         0 |
|    Section, LOS Seconds         |                                         0 |
|    Section, Errored Seconds     |                                    54,423 |
|    Section, SES                 |                                    54,423 |
|    Section, SEFS                |                                         0 |
|    Line, Code Violations        |                                         0 |
|    Line, AIS Seconds            |                                         0 |
|    Line, Errored Seconds        |                                    54,423 |
|    Line, Severely Errored Secs  |                                    54,423 |
|    Line, Unavailable Seconds    |                                    54,423 |
+---------------------------------+-------------------------------------------+
```

This example shows 24hr history for pm instance “1”.

```
pm show pm-instance 1 24hr-history

+---------------------- PERFORMANCE MONITORING INSTANCE ----------------------+
| Parameter                       | Value                                     |
+---------------------------------+-------------------------------------------+
| Instance Name                   | 1                                         |
| Instance ID                     | 1000001                                   |
| Configuration Mode              | auto-created                              |
| Alignment                       | local-clock                               |
| Instance Type                   | Proactive                                 |
| Attached Interface Type         | Port                                      |
| Attached Interface Name         | 1                                         |
```


Copyright© 2022 Ciena® Corporation

```
| Attached Interface Oper State    | Disabled                                 |
| Profile Type                     | ExtendedTxRx                             |
| Current Bin ID                   | 28                                       |
| Collection Start Date/Time       | Mon Apr 15 03:19:34 2019                 |
| Collection End Date/Time         | No end time                              |
| Configured Bin Count             | 32                                       |
| Configured Bin Duration          | 15 min                                   |
| Interval Profile                 | <none>                                   |
| Admin State                      | Enabled                                  |
| Oper State                       | Enabled                                  |
+----------------------------------+------------------------------------------+

+----------------------------------+------------------------------------------+
| Parameter                        | Value                                    |
+----------------------------------+------------------------------------------+
| Instance Name                    | 1                                        |
| Profile Type                     | ExtendedTxRx                             |
| Bin                              | 24 hour History Bin                      |
| Collection Start Date/Time       | Sat May 04 16:00:02 2019                 |
| Collection End Date/Time         | Sun May 05 16:00:01 2019                 |
| Bin State                        | Partial                                  |
+----------------------------------+------------------------------------------+
| Statistic                        | Value                                    |
+----------------------------------+------------------------------------------+
|   RxBytes                        |                                        0 |
|   RxPkts                         |                                        0 |
|   RxCrcErrorPkts                 |                                        0 |
|   RxUcastPkts                    |                                        0 |
|   RxMcastPkts                    |                                        0 |
|   RxBcastPkts                    |                                        0 |
|   UndersizePkts                  |                                        0 |
|   OversizePkts                   |                                        0 |
|   FragmentsPkts                  |                                        0 |
|   JabbersPkts                    |                                        0 |
|   RxPausePkts                    |                                        0 |
|   RxDropPkts                     |                                        0 |
|   RxDiscardPkts                  |                                        0 |
|   RxLOutRangePkts                |                                        0 |
|   RxInErrorPkts                  |                                        0 |
|   64OctsPkts                     |                                        0 |
|   65To127OctsPkts                |                                        0 |
|   128To255OctsPkts               |                                        0 |
|   256To511OctsPkts               |                                        0 |
|   512To1023OctsPkts              |                                        0 |
|   1024To1518OctsPkts             |                                        0 |
|   1519To2047OctsPkts             |                                        0 |
|   2048To4095OctsPkts             |                                        0 |
|   4096To9216OctsPkts             |                                        0 |
|   9217To16383OctsPkts            |                                        0 |
|   TxBytes                        |                                        0 |
|   TxPkts                         |                                        0 |
|   TxExDeferPkts                  |                                        0 |
|   TxDeferPkts                    |                                        0 |
|   TxGiantPkts                    |                                        0 |
|   TxUnderRunPkts                 |                                        0 |
|   TxCrcErrorPkts                 |                                        0 |
|   TxLCheckErrorPkts              |                                        0 |
|   TxLOutRangePkts                |                                        0 |
|   TxLateCollPkts                 |                                        0 |
|   TxExCollPkts                   |                                        0 |
```


Copyright© 2022 Ciena® Corporation

```
|   TxSingleCollPkts                |                                     0 |
|   TxCollPkts                      |                                     0 |
|   TxPausePkts                     |                                     0 |
|   TxUcastPkts                     |                                     0 |
|   TxMcastPkts                     |                                     0 |
|   TxBcastPkts                     |                                     0 |
|   Tx64OctsPkts                    |                                     0 |
|   Tx65To127OctsPkts               |                                     0 |
|   Tx128To255OctsPkts              |                                     0 |
|   Tx256To511OctsPkts              |                                     0 |
|   Tx512To1023OctsPkts             |                                     0 |
|   Tx1024To1518OctsPkts            |                                     0 |
|   Tx1519To2047OctsPkts            |                                     0 |
|   Tx2048To4095OctsPkts            |                                     0 |
|   Tx4096To9216OctsPkts            |                                     0 |
|   Tx9217To16383OctsPkts           |                                     0 |
|   TxDiscardPkts                   |                                     0 |
|   LinkUp                          |                                     0 |
|   LinkDown                        |                                     0 |
|   LinkFlap                        |                                     0 |
|   TX Bytes per Second             |                                     0 |
|   TX Frames per Second            |                                     0 |
|   RX Bytes per Second             |                                     0 |
|   RX Frames per Second            |                                     0 |
+-----------------------------------+---------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 10-7
Creating PM bulkstats

You can create a

- bulkstats-instance
- bulkstats-collector

  Note: The bulkstats-instance and bulkstats-collector names, and the logical-id must not be in use by another bulkstats instance or collector.

Create a bulkstats instance to define the period of statistics collection and the types of statistics that are collected at the end of each period.

You can specify up to 16 bulkstats instances. Each bulkstats instance is configured to collect a set of statistics at a desired interval.

Bulkstats instances are aligned to the system clock.

Copyright© 2022 Ciena® Corporation

This table lists the statistics that can be configured as part of a bulkstats instance.

Table 10-26
Valid values for statistics keyword

Statistic	Description
cpu	Collects CPU statistics.
cfm-delay	Collects CFM delay statistics.
cfm-mef-delay	Collects CFM MEF delay statistics.
cfm-synthetic-loss	Collects CFM synthetic loss statistics.
cfm-mef-synthetic-loss	Collects CFM MEF synthetic loss statistics.
memory	Collects memory statistics.
fans	Collects fan statistics.
temperature	Collects temperature statistics.
power	Collects power statistics.
pm-port-extendedTxRx	Collects extended transmit and receive statistics on a port if a PM instance for a port with profile-type of ExtendedTxRx is configured.
pm-port-queue-group	Collects statistics for default queue groups on a port if a PM instance for egress port queue group is configured.
pm-queue-group-profile	Collects statistics for custom queue groups on a port if a PM instance for queue group profiles is configured.
pm-tp-rsvp-ingress-corout	Collects statistics for an MPLS dynamic co-routed tunnel if a PM instance for an MPLS dynamic co-routed tunnel is configured.
pm-tp-rsvp-egress-corout	Collects statistics for an MPLS dynamic co-routed tunnel if a PM instance for an MPLS dynamic co-routed tunnel is configured.
pm-mpls-rsvp-transit	Collects statistics for an MPLS RSVP transit tunnel if a PM instance for an MPLS transit tunnel is configured.
port	Collects statistics for a port if a PM instance for a port is configured.
cfm-mep	Collects MEP statistics.

Copyright© 2022 Ciena® Corporation

Table 10-26
Valid values for statistics keyword

Statistic	Description
pm-tp-rsvp-egress-unidir	Collects statistics for an MPLS RVSP unidirectional tunnel if a PM instance for a MPLS unidirectional tunnel is configured.
pm-tp-rsvp-ingress-unidir	Collects statistics for an MPLS RVSP unidirectional tunnel if a PM instance for a MPLS unidirectional tunnel is configured.
cfm-global	Collects statistics for global.
cfm-remote-mep	Collects remote MEP statistics.
mpls-lsp	Collects statistics for an MPLS LSP if a PM instance for an MPLS LSP is configured.
qos-flow	Collects statistics for QoS flows.
cfm-frame-loss	Collects CFM frame loss statistics.
cfm-service	Collects CFM service statistics.
mpls-vc	Collects statistics for an MPLS virtual circuit.
cfm-loopback	Collects statistics for CFM loopback.
pm-mpls-rsvp-egress	Collects statistics for an MPLS RSVP tunnel if a PM instance for an MPLS RSVP tunnel is configured.
pm-mpls-rsvp-ingress	Collects statistics for an MPLS RSVP tunnel if a PM instance for an MPLS RSVP tunnel is configured.
pm-tdm-port	Collects statistics for TDM port if a PM instance for the TDM port is configured.
pm-tp-rsvp-transit-corout	Collects statistics for a RSVP transit co-routed tunnel if a PM instance for a RSVP transit co-routed tunnel is configured.
virtual-circuit	Collects statistics for a virtual circuit.
egress-port-queue-group	Collects statistics for queue groups on a port.
pm-tdm-vc	Collects statistics for a TDM virtual circuit if a PM instance for the TDM virtual circuit is configured.
pm-tp-rsvp-transit-unidir	Collects statistics for a RSVP transit unidirectional tunnel if a PM instance for a RSVP transit unidirectional tunnel is configured.

Copyright© 2022 Ciena® Corporation

Table 10-26
Valid values for statistics keyword

Statistic	Description
pm-mpls-bgp-ingress	Collects statistics for an MPLS BGP tunnel if a PM instance for an MPLS BGP tunnel is configured.
pm-mpls-bgp-egress	Collects statistics for an MPLS BGP tunnel if a PM instance for an MPLS BGP tunnel is configured.
pm-mpls-bgp-transit	Collects statistics for an MPLS BGP transit tunnel if a PM instance for an MPLS BGP transit tunnel is configured.

Step	Action

To create a bulkstats-instance

1 Create a bulkstats-instance.

```
pm bulkstats create bulkstats-instance <pm-bulkstats-
instance-object> {duration <DURATION> interval
<5m|15m|30m|60m|3h|12h|24h> logical-id <1..4294967295>
statistics <cpu|egress-port-queue-
group|fans|memory|mpls-lsp|mpls-vc|port|power|qos-
flow|temperature|virtual-circuit>}
```

where

bulkstats-instance <pm-bulkstats-instance-object>	Specifies the name of the bulkstats-instance. If you attempt to use bulkstats-instance name that is already in use, an error message is displayed.
duration <DURATION>	Defines the entire period of statistics history that is saved for this bulkstats-instance. A bulkstats-instance can define a duration of up to 1 month (30 days). This defines the amount of file history that the system retains for the bulkstats-instance. The system does not allow the configured duration to be less than the configured interval. Default is 8h.

Copyright© 2022 Ciena® Corporation

where

interval <5m|15m|30m|60m|3h|12h|24h>	Specifies the statistics collection period and allows you to select how often statistics will be collected. Default is 15m.
logical-id <1..4294967295	Specifies the logical-id for the bulkstats-instance. If you attempt to use a logical-id in use by another bulkstats-instance, an error message is displayed.
statistics <cpu|egress-port-queue-group|fans|memory|mpls-lsp|mpls-vc|port|power|qos-flow|temperature|virtual-circuit>	Specifies the statistics that are gathered for this instance. The statistics can be any mix of supported statistics. The CLI supports comma-separated listing where you can specify any mix of statistics to add to the bulkstats-instance. Default is None, empty list.

To create a bulkstats-collector

2 Configure a bulkstats-collector.

```
pm bulkstats create bulkstats-collector <pm-bulkstats-
collector-object> {push-interval <DURATION> logical-id
<1..4294967295> remote-file-prefix <NAMESTRING[1..127]>
{tftp-server <ip-host-str> [server-port <INTEGER:
1..65535>]}|
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echoless-password-attr>][server-port
<INTEGER: 1..65535>]}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echoless-password-attr>}[server-port
<INTEGER: 1..65535>]}}{login-id <login-id> [echoless-
password]}
```

where

bulkstats-collector <pm-bulkstats-collector-object>	Specifies the name of the bulkstats-collector. f you attempt to use bulkstats-collector name that is already in use, an error message is displayed.
push- interval <DurationString>	Specifies the statistics transmission period, allowing you to choose the frequency of statistics file transmission.
logical-id <1..4294967295>	is the logical ID of the bulkstats-collector.
remote-file-prefix <NAMESTRING[1..127]	Specifies the remote-file prefix for the default server of the bulkstats-collector.
tftp-server <ip-host-str>	is the tftp-server.
server-port <INTEGER: 1..65535>	is the server-port number.
ftp-server <ip-host-str>	is the ftp-server name.

Copyright© 2022 Ciena® Corporation

where

login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
server-port <INTEGER: 1..65535>	is the server-port number to connect to.

—end—

Examples

The following example creates a bulkstats-instance.

```
pm bulkstats create bulkstats-instance myInst05 duration 24h
interval 60m logical-id 50000 statistics port fans
```

The following example creates a bulkstats-collector.

```
pm bulkstats create bulkstats-collector myColl05 duration 24h
interval 60m logical-id 425000 ftp-server host1 echoless-
password
```


Copyright© 2022 Ciena® Corporation

Procedure 10-8
Adding and removing statistics from PM bulkstats

You can add and remove specified statistics from a

- bulkstats-instance
- bulkstats-collector

Step	Action

To add statistics to a bulkstats-instance

1 Add statistics to a bulkstats-instance.

```
pm bulkstats add bulkstats-instance <pm-bulkstats-
instance> statistics <cpu|egress-port-queue-
group|fans|memory|mpls-lsp|mpls-vc|port|power|qos-
flow|temperature|virtual-circuit>
```

where

bulkstats-instance <pm-bulkstats-instance>	Specifies the name of the bulkstats-instance you want to add the statistics to.
statistics <cpu|egress-port-queue-group | fans | memory | mpls-lsp | mpls-vc | port | power | qos-flow |temperature | virtual-circuit>	Specifies the statistics that are gathered for this instance. The statistics can be any mix of supported statistics. The CLI supports comma-separated listing where you can specify any mix of statistics to add to the bulkstats-instance. Default is None, empty list.

To remove statistics from a bulkstats-instance

2 Remove statistics from a bulkstats-instance.

```
pm bulkstats remove bulkstats-instance <pm-bulkstats-
instance> statistics <cpu|egress-port-queue-
group|fans|memory|mpls-lsp|mpls-vc|port|power|qos-
flow|temperature|virtual-circuit
```

To add a bulkstats-instance to a bulkstats-collector

3 Add a bulkstats-instance to a bulkstats-collector.

```
pm bulkstats add bulkstats-instance <pm-bulkstats-
collector-objects> <pm-bulkstats-instance-object>
```

where

bulkstats-instance <pm-bulkstats-collector>	Specifies the name of the bulkstats-collector you want to add the statistics to.
pm-bulkstats-instance object	Specifies the bulkstats-instance.

Copyright© 2022 Ciena® Corporation

To remove a bulkstats-instance to a bulkstats-instance

4 Remove a bulkstats-instance to a bulkstats-instance.

```
pm bulkstats remove bulkstats-collector <pm-bulkstats-
collector-objects> bulkstats-instance <pm-bulkstats-
instance-object>
```

—end—

Examples

The following example adds a bulkstats-instance.

```
pm bulkstats add bulkstats-instance myInst02 statistics ports,
fans
```

The following example removes a bulkstats-instance.

```
pm bulkstats remove bulkstats-instance myInst04 statistics
ports, fans
```

The following example adds a bulkstats- instance to a bulkstats-collector.

```
pm bulkstats add bulkstats-instance myInst02 myCol03
```

The following example removes a bulkstats-instance from a bulkstats-collector.

```
pm bulkstats remove bulkstats-collector myColl03 bulkstats-
instance myInst02 myCol103
```


Copyright© 2022 Ciena® Corporation

Procedure 10-9
Enabling and disabling PM bulkstats

You can enable or disable a

- bulkstats-instance
- bulkstats-collector

Step	Action

To enable or disable a bulkstats-instance

1 Enable or disable a bulkstats-instance.

```
pm bulkstats [enable|disable] bulkstats-instance <pm-bulkstats-instance-object>
```

where

enable | disable	Enables or disables the bulkstats-instance
bulkstats-instance <pm-bulkstats-instance-object>	Specifies the name of the bulkstats-instance you wish to enable or disable.

To enable or disable a bulkstats-collector

2 Enable or disable a bulkstats-collector.

```
pm bulkstats [enable|disable] <pm-bulkstats-instance-object>
```

where

enable | disable	Enables or disables the bulkstats-collector
pm-bulkstats-instance-object	Specifies the name of the bulkstats-collector you wish to enable or disable.

—end—

Copyright© 2022 Ciena® Corporation

Examples

The following example enables a bulkstats-instance.

```
pm bulkstats enable bulkstats-instance myInst03
```

The following example disables a bulkstats-instance.

```
pm bulkstats disable bulkstats-instance myInst04
```

The following example enables a bulkstats-instance.

```
pm bulkstats enable bulkstats-instance myInst03
```

The following example disables a bulkstats-instance.

```
pm bulkstats disable bulkstats-instance myInst04
```


Copyright© 2022 Ciena® Corporation

Procedure 10-10
Deleting PM bulkstats

You can delete a

- bulkstats-instance
- bulkstats-collector

Step	Action

To delete a bulkstats-instance

1 Delete a bulkstats-instance.

```
pm bulkstats delete <pm-bulkstats-instance-object>
```

where

delete <pm-bulkstats-instance-object>	Deletes the specified bulkstats-instance.

To delete a bulkstats-collector

2 Delete a bulkstats-collector.

```
pm bulkstats delete <pm-bulkstats-collector-object>
```

where

delete <pm-bulkstats-collector-object>	Deletes the specified bulkstats-collector.

—end—

Examples

The following example deletes the bulkstats-collector myCol01.

```
pm bulkstats delete myCol01
```

The following example deletes the bulkstats-instance myInst01.

```
pm bulkstats deletes myInst01
```


Copyright© 2022 Ciena® Corporation

Procedure 10-11
Clearing PM bulkstats

You can clear a bulkstats instance.

Step	Action
1	Clear a bulkstats-instance. `pm bulkstats clear bulkstats-instance <pm-bulkstats-instance-object>` where bulkstats-instance <pm-bulkstats-instance-object> — Specifies the name of the bulkstats-instance you wish to clear. **—end—**

Example

The following example clears the bulkstats-instance myInst02.

```
pm bulkstats clear bulkstats-instance myInst02
```


Copyright© 2022 Ciena® Corporation

Procedure 10-12
Displaying bulkstats configuration information

You can display

- all configuration and status information
- configuration and state of the specified bulkstats-collector
- bulkstats-instances and collectors, including internal use fields and flags

Step	Action

To display all configuration and status information

1 Display all configuration and status information.

```
pm bulkstats show
```

To display configuration and state of the specified bulkstats instance

2 Display the configuration and state of the specified bulkstats instance:

```
pm bulkstats show <pm-bulkstats-collector-object>
```

where

bulkstats-instance <pm-bulkstats-instance-object>	Specifies the name of the bulkstats-instance you wish to display.

To display configuration and state of the specified bulkstats collector

3 Display the configuration and state of the specified bulkstats collector:

```
pm bulkstats show <pm-bulkstats-collector-object>
```

where

bulkstats-instance <pm-bulkstats-collector-object>	Specifies the name of the bulkstats-collector you wish to display.

—end—

Copyright© 2022 Ciena® Corporation

Examples

The following example shows output for the pm bulkstats show command.

```
pm bulkstats show

+----------------------- BULKSTATS GLOBAL CONFIGURATION -----------------------+
| Item                                  | Value                                |
+---------------------------------------+--------------------------------------+
| Bulkstats Admin State                 | enabled                              |
|                                       |                                      |
+---------------------------------------+--------------------------------------+


+------------------- BULKSTATS INSTANCES SUMMARY --------------------+
|Instance Name/                 |Admin|Oper |Interval|Duration      |
|Statistics                     |State|State|        |              |
+-------------------------------+-----+-----+--------+--------------+
|smile                          |En   |En   | 15 min | 1h           |
|  cpu                          |     |     |        |              |
|  memory                       |     |     |        |              |
|  fans                         |     |     |        |              |
|  port                         |     |     |        |              |
+-------------------------------+-----+-----+--------+--------------+


+-------------------- BULKSTATS COLLECTORS SUMMARY ---------------------+
|Collector Name/                |Admin|Oper |Push              |Bulkstats|
|XFTP Settings                  |State|State|Interval          |Instances|
+-------------------------------+-----+-----+------------------+---------+
|ftp                            |En   |En   | 1h               | 1       |
|  FTP Server: 10.25.41.21      |     |     |                  |         |
+-------------------------------+-----+-----+------------------+---------+
```

The following example displays information for the bulkstats-instance myInst02.

```
pm bulkstats show myInst02

+------------------------ BULKSTATS INSTANCE SUMMARY ------------------------+
| Parameter                       | Value                                    |
+---------------------------------+------------------------------------------+
| Instance Name                   | myInst02                                 |
| Instance ID                     | 50000                                    |
| Interval                        | 10 min                                   |
| Duration                        | 1h30m                                    |
| Statistics                      | memory                                   |
|                                 | power                                    |
|                                 | virtual-circuit                          |
| Admin State                     | enabled                                  |
| Oper State                      | enabled                                  |
+---------------------------------+------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

The following example displays information for the bulkstats-collector myColl15.

```
pm bulkstats show myColl15

+------------------------ BULKSTATS COLLECTOR SUMMARY -------------------------+
| Parameter                        | Value                                     |
+----------------------------------+-------------------------------------------+
| Collector Name                   | myColl15                                  |
| Instance ID                      | 435000                                    |
| Push Interval                    | 1h10m                                     |
| Bulkstats Instance(s)            | <none>                                    |
| XFTP Server                      | TFTP Server: mytfpserver10                |
| Remote File Prefix               | 110                                       |
| Last Push Remote Name            |                                           |
| Last Push State                  | NA                                        |
| Last Push Time                   | NA                                        |
| Admin State                      | enabled                                   |
| Oper State                       | enabled                                   |
+----------------------------------+-------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 10-13
Configuring bulkstats-collector xftp settings

You can configure the bulkstats-collector xftp settings for the TFP, FTP or SFTP server. Specify the login-in authentication information for SFTP and FTP servers.

Step	Action

Configure the bulkstats-collector xftp settings

1 Configure the bulkstats-collector xftp settings:

```
pm bulkstats set bulkstats collector <pm-bulkstats-
collector-object> tftp-server <ip-host-str> [server-port
<INTEGER: 1..65535>]}|
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echoless-password-attr>][server-port
<INTEGER: 1..65535>]}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echoless-password-attr>}[server-port
<INTEGER: 1..65535>]}}
```

where

set bulkstats-collector <pm-bulkstats-collector-object>	Configures the specified bulkstats-collector.
tftp-server <ip-host-str>	is the tftp-server.
server-port <INTEGER: 1..65535>	is the server-port number.
ftp-server <ip-host-str>	is the ftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
server-port <INTEGER: 1..65535>	is the server-port number to connect to.

Clearing the bulkstats-collector xftp settings

2 Clear the bulkstats-collector xftp settings:

```
pm bulkstats unset <pm-bulkstats-collector-object> server
remote-file-prefix
```

—end—

Copyright© 2022 Ciena® Corporation

Examples

The following example configures the bulkstats-collector on a TFTP server.

```
pm bulkstats set bulkstats-collector myColl15 tftp-server
mytfpserver
```

The following example clears the bulkstats-collector xftp settings.

```
pm bulkstats unset bullkstats-collector myCol15 server remote-
file-prefix
```


Copyright© 2022 Ciena® Corporation

Procedure 10-14
Transferring the bulkstats-collector's statistics file

You can trigger the immediate transfer of the bulkstats-collector's statistics file.

Step	Action
1	Trigger the immediate transfer of the bulkstats-collector's statistics file: `pm bulkstats push <pm-bulkstats-collector-object>` where push <pm-bulkstats-collector-object> — Specifies the bulkstats-collector's statistics file you wish to transfer.

Example

The following example immediately transfers the bulkstats-collector myColl15.

```
pm bulkstats push bulkstats-collector myColl15
```


Copyright© 2022 Ciena® Corporation

Procedure 10-15
Configuring the bulkstats-collector's remote filename prefix

You can

- configure the bulkstats-collector's remote filename prefix
- remove the bulkstats-collector's remote filename prefix

Step	Action

Configuring the bulkstats-collector remote-filename prefix

1 Configure the bulkstats-collector remote filename prefix:

```
pm bulkstats set bulkstats-collector <pm-bulkstats-
collector-object> <pm-bulkstats-collector-object> tftp-
server <ip-host-str> [server-port <INTEGER: 1..65535>]}|
{ftp-server <ip-host-str> [login-id <username>
[<password-attr>|<echoless-password-attr>][server-port
<INTEGER: 1..65535>]}|
{sftp-server <ip-host-str> login-id <username>
{<password-attr>|<echoless-password-attr>}[server-port
<INTEGER: 1..65535>]}}
```

where

set <pm-bulkstats-collector-object>	Configures the specified bulkstats-collector.
tftp-server <ip-host-str>	is the tftp-server.
server-port <INTEGER: 1..65535>	is the server-port number.
ftp-server <ip-host-str>	is the ftp-server name.
login-id <username>	is the FTP/SFP username.
password-attr	enters the password in clear text.
echoless-password-attr	engages an echoless password collector.
server-port <INTEGER: 1..65535>	is the server-port number to connect to.

Remove the bulkstats-collector remote-filename prefix

2 Remove the bulkstats-collector remote filename prefix:

```
pm bulkstats unset <pm-bulkstats-collector-object>
remote-file-prefix
```

—end—

Copyright© 2022 Ciena® Corporation

Examples

The following example configures the remote-file prefix for the bulkstats-collector.

```
pm bulkstats set myCol01 remote-file-prefix prefix100
```

The following example clears the remote-file prefix for the bulkstats-collector.

```
pm bulkstats unset myCol01 remote-file-prefix
```


Copyright© 2022 Ciena® Corporation

Procedure 10-16
Configuring PM threshold crossing alerts

PM thresholds are configured using the interval profile and interval profile attributes. See Table 10-25 for a list of configurable attributes.

1 Create an interval profile using the specified name and parameters:

```
pm threshold create <interval-profile-name>
{[NAMESTRING<1...31>]} <interval-profile-object>
{[sample-interval <1m|5m|10m|15m|30m|60m|24h>][logical-
id <1..2147483647>] <interval-profile-attrs>}
```

where

<interval-profile-name>	Name of profile (up to 31 characters).
<interval-profile-object>	Configures the interval profile using the specified name and parameters.
<interval-profile attrs>	Attributes configured to define the interval profile.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-17
Clearing a threshold associated with a PM

Clear thresholds by specifying either history or statistics associated with PM threshold crossing alerts.

Step	Action
1	Clear a threshold associated with a PM instance: `pm threshold clear <pm-instance-object> {alert | history | statistics}` where **<pm-instance-object> {alert | history | statistics}** For a PM instance, clear alert TCA. For a PM instance, specify history to clear all PM threshold crossing alerts (last Adjustment TCAs and last Alert TCAs). For a PM instance, specify statistics to clear all PM threshold crossing alerts related to Adjustment/Alert TCAs. **—end—**

Copyright© 2022 Ciena® Corporation

Procedure 10-18
Deleting a threshold interval profile

Delete an interval profile using the specified name.

Step	Action
1	Specify an interval profile by name to delete: `pm threshold delete <interval-profile-object>` where <interval-profile-object> — Configures the interval profile using the specified name and parameters. **—end—**

Copyright© 2022 Ciena® Corporation

Procedure 10-19
Setting a PM threshold attribute

The attribute and the value of the attribute for a specified interval-profile can be configured. See Table 10-25 for a list of configurable attributes.

Step	Action

1 Set the attribute and attribute value of the specified interval-profile:

```
pm threshold set <interval-profile-object> {<interval-profile-attrs>}
```

where

<interval-profile-object>	Configures the interval profile using the specified name and parameters.
<interval-profile attrs>	Attributes configured to define the interval profile.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 10-20
Displaying a PM threshold

Display the PM threshold configuration.

To display a summary of the PM threshold configuration:

1 Show a summary of a PM threshold configuration.

```
pm threshold show
```

To display the details the PM threshold crossing alert for a specified PM instance:

2 Show details about the PM threshold crossing alert for a specified PM instance.

Show details about the PM threshold crossing alert for a specified PM instance.

3 `pm threshold show <pm-instance-object>`

where

<pm-instance-object> Configures the interval profile using the specified name and parameters.

—end—

Example

This example shows the output resulting when the PM instance named AutoSize is specified.

```
pm threshold show pm-instance AutoSize
```

```
+--------------- PERFORMANCE MONITORING THRESHOLD CROSSING ALERT DATA ----------------+
| Parameter                                | Value                                    |
+------------------------------------------+------------------------------------------+
| Instance Name                            | AutoSizeInstance                         |
| Interval Profile                         | AutoSize                                 |
| Adjustment TCA Units                     | bits-per-second                          |
| Adjustment TCA Scheme                    | inclusive-or                             |
| Adjustment TCA Stats                     | RX Accepted Bytes,TX Forwarded Bytes     |
| Adjustment TCA Basis Value               | 100,000,000                              |
| Adjustment TCA Basis Minimum             | 50,000,000                               |
| Adjustment TCA Basis Maximum             | 100,000,000                              |
| Adjustment TCA Configuration Status      | configured                               |
| Adjustment TCA Upper Boundary            | 102,000,000                              |
| Adjustment TCA Lower Boundary            | 98,000,000                               |
| Adjustment TCA Interval Start Date/Time  | Fri Nov 04 20:20:00 2016 (1m10s ago)     |
| Adjustment TCA Interval End Date/Time    | Fri Nov 04 20:30:00 2016 (8m50s from now)|
| Adjustment TCA Sample Start Date/Time    | Fri Nov 04 20:20:00 2016 (1m10s ago)     |
| Adjustment TCA Sample End Date/Time      | Fri Nov 04 20:25:00 2016 (3m50s from now)|
+------------------------------------------+------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

CPU rate limiting

Network protocol control frames require examination and processing from the Central Processing Unit (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.

To prevent this issue, you can control the number of protocol control frames to be processed with CPU rate limiting.

This chapter provides the following procedures for CPU rate limiting:

- "Setting CPU rate limits" on page 11-2
- "Resetting CPU rate limits to default" on page 11-5
- "Enabling CPU rate limiting" on page 11-6
- "Disabling CPU rate limiting" on page 11-7
- "Displaying CPU rate limiting configuration" on page 11-8
- "Displaying CPU rate limiting statistics" on page 11-10
- "Displaying CPU rate limiting configuration in the configuration file" on page 11-12
- "Configuring CPU rate limiting" on page 11-13

Copyright© 2022 Ciena® Corporation

Procedure 11-1
Setting CPU rate limits

Set CPU rate limits to control the number of frames that the CPU processes to help protect the CPU from resource overload, system lockup, and port link loss. CPU rate limits are configured in Packets Per Second (PPS) for each physical port.

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 passes the specified number of packets and drops all following packets of that packet class on the specified port for the remainder of the second.

Step	Action

1 Set CPU rate limits by entering the following command:

```
flow cpu-rate-limit set {port <PhyPortNameList>}{arp
<NUMBER: 0-2500>}{bootp <NUMBER: 0-2500>}{cfm <NUMBER: 0-
1000>}{cft <NUMBER: 0-2500>}{dhcpv6 <NUMBER:
0..2500>}{dot1x <NUMBER: 0-2500>} {eoam <NUMBER: 0-
2500>}{esmc <NUMBER: 0-2500>}{igmp <NUMBER: 0-2500>}{ip-
control <NUMBER: 0-5000>}{ip-icmp <NUMBER: 0-5000>}{ip-
mgmt <NUMBER: 0-5000>}{ipv6-mgmt <NUMBER: 0-5000>}{ipv6-
icmp <NUMBER: 0-5000>} {lacp <NUMBER: 0-2500>}{lldp
<NUMBER: 0-2500>}{lpbk <NUMBER: 0-2500>}{mpls <NUMBER: 0-
2500>}{pvst <NUMBER: 0-2500>}{raps <NUMBER: 0-
2500>}{rmtlpbk <NUMBER: 0-2500>}{twamp <NUMBER: 0-
2500>}{twampRsp <NUMBER: 0-2500>}{xstp <NUMBER: 0-
2500>}{cicp <NUMBER: 0..2500>} {dflt <NUMBER: 0-10000>}
```

where

port <PhyPortNameList>	is the physical port list.
arp <NUMBER: 0-2500>	is the rate limit for ARP. The default rate limit is 50 PPS.
bootp <NUMBER: 0-2500>	is the rate limit for Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) control frames. The default rate limit is 5 PPS.

Copyright© 2022 Ciena® Corporation

where

cfm <NUMBER: 0-1000>	is the rate limit for Connectivity Fault Management (CFM) control frames. The default rate limit is 50 PPS. • For 3903, 3903x, 3904, 3905, 3906, 3926, 3928, 3942, 5142, and 5160 devices the range is 0-1000.
cft <NUMBER: 0-2500>	is the rate limit for tunneled control frames. The default rate limit is 250 PPS.
dhcpv6 <NUMBER: 0..2500>	is the rate limit for dhcpv6. The default is 5.
dot1x <NUMBER: 0-2500>	is the rate limit for 802.1x port-based network access control frames. The default rate limit is 5 PPS.
eoam <NUMBER: 0-2500>	is the rate limit for Operation, Administration, and Maintenance (EOAM) control frames. The default rate limit is 5 PPS.
esmc <NUMBER:0-2500>	is the rate limit for ESMC PDUs. The default rate limit is 40 frames per second per port.
igmp <NUMBER: 0-2500>	is the rate limit for Internet Group Management Protocol (IGMP) control frames. The default rate limit is 25 PPS.
ip-control <NUMBER: 0-5000>	is the rate limit for IP control protocols. The default rate limit is 700 PPS.
ip-icmp <NUMBER: 0-5000>	is the rate limit for IP ICMP. The default rate limit is 100 PPS.
ip-mgmt <NUMBER: 0-5000>	is the rate limit for IP management protocols. The default rate limit is 700 PPS.
ipv6-mgmt <NUMBER: 0-5000>	is the rate limit for IPv6 management control frames. The default is 700.
ipv6-icmp <NUMBER: 0..5000>	is the IPv6 ICMP PPS limit. The default is 100.
lacp <NUMBER: 0-2500>	is the rate limit for Link Aggregation Control Protocol (LACP) control frames. The default rate limit is 5 PPS.

Copyright© 2022 Ciena® Corporation

where

lldp <NUMBER: 0-2500>	is the rate limit for Link Layer Discovery Protocol (LLDP) control frames. The default rate limit is 5 PPS.
lpbk <NUMBER: 0-2500>	is the rate limit for Loopback (used for debug). The default rate limit is 5 PPS.
mpls <NUMBER: 0-2500>	is the rate limit for MPLS.
pvst <NUMBER: 0-2500>	is the rate limit for Per VLAN Spanning Tree (PVST) control frames. The default rate limit is 5 PPS.
raps <NUMBER: 0-2500>	is the rate limit for RAPS control frames. The default rate limit is 5 PPS.
rmtlpbk <NUMBER: 0-500>	is the rate limit for Remote loopback, which is used for debugging purposes. The default rate limit is 5 PPS.
twamp <NUMBER: 0-2500>	is the rate limit for Two-Way Active Measurement Protocol (TWAMP) test frames. The default rate limit is 100 PPS.
twampRsp <NUMBER: 0-2500>	is the rate limit for Two-Way Active Measurement Protocol (TWAMP) response frames. The default rate limit is 250 PPS.
xstp <#0..2500>	is the rate limit for XSTP. The default rate limit is 5 PPS.
cicp <NUMBER: 0..2500>	is the CICP PPS limit. The default is 200 PPS.
dflt <NUMBER: 0-10000>	is the default rate limit. The default rate limit is 10 PPS.

—end—

Example

The following example sets a CPU rate limit of 300 for TWAMP test frames on port 15.

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


Copyright© 2022 Ciena® Corporation

Procedure 11-2
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.

Step	Action
1	Reset CPU rate limits to default: `flow cpu-rate-limit unset {port <PhyPortNameList}` where port <PhyPortName List> is the port or ports to reset.

—end—

Example

The following example resets CPU rate limits for all packet classes to default on port 15.

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


Copyright© 2022 Ciena® Corporation

Procedure 11-3
Enabling CPU rate limiting

You can enable CPU rate limiting:

- at the global (system) level
- for each 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.

Step	Action

To enable CPU rate limiting globally

1 Enable CPU rate limiting globally:

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

To enable CPU rate limiting per port

2 Enable CPU rate limiting per port:

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

where

<PhyPortNameList> is the port that you want to enable CPU rate limiting on.

—end—

Examples

The following example enables CPU rate limiting globally.

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

The following example enables CPU rate limiting on port 15.

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


Copyright© 2022 Ciena® Corporation

Procedure 11-4
Disabling CPU rate limiting

You can disable CPU rate limiting:

- at the global (system) level
- for each port

Step	Action

To disable CPU rate limiting globally

1 Disable CPU rate limiting globally:

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

To disable CPU rate limiting per port

2 Disable CPU rate limiting per port:

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

—end—

Examples

The following example disables CPU rate limiting globally.

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

The following example disables CPU rate limiting on port 15.

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


Copyright© 2022 Ciena® Corporation

Procedure 11-5
Displaying CPU rate limiting configuration

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 to determine what type of control frames are being dropped. You can also display the rate limits per port.

Step	Action

To display the global status of CPU rate limiting

1 Display the global status of CPU rate limiting:

```
flow cpu-rate-limit show
```

To display the CPU rate limits for a specific port

2 Display CPU rate limits for a specific port:

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

where

<PortName> is the port that you want to display CPU rate limits for.

—end—

Example

The following example shows sample output for the flow cpu-rate-limit show command.

```
flow cpu-rate-limit 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    |          |
...
+--------+-----------+---------------+----------+
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the flow cpu-rate-limit show port 15 command.

```
flow cpu-rate-limit show port 15
+--- CPU-RATE-LIMIT PPS RATE LIMITS ----+
| Port     | Packet Class     | PPS Rate |
+----------+------------------+----------+
| 12       | ARP              |       50 |
| 12       | Bootp/DHCP       |        5 |
| 12       | CFM              |       50 |
| 12       | CFT              |      250 |
| 12       | DHCPv6           |        5 |
| 12       | Dot 1X           |        5 |
| 12       | EOAM             |        5 |
| 12       | ESMC             |       40 |
| 12       | IGMP             |       25 |
| 12       | IP-MGMT          |      700 |
| 12       | IPv6-MGMT        |      700 |
| 12       | IP-CONTROL       |      700 |
| 12       | IP-ICMP          |      100 |
| 12       | IPv6-ICMP        |      100 |
| 12       | LACP             |        5 |
| 12       | LLDP             |        5 |
| 12       | PVST             |        5 |
| 12       | RAPS             |      200 |
| 12       | Loopback         |        5 |
| 12       | Remote Loopback  |        5 |
| 12       | TWAMP TST        |      100 |
| 12       | TWAMP RSP        |      250 |
| 12       | xSTP             |        5 |
| 12       | CICP             |      200 |
| 12       | Default          |       10 |
+----------+------------------+----------+
```

Note: The order of the protocols displayed in the `flow cpu-rate-limit show port` command is not the order in which they are actually tested. For example, Multicast/Broadcast frames are the first frame type tested, so if a Multicast LACP frame fails the configured rate limit test, it would be dropped. In addition, when traffic is sent at exactly the rate limit configured, an occasional drop may be seen in the test results simply due to the fact that the sample window is not exact and shifts slightly because it is not run by a high precision timer. Results are rounded to the nearest 0.1 percent.

Copyright© 2022 Ciena® Corporation

Procedure 11-6
Displaying CPU rate limiting statistics

Display CPU rate limiting statistics.

Step	Action
1	Display CPU rate limiting statistics for a specific port : `flow cpu-rate-limit show port <PortName> statistics`

—end—

Example

The following example shows sample output for the flow cpu-rate-limit show port command.

```
flow cpu-rate-limit show port 7 statistics

+----------- CPU-RATE-LIMIT PACKET STATISTICS -----------+
| Port     | Packet Class     |   Dropped    |   Passed    |
+----------+------------------+--------------+-------------+
| 7        | ARP              |            0 |           0 |
| 7        | Bootp/DHCP       |            0 |           0 |
| 7        | CFM              |            0 |           0 |
| 7        | CFT              |            0 |           0 |
| 7        | DHCPv6           |            0 |           0 |
| 7        | Dot 1X           |            0 |           0 |
| 7        | EOAM             |            0 |           0 |
| 7        | ESMC             |            0 |           0 |
| 7        | IGMP             |            0 |           0 |
| 7        | IP-MGMT          |            0 |           0 |
| 7        | IPv6-MGMT        |            0 |           0 |
| 7        | IP-CONTROL       |            0 |           0 |
| 7        | IP-ICMP          |            0 |           0 |
| 7        | IPv6-ICMP        |            0 |           0 |
| 7        | LACP             |            0 |        5801 |
| 7        | LLDP             |            0 |       17232 |
| 7        | PVST             |            0 |           0 |
| 7        | RAPS             |            0 |           0 |
| 7        | Loopback         |            0 |           0 |
| 7        | Remote Loopback  |            0 |           0 |
| 7        | TWAMP TST        |            0 |           0 |
| 7        | TWAMP RSP        |            0 |           0 |
| 7        | xSTP             |            0 |       86373 |
| 7        | CICP             |            0 |           0 |
| 7        | Default          |            0 |           0 |
+----------+------------------+--------------+-------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 11-7
Clearing CPU rate limiting statistics

Clear CPU rate limiting statistics.

Step	Action
1	Clear CPU rate limiting statistics for a specific port: `flow cpu-rate-limit clear port <PortName> statistics` **—end—**

Example

The following example clears CPU rate limiting statistics on port 15.

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


Copyright© 2022 Ciena® Corporation

Procedure 11-8
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.

Step	Action
1	Display CPU rate limiting configuration in the configuration file: `configuration show`

—end—

Example

The following example shows sample output for the configuration show command.

```
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
!
!
!...
```


Copyright© 2022 Ciena® Corporation

Procedure 11-9
Configuring CPU rate limiting

You can configure 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 the default.

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

—end—

Example

The following example configures CPU rate limiting.

```
flow cpu-rate-limit set port 1-5 bootp 50
flow cpu-rate-limit set port 1-5 cft 50 cfm 0 inet 5 dflt 10
flow cpu-rate-limit set port 25-28 rstp 50 lacp 10 lldp 25
flow cpu-rate-limit set port 25-28 cft 10
flow cpu-rate-limit enable
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

39XX/51XX Switches and Platforms

Fault and Performance Management

Copyright© 2022 Ciena® Corporation. All rights reserved.

SAOS 6.21.2
Publication: 009-3458-009
Document status: Standard
Revision A
Document release date: March 2022

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