39XX/51XX Switches and Platforms

Advanced OAM Configuration

SAOS 6.21.2

What's inside...

New in this release
Connectivity Fault Management (CFM) configuration
Signal degrade detection
Ethernet Operations, Administration and Maintenance (EOAM) configuration
Two-Way Active Measurement Protocol
System performance testing with RFC2544 and Y.1564 benchmark services
Network management IP interface

009-3458-044 - 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 xv

New in this release 1-1

Connectivity Fault Management (CFM) configuration 2-1

Overview 2-1
- MIP transparency 2-3
- Hardware-based CFM services 2-3
- Maintenance Domains 2-4
- Maintenance Associations 2-7
- MEPs 2-8
- MIPs 2-11
- Continuity Check Messages 2-11
- Loopback Messages 2-11
- Linktrace Messages 2-11
- ITU-T Y.1731 Performance Measurements 2-12

MEF 35 service OAM performance monitoring 2-19
- PM session mode 2-20
- PM session types 2-21
- MEF object indexing 2-21
- Session model information 2-24
- Key performance indicators 2-28
- Delay measurement sessions 2-29
- Synthetic loss sessions 2-32
- Session history 2-34
- Threshold crossing alerts 2-35
- Stateless TCA reporting 2-35
- Stateful TCA reporting 2-36
- TCA profiles 2-36

OAM system offloaded MEF session 2-37
- Scalability 2-38

Maintenance Association examples 2-39
- Provider 2-40
- Operator 2-40
- Customer 2-41
- Physical Link 2-42

CFM on Ethernet type virtual switches 2-43

CFM Over Q-in-Q 2-43

Copyright© 2022 Ciena® Corporation

CFM Frame Origination 2-44
Handling CFM Frames Received on a VS 2-45
CFM services on MPLS virtual switches 2-46
Enhanced OAM module platforms 2-47
OAM session resources 2-47
Offloading sessions to hardware 2-48
Configuration constraints 2-50
System scale limits 2-51
OAM frame rate scale limits 2-52
CFM service statistics 2-52
DMM/DMR Hardware Assist (3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, 5160 only) 2-53
Understanding Ingress CFM Frame Classification 2-54

List of procedures

2-1 Configuring and displaying CFM global settings 2-57
2-2 Configuring maintenance domains 2-62
2-3 Displaying maintenance domains 2-64
2-4 Creating and deleting CFM services 2-66
2-5 Setting attributes for CFM services 2-68
2-6 Enabling and disabling a CFM service 2-73
2-7 Displaying CFM services 2-74
2-8 Configuring a hardware-based service 2-79
2-9 Moving a CFM service between hardware and software 2-81
2-10 Moving a CFM service between software and hardware 2-82
2-11 Configuring MEPs 2-83
2-12 Setting MEP attributes 2-86
2-13 Deleting a MEP 2-88
2-14 Enabling and disabling a MEP 2-89
2-15 Displaying MEPs 2-91
2-16 Creating a remote MEP 2-94
2-17 Deleting a remote MEP 2-96
2-18 Enabling and disabling remote MEPs and MEP discovery 2-97
2-19 Displaying remote MEPs 2-99
2-20 Creating MIPs 2-102
2-21 Deleting MIPs 2-103
2-22 Enabling and disabling the MIP database 2-104
2-23 Displaying MIP configuration and MIP database 2-105
2-24 Sending and displaying loopback messages 2-106
2-25 Sending and displaying linktrace messages 2-109
2-26 Configuring Y.1731 DMMs 2-114
2-27 Configuring DMM responders 2-121
2-28 Displaying statistics 2-124
2-29 Configuring Y.1731 LMMs 2-133
2-30 Configuring LMM responders 2-140
2-31 Configuring single-ended synthetic frame loss measurement 2-143
2-32 Displaying and clearing CFM statistics 2-148
2-33 Displaying CFM port stack information 2-156
2-34 Configuring a VLAN CFM service 2-157
2-35 Configuring CFM services for a virtual switch service 2-159

Copyright© 2022 Ciena® Corporation

2-36 Configuring CFM over MPLS 2-161
2-37 Displaying SLM frame loss test results 2-168
2-38 Configuring a MEF 35 compliant delay session 2-169
2-39 Configuring a MEF 35 compliant synthetic loss measurement session 2-172
2-40 Deleting a MEF 35 compliant delay session 2-176
2-41 Deleting a MEF 35 compliant synthetic loss measurement session 2-177
2-42 Disabling a MEF 35 compliant delay measurement session 2-178
2-43 Disabling a MEF 35 compliant synthetic loss measurement session 2-179
2-44 Configuring a MEF 35 compliant frame delay range 2-180
2-45 Configuring a MEF 35 frame delay range bins lower threshold 2-181
2-46 Deleting a MEF 35 frame delay range binning profile 2-182
2-47 Displaying MEF 35 delay measurement information 2-183
2-48 Displaying MEF 35 synthetic loss session information 2-189
2-49 Displaying MEF 35 SOAM sessions on a MEP sorted by session index 2-196
2-50 Displaying MEF 35 frame relay range profiles 2-197
2-51 Creating a MEF 35 compliant threshold profile 2-199
2-52 Deleting a MEF 35 compliant threshold profile 2-200
2-53 Configuring parameters to a MEF 35 compliant threshold profile 2-201
2-54 Attaching a threshold profile to MEF 35 compliant sessions 2-204
2-55 Displaying MEF 35 compliant threshold profiles 2-206

Signal degrade detection 3-1

Bit error rate to frame error rate relationship 3-1
Signal degrade detection 3-2
- Synthetic-loss test frames 3-3
- Synthetic-loss test session duration 3-3
- Signal degrade detection thresholds 3-5
- Signal degrade detection based on delay/jitter 3-5
- Frame error rate to signal degrade threshold relationship 3-8

List of procedures

3-1 Configuring signal degrade detection on a port 3-9
3-2 Displaying signal degrade detection information 3-16
3-3 Displaying MEPs with signal-degrade monitoring filter 3-18
3-4 Displaying signal degrade set and clear thresholds on a synthetic-loss session 3-19
3-5 Displaying operational information for signal degrade enabled synthetic loss sessions 3-21
3-6 Displaying historical information for signal degrade enabled synthetic loss sessions 3-22
3-7 Displaying signal degrade set and clear thresholds on a delay measurement session 3-24
3-8 Displaying operational information for signal degrade enabled delay measurement session 3-27
3-9 Displaying historical information for signal degrade enabled for delay measurement sessions 3-28

Ethernet Operations, Administration and Maintenance (EOAM) configuration 4-1

Copyright© 2022 Ciena® Corporation

Support of standard tools 4-2
FPGA hardware assist 4-2
Link events 4-3
Critical events 4-4
Non-critical events 4-4

List of procedures
4-1 Enabling OAM on a port 4-5
4-2 Enabling loopback 4-9
4-3 Displaying EOAM information 4-11

Two-Way Active Measurement Protocol 5-1

Protocols 5-2
Operational roles 5-2
Relationship Between Protocols and Operational Roles 5-2
TWAMP Light Responder 5-3
TWAMP Complete Server 5-4
TWAMP Client 5-4
TWAMP-Test Packets 5-5
TWAMP server session deny 5-6

List of procedures
5-1 Configuring global TWAMP attributes 5-9
5-2 Enabling TWAMP 5-11
5-3 Displaying TWAMP information 5-12
5-4 Enabling TWAMP Light Responder 5-14
5-5 Enabling TWAMP complete server 5-15
5-6 Enabling TWAMP client 5-16
5-7 Creating a TWAMP client session 5-17
5-8 Displaying TWAMP client sessions 5-20
5-9 Updating a TWAMP client session 5-22
5-10 Deleting a TWAMP client session 5-23
5-11 Establishing and stopping a test session 5-24
5-12 Configuring TWAMP server session deny 5-25
5-13 Displaying and clearing TWAMP client statistics 5-28
5-14 Displaying active TWAMP server sessions on the target device 5-29
5-15 Clearing a TWAMP server session on the target device 5-30
5-16 Displaying TWAMP configuration in the configuration file 5-31

System performance testing with RFC2544 and Y.1564 benchmark services 6-1

Benchmarking test types 6-1
Throughput test 6-2
Frame loss test 6-2
Latency test 6-3
Packet delay variation test 6-3
Outage test 6-4
RFC2544 test 6-4
Y.1564 test 6-4
Test profile 6-6

Copyright© 2022 Ciena® Corporation

Test instance 6-6
Operational roles 6-7
UNI Generator 6-7
UNI Reflector 6-8
Port under test 6-9
Static Reflector 6-9
Benchmark testing scalability by platform 6-12
About test packets 6-13
Testing modes 6-13
Software upgrades and downgrades 6-14
Benchmark statistics 6-14
Packets that match the configured profile 6-15
Showing statistics 6-16
Test results 6-17
Benchmark NETCONF 6-17
Procedures 6-17

List of procedures

6-1 Configuring benchmark support on 3926, 3928, and 5160 switches 6-20
6-2 Configuring a custom EMIX sequence 6-22
6-3 Displaying EMIX sequence information 6-25
6-4 Configuring benchmark generator KPI profiles 6-27
6-5 Displaying KPI profile information 6-31
6-6 Configuring benchmark generator bandwidth allocation profile 6-33
6-7 Displaying bandwidth allocation information 6-36
6-8 Configuring a 39XX/51XX switch as a generator 6-38
6-9 Configuring a 39XX/51XX switch as a reflector 6-40
6-10 Modifying a generator 6-42
6-11 Modifying global attributes for a generator 6-43
6-12 Modifying a reflector 6-44
6-13 Displaying all benchmark entities 6-46
6-14 Displaying generator entity information 6-47
6-15 Deleting a generator or reflector 6-48
6-16 Configuring generator test profiles 6-49
6-17 Displaying generator test profiles 6-53
6-18 Configuring test attributes 6-55
6-19 Configuring traffic test types 6-58
6-20 Configuring payload information 6-61
6-21 Creating test instances 6-65
6-22 Creating generator test instances 6-67
6-23 Starting and stopping generator test instances 6-69
6-24 Generating untagged traffic 6-70
6-25 Generating single-tagged traffic 6-72
6-26 Generating double-tagged traffic 6-76
6-27 Reflecting untagged traffic 6-79
6-28 Reflecting single-tagged traffic 6-81
6-29 Reflecting double-tagged traffic 6-83
6-30 Displaying benchmark status information 6-86
6-31 Displaying benchmark test information 6-88
6-32 Displaying benchmark test statistics 6-91

Copyright© 2022 Ciena® Corporation

6-33 Displaying reflector global statistics 6-93
6-34 Clearing reflector global statistics 6-95
6-35 Clearing benchmark reflector test instance statistics 6-96
6-36 Clearing generator test instance statistics 6-97
6-37 Configuration example for MPLS 6-98

Network management IP interface 7-1

IPv6 7-1
IPv6 address format 7-1
IP address usage 7-2
IPv4 and IPv6 dual stack 7-4
Multiple IPv6 addresses 7-4
Multiple gateways 7-4
In-band management bridging 7-5
Topology setup 7-7
VLAN management 7-8
Local interface interaction 7-8
DHCP client interaction 7-9
DHCP relay interaction (option 82) 7-9
Private forwarding group interaction 7-9
Traffic profiling 7-9
Limitations 7-9
EVC ping 7-11
Local EVC ping 7-13
Auxiliary ping 7-16
Auxiliary ping scope 7-16
Connectivity 7-19
SNMP 7-20
Security 7-20
Limitations 7-21
Double-tagged management interface 7-22
Limitations 7-22
Configuring egress packet priority on IP interfaces 7-22
Limitations 7-23
IP unnumbered interfaces 7-24
Limitations 7-25
Virtual switch transform 7-26

List of procedures

7-1 Creating interfaces 7-27
7-2 Deleting an IP or loopback interface 7-30
7-3 Modifying an IP or loopback interface 7-31
7-4 Enabling and disabling an IP interface 7-32
7-5 Configuring IPv6 interfaces manually 7-33
7-6 Displaying an IP interface 7-35
7-7 Creating an IPv6 interface 7-38
7-8 Configuring IPv6 stack settings 7-40
7-9 Setting IPv6 stack settings to default values 7-42
7-10 Enabling and disabling an IPv6 stack 7-43
7-11 Displaying IPv6 stack settings 7-44

Copyright© 2022 Ciena® Corporation

7-12 Configuring IPv4 stack settings 7-45
7-13 Setting IPv4 stack settings to default values 7-46
7-14 Displaying IPv4 stack settings 7-47
7-15 Configuring interface TCP stack settings 7-48
7-16 Setting interface TCP stack settings to default values 7-49
7-17 Displaying TCP stack settings 7-50
7-18 Configuring in-band management bridging 7-51
7-19 Modifying the VLAN for in-band management bridging 7-53
7-20 Adding an IP route 7-55
7-21 Removing an IP route 7-56
7-22 Displaying the routing table 7-57
7-23 Displaying FIB entries 7-58
7-24 Enabling Layer 3 switching 7-60
7-25 Disabling Layer 3 switching 7-61
7-26 Displaying the status of Layer 3 switching 7-62
7-27 Clearing all FIB or AIB entries 7-63
7-28 Enabling logging of FIB or AIB events 7-64
7-29 Displaying FIB information 7-65
7-30 Adding a static ARP entry 7-66
7-31 Removing static ARP entries 7-67
7-32 Configuring EVC ping for use case A 7-68
7-33 Configuring EVC ping for use case B 7-73
7-34 Configuring EVC ping for use case C 7-78
7-35 Configuring EVC ping for use case D 7-82
7-36 Configuring EVC ping for use case E 7-88
7-37 Configuring double-tagged management 7-94
7-38 Displaying double-tagged management 7-96
7-39 Creating an unnumbered IP interface 7-97
7-40 Deleting an unnumbered IP interface 7-99
7-41 Modifying an unnumbered IP interface 7-100
7-42 Displaying static ARP entries 7-101
7-43 Displaying the AIB table 7-102
7-44 Configuring an auxiliary IP interface 7-103
7-45 Generating a ping 7-104

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

About this document

This document describes how to configure advanced Operation, Administration, and Maintenance (OAM) features on 39XX/51XX Switches and Platforms.

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 documentation suite, see *39XX/51XX Switches and Platforms Product Fundamentals*.

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

New in this release

There are no documentation changes in *39XX/51XX Switches and Platforms Advanced OAM Configuration* for SAOS 6.21.2.

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Connectivity Fault Management (CFM) configuration

This chapter describes the Ciena implementation of the IEEE P802.1ag Connectivity Fault Management (CFM) protocol that is used to detect and isolate network service connectivity problems. Topics are

- "Overview"
- "MEF 35 service OAM performance monitoring"
- "CFM on Ethernet type virtual switches"
- "CFM Over Q-in-Q"
- "CFM services on MPLS virtual switches"
- "Enhanced OAM module platforms"
- "CFM service statistics"

Note: In order to configure CFM, you need to install the Advanced OAM (AOAM) license key. To obtain the Advanced-OAM license key, contact Ciena Sales.

Overview

Connectivity Fault Management (CFM) provides a method to continuously monitor the end-to-end network connectivity of a network service, such as a Virtual Switch (VS) or a VLAN. CFM provides utilities to maintain network connectivity including:

- Path discovery—Linktrace messages are used to determine the path taken to a target MAC address.
- Fault detection—CCMs are used to detect both connectivity failures and unintended connectivity between Service Instances.
- Fault verification and isolation—Loopback messages are used to perform fault verification, or to confirm successful initiation or restoration of connectivity. Linktrace messages and loopback messages are used to isolate faults.

Copyright© 2022 Ciena® Corporation

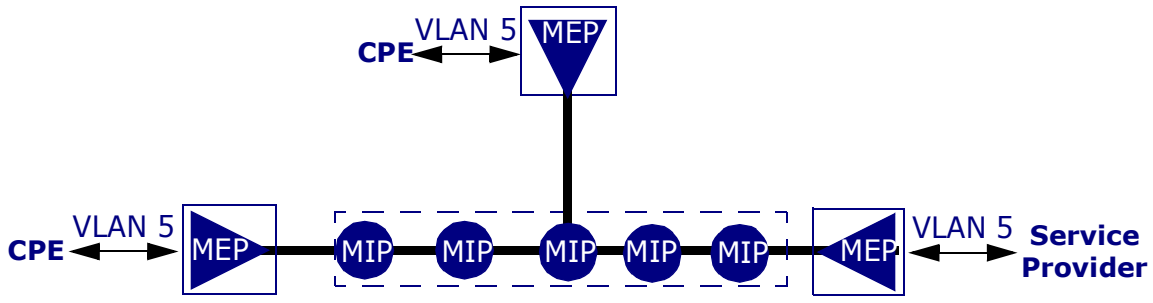
Services can be monitored over a single hop, a point-to-point link, or over multiple hops, using equipment managed by one or more service providers and operations entities. Services are identified by a collection of Service Access Points (SAPs) called a Service Instance. There are two types of SAPs:

- Maintenance End Points: Maintenance End Points (MEPs) are created at the edge (entry/exit) points of the service being monitored.
- Maintenance Intermediate Points: Maintenance Intermediate Points (MIPs) are created between MEPs to track faults at intermediate points.

MEPs send periodic multicast messages (called Continuity Check Messages or CCMs) to each other through the VS or VLAN service to determine the status of the service connection. These can be thought of as heartbeat messages. Devices not configured for CFM forward CCMs as they would any other multicast message. If an expected CCM is not received by a MEP on a participating network device within the specified period, a fault alarm regarding the service is issued in the form of an SNMP trap and system log message.

In Figure 2-1, the service being monitored is VLAN 5. The Maintenance Association (MA) consists of three MEPs (one on each edge of the service) and several MIPs. One of the MEPs monitors VLAN 5 at its source, which is the connection to the service provider. The other two MEPs monitor VLAN 5 at the devices that connect directly to the customer premise equipment (CPE). The MIPs represent one or more CFM-configured network devices used to connect VLAN 5 to multiple subscribers.

Figure 2-1
Example Maintenance Association (MA)



When a MIP is provisioned for a specific VLAN and Maintenance Domain (MD)-level, CFM frames with a matching VLAN and MD-level are switched as customer data frames and forwarded in hardware for DMR, DMM, 1DM, LMM, LMR, SLM, SLR and CCM. If an MEP exists on the same VLAN at a higher MD-level than the MIP, the frame is forwarded to the CPU for further

Copyright© 2022 Ciena® Corporation

processing rather than switched. MD-level 0 is not supported. For any level 0 MIP configured, all CCM and Y1731 frames with level 0 are going through the CPU. This configuration is supported on NNI and UNI ports.

MIP transparency

A MIP's presence does not affect the latency or jitter of CFM frames switched through the VLAN or virtual switch at the same MD level as the MIP unless those frames are linktrace or loopback frames destined for that MIP.

Y.1731 frames or CCM frames are also not affected by the presence or absence of a MIP. Delay measurement frames are consistent regardless of a MIP's presence.

The only exception is where a MEP exists at a higher MD level than a MIP on the same VLAN or virtual switch as a MIP. In this case, the MEP may affect frames at the MIPs by causing them to be forwarded to the CPU for processing. In a normal network configuration the MIP MD levels will be higher than the MEP MD levels.

There is no transparency for CCM frames if the MIP CCM database is enabled.

> ***Note:*** MIP Transparency for Maintenance Domain Level 0 is not supported. For any MIP 0 configured, CCM and Y.1731 frames go through the CPU.

Hardware-based CFM services

All CFM services are software-based by default. When you create a CFM service, you can designate it as accelerated, which moves CCM processing into hardware. Using hardware CFM capabilities reduces the CPU load imposed by software-based CCM processing.

Accelerated CFM services on 3926 and 3928 platforms can only be created after adding the enhanced cfm port.

If a CFM service is hardware-based, all the local and remote MEPs associated with the CFM service are hardware based. Note that only MEPs of type down can be hardware accelerated; hardware-based MEPs of type up are not supported. For more information about up and down MEPs, refer to "MEPs" on page 2-8.

Hardware-assisted CFM is not as feature-rich as software-based CFM. Statistics are not supported. Only the default Ethertype is supported: global can be changed but hardware always uses 0x8902.

Copyright© 2022 Ciena® Corporation

Note that a configuration error is returned when a command violates hardware feature restrictions. The system displays a warning message when a global CFM configuration applies only to software-based services.

CCMs for accelerated sessions impact CPU in some scenarios:

- during remote MEP initialization (discovered and static), CCMs are sent to the CPU for inspection prior to hardware provisioning
- lower-level MD cross-connect fault condition
- unknown MEPID Error CCM faults

Hardware-based CFM is limited to certain ports on some platforms. Table 2-1 lists port limitations for hardware-based CFM.

Table 2-1
Port limitations for hardware-based CFM services

Platform	Accelerated CFM ports	Accelerated local MEPs	Accelerated remote MEPs
3903, 3903x, 3904, 3905, 3906, 3942	All ports	512	2048
3924, 3926, 3928	All ports	192	2048
5142, 5160	All ports	512	2048

Note 1: CCM transmission is not staggered significantly across local MEPs, resulting in CCM bursts when many CFM services are active. While CCMs from software based MEPs are distributed across an interval of several hundred milliseconds, all hardware-based MEPs may transmit within the same millisecond period.

Note 2: Hardware-based CFM services are able to process such CCM bursts without problem. However, software based MEPs handling bursts generated by a hardware based MEPs may result in significant CPU load spikes, and temporarily exhaust internal software frame processing resources. The severity of this issue is dependent on the total number of hardware and software MEPs configured within the same service network, and should be taken into consideration for deployments with a mix of software and hardware-based CFM services.

Maintenance Domains

Unless a dedicated end-to-end physical connection is used, for example, a fiber optic cable, delivering Ethernet services between remote sites typically requires connections through equipment installed and controlled by a separate administrative entity. Each of these entities needs to monitor the status of the services that they are providing in order to be aware of any loss of service and at what point the service has been disrupted.

Copyright© 2022 Ciena® Corporation

In order to monitor the same service through the equipment used by various carrier entities, portions of the network under the control of a common administrative entity are identified by a Maintenance Domain (MD). CFM provides up to eight MDs each numbered from 0-7 to identify its position relative to adjacent CFM domains. The values assigned must be carefully chosen, with the lowest numeric value used for the “inner most” domain levels and higher numbered domain levels assigned in sequence as they are configured outward toward the ends of the service. CFM domains must be fully nested, that is, an inner domain must be fully contained within a surrounding domain.

The default MD level is 3. The MD level does not necessarily have to be changed to configure CFM. The level would only have to be changed when the Operator’s CFM needs are different from what a level 3 MD can provide.

> ***Note:*** If a Maintenance Domain name is changed, it must be changed on *all* other units. The name must be the same on each end point.

The three general types of domains are: Customer, Provider, and Operator. These names are guidelines to indicate the type of entity typically associated with a particular maintenance domain.

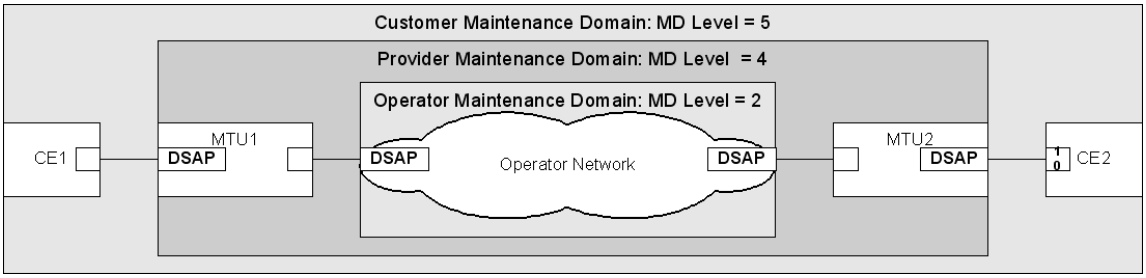
- Customer domains contain the devices connected to the customer and to the source of the service being monitored. For example, if two physically separate business entities are connecting to each other, customer equipment is configured for CFM operation at both ends to monitor the connection, specifying the same domain at both ends. The Customer domain is assigned a level in the range of 5 to 7.
- Provider domains represent the connection used to join each end of the Customer domain. For example, this could be the Internet service provider used by the business. The Provider domain is assigned a level in the range of 3 to 4.
- Operator domains are the central physical infrastructure provider. This could be the owner of a fiber optic network that spans the distance between the cities where the two business units are located. The Operator domain is assigned a level in the range of 0 to 2.

Figure 2-2 shows three Maintenance Domains associated with a Service Instance used to monitor connectivity across a Provider network between two CE devices. Devices CE1 and CE2 reside in the outer-most MD at MD Level 5. The CE devices may be administered by either the Customer or the Provider. The Provider administers devices MTU1 and MTU2 in a second MD at MD Level 4, which is surrounded by the Customer MD. The CE devices connect to the service at Domain Service Access Points (DSAPs) on the boundary between the Customer and Provider MDs. DSAPs are members of the MD that offer the ability to connect to external systems and lie on the edge

Copyright© 2022 Ciena® Corporation

of the MD. These DSAPs correspond to the same physical ports as those associated with the SAPs in Figure 2-2. The example includes a third MD at MD Level 2, contained within the Provider MD. This illustrates that the Provider has contracted with an Operator to transport the service between its MTU devices. The Provider connects its devices to the Operator's network at a second set of DSAPs, which lie on the boundary between the Provider and Operator Maintenance Domains. The Provider has no knowledge of the internal topology or configuration of the network contained within the Operator MD.

Figure 2-2
Nested Maintenance Domains



MEPs pass CCMs of higher relative domain levels without acting on them. For example, when one of the MEPs in the Customer domain sends a CCM, the MEPs in the Provider and Operator domain pass the CCMs on to the MEP at the other end of the Customer domain. This is what allows Connection Fault Management to work across multiple domains. However, CCMs with equal or lower relative domain levels are not passed on by MEPs in order to contain those messages within their respective domains.

Eight permanent Maintenance Domain (MD) levels are available by default. The name for each MD level defaults to “md” followed by the number of the level. For example, *md0*, *md1*, *md2*, and so on. The name for these MDs can easily be changed to adapt to an a network’s naming convention.

> ***Note:*** If a Maintenance Domain name is changed, it must be changed on *all* other devices involved in the service. The name must be the same on each end point.

When two CFM Services at the same MD Level belong to Maintenance Associations that use different MD names, it is necessary to create additional MDs for that level. An MD must be given a locally unique management name used to identify it for configuration purposes. A CFM Service is assigned to an MD by either specifying an MD Level or an MD management name. When an MD Level is specified, the CFM Service is assigned to the default MD for that level.

Copyright© 2022 Ciena® Corporation

An MD Name is encoded in the MAIDs of the CFM services assigned to an MD and is configurable separately from MD management name. An MD Name value can be specified in several different formats, each uses one or more parameters to set the name value. By default, the MD name is a string equal to the MD's management name.

Table 2-2 describes maintenance name formats.

Table 2-2
Maintenance name formats

MD name format	Format type keyword	Format value parameters	CLI example
No MD present	none	N/A	`cfm md set md md4 md-name-format none`
Character string	string	md-name-string	`cfm md set md md4 md-name-format string md-name-string serv`
Domain Name based string	dns	md-name-string	`cfm md set md md4 md-name-format dns md-name-string www.ciena.com`
MAC Address + 2-octet integer	mac-int	md-name-mac-addr md-name-integer	`cfm md set md md4 md-name-format mac-int md-name-mac 00:02:a1:01:23:45 md-name-integer 1000`

When the format of an MD Name is modified, a new MD name value must also be specified. However, if the new name is in the current MD Name format, then the md-name-format parameter is not required.

Maintenance Associations

A Maintenance Association (MA) relates a Service Instance with a Maintenance domain and includes the group of SAPs belonging to the Service Instance. CFM frames carry a Maintenance Association Identifier (MAID) that identifies the connection between SAPs. The MAID includes the Maintenance Domain name along with a Short MA Name.

MAID Configuration

Every CFM Service is logically associated with a Maintenance Association (MA) identified by a Maintenance Association Identifier (MAID). A CFM Service's MAID is constructed indirectly by concatenating the MD Name of its MD with its own Short MA Name.

A CFM Service's Short MA Name is fully configurable, and can be specified in several different formats. Each format uses one or more parameters to set the name value. By default, the short MA name is a string equal to the CFM service name.

Copyright© 2022 Ciena® Corporation

Table 2-3
Maintenance Association Name Formats

Short MA Name Format	Format Type Keyword	Format Value Parameters	CLI Example
Primary VID	vid	ma-name-vid	`> cfm service set service VLAN#1001 ma-name-format vid ma-name-vid 1001`
Character String	string	ma-name-string	`> cfm service set service VLAN#1001 ma-name-format string ma-name-string serv`
2-octet integer	integer	ma-name-integer	`> cfm service set service VLAN#1001ma-name-format integer ma-name-integer 1001`
VPN ID	vpnid	ma-name-vpn-oui ma-name-vpn-index	`> cfm service set service VLAN#1001 ma-name-format vpnid ma-name-vpn-oui 00:02:a1 ma-name-vpn-index 1001`
ICC Based	icc-based	ma-name-string	`> cfm service set service VLAN#1001 ma-name-format icc-based ma-name-string USA1001`

When the format of a short MA name is modified, a new name value must also be specified. However, if the new name is in the current Short MA Name format, then the ma-name-format parameter is not required. In this example a CFM service is created, and its Short MA Name is set to a new string. The short MA name format and value are then changed.

```
cfm service create vlan 20 name VPLS:30203-4 md VPLS:30203-4
cfm service set service VPLS:30203-4 ma-name-string serv
cfm service set service VPLS:30203-4 ma-name-format vpnid ma-name-vpn-oui
00:02:a1    ma-name-vpn-index 1001
```

The detailed information displayed with a CFM service includes a breakdown of its MAID and shows the formats and values of its MD name and short MA name components.

MEPs

MEPs send and receive continuity check messages (CCMs) over the service on a periodic basis to determine if that service is still available. Each MEP is assigned a unique numeric identifier (MEPID) and maintains a table of other MEPs (referred to as remote MEPs) that belong to its MA. This table, called the MEP-CCM-Database, is used to determine if one or more remote MEPs are no longer sending CCMs.

MEPs are directional: Up or Down. The direction determines whether CFM Messages processed by a MEP ingress and egress through its associated logical interfaces (down), or are logically forwarded to and from its logical

Copyright© 2022 Ciena® Corporation

interface from other logical interfaces in the service instance (up). A Down MEP sends CCMs towards and receives them from the physical link to monitor service connectivity from one device to another carrying the same service. This could be a direct connection or a connection through several other devices and MIPs. An Up MEP sends CCMs towards and receives them from other logical interfaces in the service instance.

> ***Note:*** To lessen the number of CCMs lost due to ingress CPU rate limiting on a remote device, the startup of sending CCMs from different MEPs is staggered. Upon system startup or when CFM is globally enabled, each MEP will send CCMs based on ten staggering slots where each slot is separated by 1 second. For example, if you have 64 CFM services configured, and the CCM interval is set to 10 seconds, the CCMs are staggered every second. As a result, at second 0, services 1, 11, 21, 31, 41, 51, and 61 transmit. At second 1, services 2, 12, 22, 32, 42, 52, and 62 transmit, and so on.

MEP transparency

By default, MEPs terminate CFM PDUs that have a lower or equal MD value than the MEP associated with the service. For example, an MD level 2 MEP will drop an MD level 0 CCM. MEP transparency is an optional setting that, when enabled, will allow lower-MD-level CCMs to pass through a higher-MD-level MEP. Once enabled, the MD transparency level can be configured to control for what CCMs the MEP is transparent. For example, if the MD transparency level is set to 1, the MEP is transparent to MD level 0 and 1 CCMs. The transparency setting applies to CCMs received in either direction. When enabled, the default MD transparency level is 0.

MEP transparency applies to CCMs only. Other CFM and Y.1731 messages are not affected.

MEPs in CLI commands

After creation, a MEPs can be identified in one of three ways for all commands that pertain to MEPs:

- By MEPID using the local-mepid parameter. This form is applicable to both subscriber and provider ports, and is the recommended form:

  ```
  cfm mep set service CFM_VLAN_777 local-mepid 2 ccm-
  priority 4
  ```

  Note: In some commands including, `clear, create, delete, disable, enable`, and `show`, the MEPID parameter is identified as `mepid` instead of `local-mepid`.

- By port only. This is applicable to both subscriber and provider ports, but on a provider port, it is the equivalent of specifying the port with vlan 0:

  ```
  cfm mep set service CFM_VLAN_777 port 10 ccm-priority 4
  ```


Copyright© 2022 Ciena® Corporation

- By port and VLAN. This form is applicable to subscriber ports only:

```
cfm mep set service CFM_VLAN_777 port 3 vlan 10 ccm-
priority 4
```

Remote MEPs

A remote MEP monitors connectivity with a service endpoint on another device in the network. Every valid CCM received from a MEP on a remote device that belongs to the same MA as a local service is associated with a remote MEP in the service.

A remote MEP can either be manually created or added to a service upon discovery through CCM reception. Once CCMs are consistently received from a remote MEP for a configurable hold-time, it is automatically activated. Failure to receive a configurable number of consecutive CCMs from an active remote MEP constitutes loss of connectivity with the remote endpoint, and triggers a service fault. Remote MEP discovery can be enabled or disabled per CFM service.

A remote MEP also serves as the target for Loopback and Linktrace operations used for monitoring service health and troubleshooting service faults.

Remote MEP states

The enable/disable operation and hold-state settings are factors in determining remote MEP operational state. The following rules apply to remote MEP states:

- A discovered remote MEP is initially administratively-enabled, while a manually-created remote MEP is initially administratively-disabled.
- A remote MEP can only cause a service fault when it is operationally-enabled.
- A remote MEP that is administratively-disabled is always operationally-disabled.
- Remote MEP hold-state has three settings: enable, disable, and lock.
  - — When a remote MEP is administratively-enabled and its hold-state is "disable", it immediately becomes operationally enabled.
  - — When a remote MEP is administratively enabled and its hold-state is "enable" it will transition to an operational "hold" state, and remains there until it is free of RMEP faults for a period of time equal to the global rmep-hold-time setting. Once this occurs, the remote MEP transitions to an operationally enabled state.

Copyright© 2022 Ciena® Corporation

— If the hold-state is set to "lock", then the behavior in the previous bullet applies, except the remote MEP will remain in an operational "hold" state indefinitely. The "lock" hold-state is used to hold the remote MEP in a diagnostic state that is fully operational other than it cannot trigger a service fault.

MIPs

Like MEPs, MIPs respond to and forward linktrace messages that are used to identify the point in an MA where the service is lost. MEPs and MIPs also respond to loopback messages that are also used to isolate faults at intermediate service nodes. Unlike MEPs, MIPs do not exchange CCMs, but they do act on CCMs and forward them. A MIP is not affiliated with a single MA, and processes CFM protocol frames for all MAs traversing an SI at or optionally at and below its MD Level. Another function of a MIP is to record all CCMs received by a logical interface in order to construct the MIP-CCM Database. This database serves as a record of the CFM monitored services that are using a service instance, and provides a learn table of the MAC addresses used by MEPs. In the event that entries have aged-out of the normal MAC learn table due to a service failure, the MIP-CCM database can be alternatively queried to resolve forwarding information for Linktrace requests during the troubleshooting process.

Continuity Check Messages

CCMs have the following characteristics:

- Transmitted at a configurable interval (see Table 2-26 on page 2-69); the same value is used for all MEPs in the MA.
- Catalogued by MIPs at the same MD level.
- Terminated by remote MEPs at the same MD level.
- Carry information that drives several internal state machines, but do not solicit a response.

Loopback Messages

Loopback messages are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular MEP or MIP. Upon reception, the MEP or MIP transmits a Loopback Reply (LBR) to the initiator. A loopback message can also be configured to contain arbitrary data, which can be used to diagnose faults that are sensitive to frame size, or a specific data pattern.

Linktrace Messages

Linktrace messages are multicast frames that a MEP transmits, at the request of an administrator, to either isolate a service fault to a specific MEP, or to trace the path through the network to a particular MEP or Target MAC address. When the `fdb-only` parameter is specified, only the normal forwarding

Copyright© 2022 Ciena® Corporation

database is used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise. When processing a received linktrace message, the UseFDBonly flag in the message is honored when looking up the target MAC.

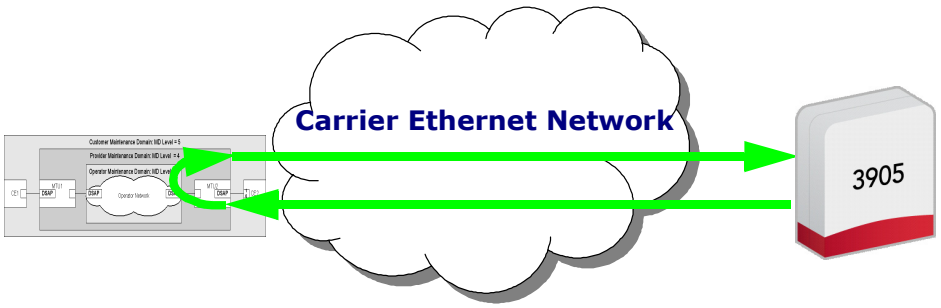
For each visible MIP, linktrace messages indicate ingress action, relay action, and egress action. Linktrace messages also contain a TTL value (configurable), which is decremented each time the Linktrace messages are forwarded by the MEP or MIP. Linktrace messages are multicast, reply messages are unicast.

ITU-T Y.1731 Performance Measurements

Y.1731, introduced by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) complements the IEEE 802.1ag standard, adding the following:

- Frame delay - the Delay Measurement Message (DMM) and the Delay Measurement Reply (DMR) include time stamps that are used to calculate two-way frame delay. These measurements are configured per CFM service. Each MEP can be enabled to perform frame delay and frame delay variation measurements between two point-to-point MEPs in the same MA.
- Jitter - frame delay variation is calculated by tracking the round-trip DMMs. Note that all DMMs expected must be returned in order to make the jitter calculation.
- Frame loss - frame loss is calculated by sending counters within Loss Measurement Messages (LMMs) and Loss Measurement Replies (LMRs). The far-end counters are then compared with the local counters to calculate frame loss for two-way delay measure, port-to-port measurements as a ratio. A bidirectional service is determined unavailable if either of the two directions is declared unavailable, therefore, each MEP must be able to perform near-end and far-end frame loss measurements.

Figure 2-3
Y.1731 Messages Are Initiated Between Two MEPs



Copyright© 2022 Ciena® Corporation

Y.1731 tests are initiated by the network administrator and are sent between two point-to-point MEPs in the same MA. This then triggers the unicast DMMs or LMMs to be sent to the desired remote MEP with a specified packet count at a configurable interval (default is 100 ms). MIPs do not participate in delay/jitter or frame loss measurements.

As an example, in Figure 2-4, MEP 12 could initiate a delay/jitter or frame loss measurement test to MEP 10 or 11. When the test is completed, the delay and jitter measurements from the test will be available and will remain in the system until it is rebooted or another test is run for the same service.

Figure 2-4
Illustration of Path Taken by Y.1731 Messages

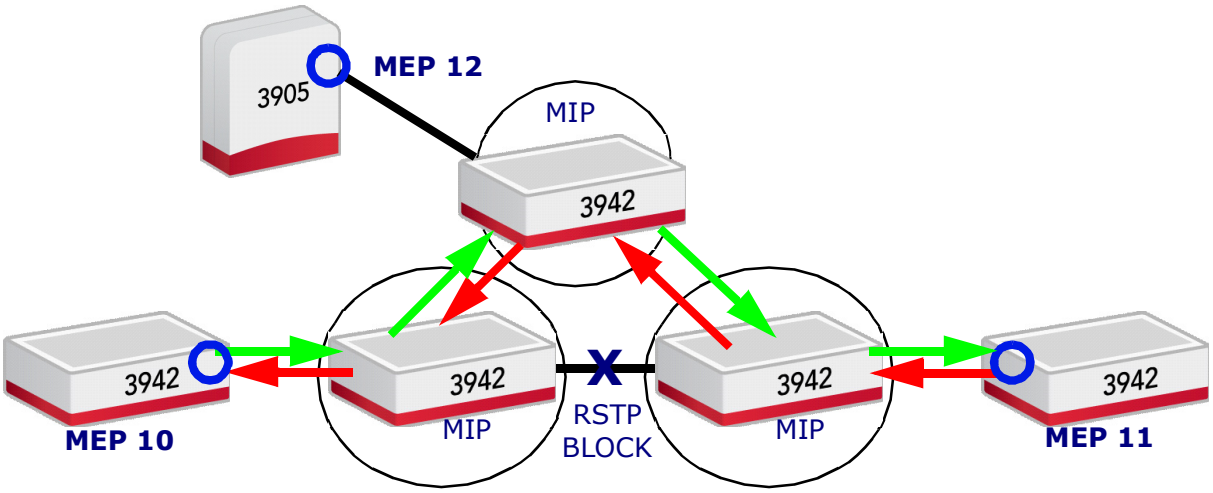


Figure 2-4 displays the path that DMMs and LMMs would take (green lines) and the return path for DMRs and LMRs (red lines) for a test of delay/jitter or frame loss initiated on MEP 10 to MEP 11.

Synthetic Loss Measurement

Synthetic loss measurement (SLM) is a mechanism to measure frame loss using synthetic frames, rather than data traffic. A number of synthetic frames are sent and received, and the system calculates the number of synthetic frames that are lost. This calculation can be treated as a statistical sample, and used to approximate the frame loss ratio of data traffic.

SLM is used to perform on-demand or pro-active tests by sending a finite number of frames with SLM information to a peer MEP and similarly receiving frames with SLM information from the peer MEP.

Copyright© 2022 Ciena® Corporation

A MEP maintains the following local counters for each test ID and for each peer MEP being monitored in a ME for which loss measurements are performed:

- TxFC1, which is the number of synthetic frames transmitted towards the peer MEP and part of a given test ID. A source MEP increments this number for successive transmission of synthetic frames with ETH-SLM request information while a responder MEP increments it for successive transmission of synthetic frames with ETH-SLM reply information.
- RxFC1, which is the number of synthetic frames received from the peer MEP and part of a given test ID. A source MEP increments this number for successive reception of synthetic frames with ETH-SLM reply information while a responder MEP increments it for successive reception of synthetic frames with ETH-SLM request information.

ETH-SLM is an application that lets you calculate frame loss by using synthetic frames instead of data traffic. Each MEP performs frame loss measurements which contribute to unavailable time.

A MEP uses the following values to determine near-end and far-end frame loss in the measurement period:

- Last received SLR frame's TxFCf and TxFCb values and local counter RxFC1 at the end of the measurement period. These values are represented as TxFcF[t_c], TxFCb[t_c] and RxFcI[t_c], where t_c is the end time of the measurement period.
- SLR frame's TxFCf and TxFCb values of the first received SLR frame after the test starts and local counter RxFC1 at the beginning of the measurement period. These values are represented as TxFcf[t_p], TxFCb[t_p] and RxFC1[t_p], where tp is the start time of the measurement period.

The frame loss formula is as follows:

$$\text{Frame loss far-end} = \left| TxFCf[t_c] - TxFCf[t_p] \right| - \left| TxFCb[t_c] - TxFCb[t_p] \right|$$

$$\text{Frame loss near-end} = \left| TxFCb[t_c] - TxFCb[t_p] \right| - \left| RxFC1[t_c] - RxFC1[t_p] \right|$$

No synchronization is required of test ID value between initiating and responding MEPs, as the test ID is configured at the initiating MEP, and the responding MEP uses the test ID it receives from the initiating MEP.

Copyright© 2022 Ciena® Corporation

Table 2-4 describes the meaning of each variable.

Table 2-4
Counter variables

Variable	Meaning
TxFCf	Each SLM frame includes the TxFCf counter value that increments with each SLM sent. The corresponding SLR frame also carries the same TxFcF value.
TxFCb	Each SLR frame included the TxFCb counter value that increments with each SLR sent.
t_p	Corresponds to the start of the measurement period with the first SLR received for a given iteration.
t_c	Corresponds to the end of the measurement period with the last SLR received for a given iteration.

Frame delivery ratio

The Frame delivery ratio is the ratio, expressed as a percentage, of the total number of SLR frames received divided by the total number of SLM frames sent during a certain time period.

Synthetic Loss Transaction generates frame delivery ratio statistics. They are displayed in the output from the SLM show commands.

Frame Delivery Ratio is calculated as follows:

```
Frame delivery ratio = 100 x (RxSLR)/(TxSLM)
```

Frame loss ratio

Frame loss ratio is a ratio, expressed as a percentage, of the number of frames not delivered divided by the total number of frames during an interval of time. The number of frames not delivered is the difference between the number of frames arriving and being delivered to the ingress ETH flow point and the number of frames delivered at the egress ETH flow point in a point-to-point ETH connect or multipoint ETH connectivity.

The frame loss ratio is measured using either service frames or synthetic frames belong to a single CoS. Synthetic frames are also applicable for multipoint ETH connectivity. Service frames are applicable only to point-to-point ETH connections where all the frames arriving at the ingress ETH flow point are to be delivered to the egress ETH flow point.

Copyright© 2022 Ciena® Corporation

The frame loss ratio formula is as follows:

$$FLR\ far\text{-}end = \frac{|\ TxFCf[t_c]\text{-}TxFCf[t_p]\ |\ -\ |\ TxFCb[t_c]\ -\ TxFCb[t_p]\ |}{|\ TxFCf[t_c]\ -\ TxFCf[t_p]|}$$

$$FLR\ far\text{-}end = \frac{|\ TxFCb[t_c]\text{-}TxFCb[t_p]\ |\ -\ |\ RxFC1[t_c]\ -\ RxFC1[t_p]\ |}{|\ TxFCb[t_c]\ -\ TxFCb[t_p]|}$$

One-way delay jitters

The two-way delay measurement transaction is used to calculate One-way jitter, and it generates the statistics that are displayed in the delay show commands. One-way jitter for forward and backward directions is calculated when DMR PDUs are received. DMR PDUs carry timestamp information that is used to calculate the Inter Frame Delay Variation (IFDV). In the IFDV calculation, Far and Near nodes need not be time synchronized. For Jitter calculation, a minimum of two DMR PDU receptions are required.

One-way forward performance jitter: This is the inter-frame delay variation measured in the near- to-far direction. This is calculated as:

$$Jn = Dn - Dn_{-1}$$

where D_n is the delay in forward direction when the nth DMR is received and J_n is the Jitter value.

$$\text{Total Forward Jitter for a transaction} = \Sigma\ Ji, \text{ where i is 1 to n-1.}$$

$$\text{Average Forward Jitter for a transaction} = (\Sigma\ Ji)/\ (n-1).$$

Minimum and maximum forward jitter can be maintained per delay session.

One-way backward performance jitter: This is the Inter Frame Delay Variation in the far-to-near direction. This is calculated as:

$$Jn = Dn - Dn_{-1}$$

where D_n is the delay in backward direction when the nth DMR is received and J_n is the jitter value.

$$\text{Total Backward Jitter for a transaction} = \Sigma\ Ji, \text{ where i is 1 to n-1.}$$

$$\text{Average Backward Jitter} = \text{Summation of } (\Sigma\ Ji)/\ (n-1).$$

Minimum and maximum backward jitter can be maintained per delay session.

$$\text{Total Two-way Jitter} = \text{Total Forward Jitter} + \text{Total Backward Jitter}$$

One-way delay jitter bins: Similar to Two-way Jitter Bins, the Jitter Bin Profile can be selected for One-way Jitters (Forward/Backward) separately. As per the threshold configured in the Jitter Bin Profile, counters are incremented for the corresponding bin when Jitter is calculated.

Copyright© 2022 Ciena® Corporation

One-way delay measurement

One-way delay measurements use the existing DMM/DMR protocol to compute one-way forward and backward delay. The existing two-way DMM/DMR configuration parameters and display CLIs at DMM sessions at the initiator and responder are used for non-accelerated one-way delay measurement sessions. Accelerated hardware assist sessions at initiator and responder are not available for one-way delay sessions.

> ***Note:*** One-way delay measurement is supported on 3903, 3903x, 3905, 3924, 3926, and 3928 platforms.

Using the NTP protocol, you can synchronize the clocks at the initiator and the responder to a common external NTP server. The following describes the two ways to synchronize the two devices using NTP:

- Initiator device: NTP client to an external NTP server

  Responder device: NTP client to the same external NTP server

- Initiator device: NTP client to an external NTP server and server peering enable

  Responder device: NTP client to initiator device (initiator acts as the NTP server)

NTP must be configured first before starting one-way delay measurement tests and wait for enough time for NTP to converge and for the clocks to synchronize. For non-accelerated/one-way delay sessions, DMMs and DMRs are timestamped by CFM software from the clock synchronized by NTP.

Non-accelerate responders must also be configured to ensure correct one-way delay measurements. DMM/DMRs for a delay session are timestamped by CFM software when non-accelerated responders are configured at the responder node for that session.

CFM delay measurements cannot guarantee one-way delay results accuracy. This depends on clock synchronization using the NTP protocol.

Hardware timestamping for software-based DM test sessions is available on the 3924, 3926, 3928, 3942, 5142-931, and 5160 platforms for MPLS transport. On 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved before creating test sessions. When a port is reserved for enhanced CFM, it cannot be used as a front panel port for customer traffic. When a port is reserved for enhanced CFM, the device port is connected to the OAM integrated circuit instead of the front panel port.

Copyright© 2022 Ciena® Corporation

CFM frame processing capabilities

CFM frame processing capabilities vary depending upon several factors. These factors include the CPU utilization and whether hardware or software is used for processing. In general, the 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 switches are capable of processing what is described in Table 2-5.

Table 2-5
CFM frame processing capabilities

<table>
<tr><th colspan="2" rowspan="2">Session Type
System Maximum</th><th colspan="4">Maximum Hardware Accelerated Sessions</th></tr>
<tr><th>5160</th><th>5142-931
3942</th><th>5142-930
390x
393x</th><th>3924, 3926
3928</th></tr>
<tr><td>Local MEPs (CCM Tx)</td><td>1000: 390x, and 393x
4000: All other products</td><td colspan="3">512 at any ccm-interval <= 10 sec</td><td>192</td></tr>
<tr><td>Remote MEPs (CCM Rx)</td><td>8192</td><td colspan="3">2048</td><td>2048</td></tr>
<tr><td>LMM Initiator</td><td>4000</td><td colspan="2" rowspan="2">255 total shared by LMM session types. *
Note: 5142-930 also supports 255.</td><td rowspan="2">120 total shared by both LMM session types. *</td><td>LMM Initiator + LMM Responder = 96(that is Merge LMM Initiator and LMM Responder rows' last column and sum of both these can be less than or equal to 96)</td></tr>
<tr><td>LMM Responder</td><td>8192</td><td></td></tr>
<tr><td>DMM Initiator</td><td>4000</td><td rowspan="4">16000 total shared by DMM and SLM.</td><td rowspan="4">4000 total shared by DMM and SLM.</td><td>0</td><td rowspan="4">8000</td></tr>
<tr><td>DMM Responder</td><td>8192</td><td></td></tr>
<tr><td>SLM Initiator</td><td>4000</td><td></td></tr>
<tr><td>SLM Responder</td><td>8192</td><td></td></tr>
<tr><td colspan="5">Note: In general, accelerated sessions do not consume frame-budget.
* Accelerated LMM consumes frame-budget on these platforms.</td><td></td></tr>
</table>

Copyright© 2022 Ciena® Corporation

Table 2-6 lists the maximum number of OAM enhanced module offloaded DM/SLM sessions supported on 3924, 3926 and 3928 platforms.

Table 2-6
3924, 3926 and 3928 platform support

Interval	SLM initiator (S)	DMM initiator (D)	SLM responder (SR)	DMM responder (DR)	Maximum scale limit conditions
10ms or slower	4000	4000	4000	4000	S+D+SR+DR≤8000, where 0≤S≤4000, 0≤D≤4000, 0≤SR≤4000, 0≤DR≤4000
3.3ms	3000	3000	4000	4000	S+D+SR+DR≤8000, where (0≤S+D≤3000, where 0≤S≤3000, 0≤D≤3000), 0≤SR≤4000, 0≤DR≤4000

Note: OAM enhanced module offloaded DM/SLM sessions are not supported for CFM over MPLS scenarios. For non-MPLS scenarios, the scale numbers shown in Table 2-6 are supported on 3924, 3926 and 3928 platforms.

MEF 35 service OAM performance monitoring

MEF 35 provides service, operations, administration and maintenance that extends the performance monitoring (PM) framework. The following enhancements to CFM/Y.1731 performance monitoring capabilities supports MEF 35 compliance:

- MEF compliant data object indexing — Internal data objects such as MD, CFM service, MEP and Y.1731 session data objects are accessible through other MEF compliant indexes.
- Standard MEF PM session configuration and operation model — A MEF compliant session operation mode that is provisioned through the standard configuration model addresses discrepancies between the legacy SAOS Y.1731 performance monitoring session configuration model and the MEF 35 standard. The legacy session differences include using non-standard keywords for common parameter names, and not supporting some required parameters.

Copyright© 2022 Ciena® Corporation

- Enhanced PM result data sets — Missing statistics are added to the PM result data sets for current and historic measurement intervals. These gaps include:
  - Measured statistics for delay measurement (DM) and synthetic loss measurement (SLM) from the last protocol data unit (PDU) received.
  - Frame delay range (FDR) statistics and associated measurement bin counters.
  - SLM availability related performance metrics.
- Reworked PM session histories — A dedicated history buffer of determined size is individually allocated for each PM session for MEF 35 compliance. The legacy SAOS Y.1731 session history implementation stores history entries for all of a local MEP sessions in a shared history buffer. The amount of history allocated to each session is undetermined and dependent on the configuration of all PM sessions associated with the same MEP.
- Frame delay range — Support for frame delay range PM statistics, which is similar to frame delay, but normalized by subtracting a minimum delay value from all calculated result values.
- Synthetic loss availability — SLM sessions accommodate and report availability related performance metrics.
- Extended CFM CLI command set — New commands for provisioning sessions and displaying them are added to manage PM sessions operating in MEF compliance mode. Show command output accommodates the MEF 35 feature capabilities.
- MEF 36 service OAM performance monitoring MIB — The MIB defined in MEF 36 is supported for PM data retrieval. Access is restricted to read-only for OIDs associated with supported MEF 35 capabilities. MEF compliant PM sessions must be initiated by using the CLI command. MEF sessions can also be initiated by Netconf YANG.

PM session mode

Each PM session operates in one of two modes:

- Legacy mode — Maintains previously supported session behavior and capabilities for maintaining backwards compatibility. Legacy mode is not capable of supporting all functionality required by MEF 35.
- MEF mode — Supports all functionality required by MEF 35, although SAOS does not currently support all MEF 34 requirements. Resources for each PM session type (delay or synthetic loss) are allocated from a common pool. The underlying session data objects support either mode, which is determined by how a session is provisioned.

Copyright© 2022 Ciena® Corporation

A session created using pre-existing CFM CLI commands or the Ciena MIB operates in Legacy mode. A session created using the new alternate CFM MEF CLI command set or set/create operates by means of MEF 36 MIB (or MEF 39 YANG module) operates in MEF mode.

Legacy mode sessions operate the same regardless of MEF mode sessions.

Note: The session mode is determined based on how the PM session was started on the initiator. Responder does not differentiate between MEF mode and legacy mode, and responds to SLM/delay measurement message (DMM) frames in the same way.

PM session types

A MEF mode PM session is classified as a proactive or an on-demand session. A proactive session runs continuously once it has been created and started. Proactive sessions must start immediately and run forever. The default is proactive.

On-demand sessions run when required. Fixed or relative start and stop times can be configured if these values are known. Otherwise, the start time of “immediate” and/or a stop time of “forever” can be specified if the monitoring period is unknown until troubleshooting is completed.

MEF object indexing

MEF 35 PM data models index objects differently than the legacy index objects. To support MEF 35, objects are accessible through MEF compatible indexes and through the existing SAOS indexing. Table 2-7 compares legacy and MEP session keys.

Table 2-7
Legacy and MEP session key comparison

Object	MEF Key		Legacy Key		Notes
	Name	Type	Name	Type	
Maintenance Domain	MD Index	Unsigned32	MD Index	Unsigned16	MD Index is stored internally as an unsigned 16 value. Existing MD APIs can be used by typecasting a 32-bit index value to a 16-bit value.

Copyright© 2022 Ciena® Corporation

Table 2-7
Legacy and MEP session key comparison

Object	MEF Key		Legacy Key		Notes
	Name	**Type**	**Name**	**Type**	
Maintenance Association	MD Index MA Index	Unsigned32 Unsigned32	CFM Service Name or CFM Service Index	String or Unsigned16	A MEF MA object does not correlate directly to a Ciena CFM service object. However, MEF MA APIs allow a CFM service to be exposed as an MA for GET requests.
Local MEP	MD Index MA Index MEPID	Unsigned32 Unsigned32 Unsigned 16	CFM Service MEPID or Port/VLAN	String /U16 Unsigned16 Pgid/VID	Some MEF MEP level data is currently stored in its associated CFM service. The new MEF MEP APIs allow all MEP and service data to be accessed using a MEF compatible key.
Performance Monitoring Session	MD Index MA Index MEPID Session Id	Unsigned32 Unsigned32 Unsigned16 Unsigned32	CFM Service Local MEPID Remote MEPID Test Id	String /U16 Unsigned16 Unsigned16 Unsigned32	MEF session Id is automatically assigned by the system. Every PM session is assigned a session Id, including those operating in legacy mode. However, session Id is only an index component for sessions operating in MEF mode.

Copyright© 2022 Ciena® Corporation

PM session identifier

Every session is assigned a PM session identifier or SessionId that is unique for a local MEP. A SessionId is automatically assigned by the system from an index that continually increments and is maintained per MEP. Delay and synthetic-loss session types are assigned a SessionId from the same index variable. Table 2-8 describes how a SessionId is obtained and used.

Table 2-8
Determining the SessionId

Provisioning Mechanism	Session Mode	SessionId details
Interactive CLI	Legacy	A SessionId is automatically assigned when a session is successfully initiated. A SessionId is not required by legacy CLI commands, and it is transparent to the session operation.
	MEF	A SessionId is automatically assigned when a session is successfully initiated by a CFM MEF CLI command. A message containing the SessionId of the new session is displayed in a CLI message. Subsequent commands referencing the session must specify the Session ID as a parameter.
System Configuration File	Legacy	There is no change to the existing syntax of commands written to the configuration file. The SessionId is automatically assigned as sessions are initiated when the configuration is loaded.
	MEF	The SessionId persists across system reboots and is written to the configuration file. The syntax of the CFM MEP CLI commands written to the configuration file includes SessionId. The SessionId command parameter is accepted when a session is loaded, but not initiated interactively.
SNMP	Legacy	A SessionId is automatically assigned when a session is initiated from the Ciena MIB. The value assigned is not exposed through the Ciena MIB.
	MEF	A SessionID is an index component for all session tables in the service, operation, administration and maintenance PM MIB. If session creation is supported, the next available SessionId is obtained from mefSoamPmMepOperNextIndex.

Copyright© 2022 Ciena® Corporation

Session model information

A MEF 35 compliant PM session is configured using a different parameter set than a legacy PM session. Some parameters differ in name only, while others operate differently between the session modes. This section describes the configuration parameters and operation details for each session model.

Legacy mode session model

A legacy mode session consists of one or more test iterations. Message interval is the frequency at which PDUs are transmitted during each iteration. Test iteration duration is specified indirectly by a message count or directly by a length of time. The end of an iteration includes a configurable Rx timeout period. Response messages not received within this period are lost. Repeat delay is the time to wait between subsequent iterations. Iterations are contiguous when the repeat delay is 0. Performance metric result calculations are finalized and written to session history at the end of each iteration. Iteration count specifies the number of iterations in a session, with a value of 0 indicating that the session runs continuously until canceled. Immediate session start is supported. Figure 2-5 shows a legacy mode session.

Copyright© 2022 Ciena® Corporation

Figure 2-5
Legacy mode session

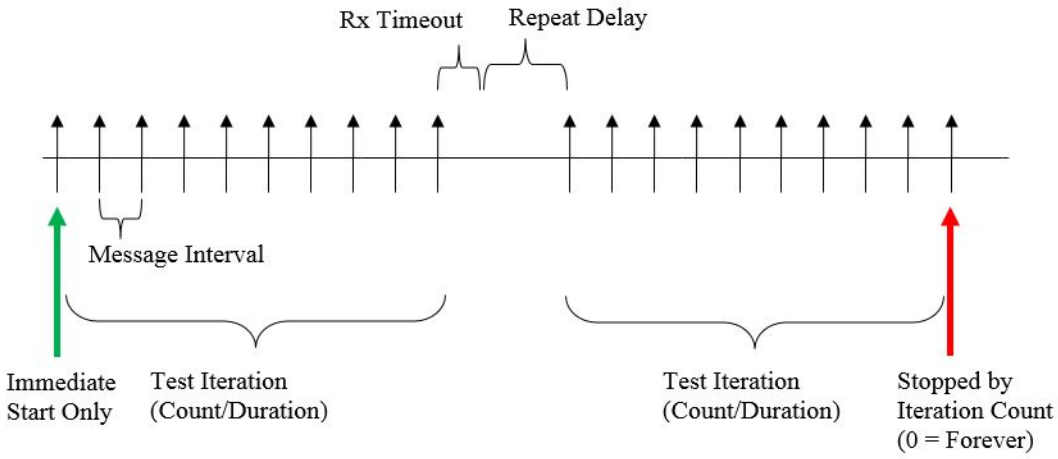


Table 2-9 describes legacy mode session configuration parameters.

Table 2-9
Legacy mode session parameters

Parameter or Term	Description	Notes
CFM Service	Provides CFM service context	
Local MEPID	Provides local MEP context	
Remote MEPID	Provides remote MEP context	Indirectly specifies the target mac-address.
Test ID	Uniquely identifies the session within the service/lmep/rmep context.	Test ID value is explicitly configured and also encoded in TestID PDU fields.
Priority	CoS value encoded in VLAN tag priority bits.	Alternate session identifier for sessions operating in cos-mode.
Message Interval	Frequency of PDU request message transmission	
Message Count	Number of request messages transmitted per test iteration.	Either message count or duration is specified when a session is initiated.
Iteration Duration	Test iteration duration.	The unspecified value is implicitly calculated.

Copyright© 2022 Ciena® Corporation

Table 2-9
Legacy mode session parameters

Parameter or Term	Description	Notes
Rx Timeout	The amount of time to wait for response messages after the last request message in a test iteration is transmitted. Any responses not received before Rx timeout are considered lost.	Included in test iteration duration: Duration = (Message Count - 1_ + Rx Timeout
Repeat Delay	Amount of time to wait between subsequent test iterations.	A value of 0 causes the next test iteration to start immediately after Rx Timeout of the preceding iteration.
Iteration Count	Number of test iterations to execute before the session runs to completion and stops automatically.	A value of 0 causes the session to run continuously until explicitly canceled.
Frame Size	The size of request message PDU frame generated by the local MEP.	The frame is padded to the required size using a Data TLV. The data pattern is not configurable.

MEF mode session

A MEF mode session consists of one or more measurement intervals. The message period is the frequency at which PDUs are transmitted during each measurement interval. The measurement interval duration is a length of time. The repetition period is the time between the start of subsequent measurement intervals. The default value is none, meaning that there is no time gap between the end of one measurement interval and the start of another one.

Measurement intervals are contiguous when the repetition period and measurement interval are the same length. Performance metric result calculations are finalized and written to session history at the end of each measurement interval.

A MEF mode session is proactive or on-demand. A proactive session starts immediately and runs until canceled. An on-demand session can also be scheduled to run at a specified time or a time relative to when it is created. Sessions of both types can be aligned to start at a specific offset relative to the top of the hour.Figure 2-6 shows a MEF mode session.

Copyright© 2022 Ciena® Corporation

Figure 2-6
MEF mode session

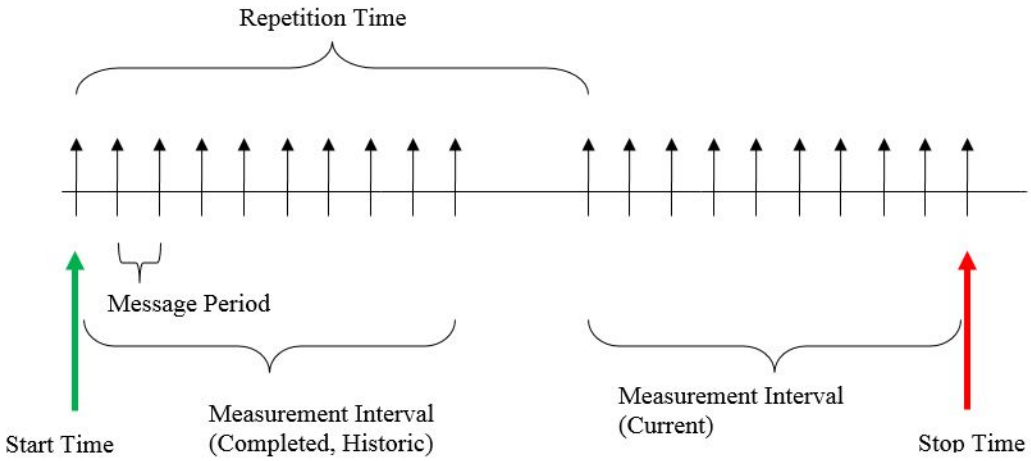


Table 2-10 describes MEF mode session configuration parameters.

Table 2-10
MEF mode session parameters

Parameter or Term	Description	Notes
MD Index	Maintenance Domain context	
MA Index	Maintenance Association context	
MEPID	Local MEPID context	
SessionId	Unique session identifier within the local MEP context. Default is 1.	Automatically assigned by the system per MEF.
Remote MEP	PM session target MEP	Specified by either a MEPID or mac-address.
Priority	CoS value encoded in VLAN tag priority bits.	
Measurement Interval	Discrete interval of time over which a set of PM statistics are calculated and stored.	
Message Period	Frequency of PDU request message transmission.	
Repetition Time	Period of time between the start of subsequent measurement intervals.	A value of 0 causes the next measurement interval to start immediately after the preceding one completes.

Copyright© 2022 Ciena® Corporation

Table 2-10
MEF mode session parameters

Parameter or Term	Description	Notes
Start Time	Scheduled time at which the PM session becomes operational	Multiple modes are supported: • Immediate • Absolute Time • Relative Time The default is Intermediate.
Stop Time	Time at which the PM session terminates.	Multiple modes are supported: • None (runs forever) • Absolute Time • Relative to Start Time The default is None.
Session Type	A session is explicitly designed as proactive or on-demand.	Determines which Stop/Start Time modes are valid.
Align Measurement Intervals	Allows measurement intervals to be aligned with the hour or on a time-of-day clock.	Requires the measurement interval to be evenly divisible by an hour. The default is false meaning the test session will not be aligned.
Alignment Measurement Offset	Allows measurement intervals to be offset a number of minutes from the hour when Align Measurement Intervals is in effect.	
Number of intervals stored	Determines session history size.	The supported range is 2 to 96. The default is 32.
Frame Size	Size of request message PDU frame generated by the local MEP.	PDU is padded using either a Data TLV or Test TLV. If a 0 value is specified, it denotes the default frame size for that test session.

Note: SAOS currently supports frame padding with zeroPattern Data TLV. This value is non-configurable.

Key performance indicators

Key performance indicators (KPIs) are collected on delay measurement sessions and synthetic loss sessions by Y.1731 PM sessions and stored as session result statistics. MEF 35 compliant KPIs are supported on the following platforms: 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160.

Copyright© 2022 Ciena® Corporation

Note: The configuration of performance thresholds is not allowed.

Delay measurement sessions

This section describes the functionality of delay measurement sessions that is required for MEF 35 compliance. The KPIs supported by delay measurement sessions are described in this section.

Inter-frame delay variation

MEF supports configurable selection of DMR frame pairs for inter-frame delay variation (IFDV) measurement purposes.

Note: SAOS does not support configuration selection offset and uses a hard-coded value of 1.

Delay measurement measured statistics

The following PM statistics are maintained per delay measurement session and updated as delay measurement responses are received, but they are not recorded in the session history:

- frame delay (FD) two-way
- inter-frame delay variation (IFDV) two-way
- IFDV forward
- IFDV backward

Note: These statistics are not supported for accelerated sessions.

Delay measurement PM data set

The following general delay measurement PM statistics and related data are maintained for the current measurement interval and stored in the session history for each completed measurement interval:

- Measurement interval index
- Start time
- Elapsed time
- Suspect status
- DMM Tx
- DMR Rx
- Measurement bin two-way FD counters
- Mean two-way FD
- Minimum two-way FD
- Maximum two-way FD
- Measurement bin one-way IFDV forward counters
- Mean one-way IFDV forward

Copyright© 2022 Ciena® Corporation

- Minimum one-way IFDV forward
- Maximum one-way IFDV forward
- Measurement bin IFDV one-way backward counters
- Mean one-way IFDV backwards
- Minimum one-way IFDV backward
- Maximum one-way IFDV backward
- Measurement bin two-way FDR counters
- Mean two-way FDR
- Maximum two-way FDR

Frame delay range

Frame delay range is the normal delay achieved by subtracting the estimated minimum from each delay measurement. As each delay measurement response is received, the estimated minimum is set to the minimum of the current measurement delay and the previous estimate. The minimum delay of a given measurement interval is used as an estimated minimum at the beginning of the following measurement interval.

Note: SAOS supports maximum and mean two-way FDR.

Measurement bins

Delay measurement results (FD, IFDV, FDR) are recorded in measurement bins on a per-measurement-interval basis. SAOS supports a configurable number of bins for FD, IFDV and FDR to record two-way measurements. A measurement bin is a counter that records the number of performance measurements falling within a specified range.

Each bin is associated with a specific range of observed delay, IFDV or FDR. as bins are contiguous, with each bin configured with its lower bound. The lowest bin is assumed to always have a lower bound of zero, and the highest bin is assumed to have an upper bound of infinity. Table 2-11 shows how three bins can be used to count measurements falling in their respective ranges.

Table 2-11
Bin measurements

Bin	Lower Bound (in us)	Range
0	0	0 less than or equal to measurement less than 5000 us
1	5000	5000 us less than or equal to measurement less than 10000 us
2	10000	10000 us less than or equal to measurement less than infinity

Copyright© 2022 Ciena® Corporation

Each measurement bin is associated with a single counter. It is set to 0 at the start of the measurement interval and is incremented to record the number of measurements falling within the range represented by that bin.

> ***Note:*** A bin 0 counter does not need to be implemented because it can be determined by subtracting summation of all other bins from the total number of measurements.

Service performance metrics are defined in terms of percentile of FD, IFDV or FDR. One-way results are preferred for performance measurement between ingress and egress UNIs. However, as one-way delay is difficult to measure, therefore, one-way results are approximated from two-way measurements.

- Frame delay performance is measured between two service endpoints. For example, for an objective between two service endpoints that 95th percentile of delay must be less than 2 milliseconds, if fewer than 5 out of 100 of the received frames have delay of greater than 2 milliseconds, then the 95th percentile of delay must be less than 2 milliseconds.
- Inter-frame delay variation (IFDV) is measured between two service endpoints. A minimum of two bins and a maximum of 10 bins are supported. A default profile is used when a bin specific profile is not specified.

  To determine if this object is set, one or more of m IFDV bins (defined for those service endpoints) must be configured to have lower bound equal to the IFDV performance objective set for those endpoint pairs.

  Table 2-12 shows the bin measurements for an IFDV object between two service endpoints where the 99.9th percentile is less than 3 milliseconds. These statistics listed were recorded in a given measurement interval having 9000 IFDV measurements.

Table 2-12
IFDV bin measurements

Bin	Lower Bound (in us)	Bin counter
0	0	8500
1	1800	199
2	2100	250
3	2400	50
4	3000	1

  Bin 4 has a lower bound equal to the IFDV performance object of 3 milliseconds.

- Frame delay performance is measured between two service endpoints.

Copyright© 2022 Ciena® Corporation

To determine if this object is set, one of n FDR bins (defined for those service endpoints) must be configured to have lower bound equal to the FDR performance objective set for those endpoint pairs.

You can create a measurement bin profile for frame delay, inter-frame delay variation and frame delay range measurements as follows:

- A measurement bin profile is uniquely identified by a user-defined name.
- A measurement bin profile consists of multiple bins with each bin having a configured threshold.
- A delay session (the combination of service, local MEP and session index) is bound to a profile for recording the results of performance measurement.
- Each session is bound to a default profile for each measurement bin type. The default delay threshold values are 5000, 10,000 and 15,000. The default jitter and FDR threshold values are 5000 and 10,000.

Synthetic loss sessions

This section describes synthetic loss measurement sessions that are required for MEF 35 compliance. The KPIs supported by synthetic loss sessions are described in this section.

SLM PM data set

The following general SLM PM statistics and related data are maintained for the current MI and stored in the session history when each MI completes:

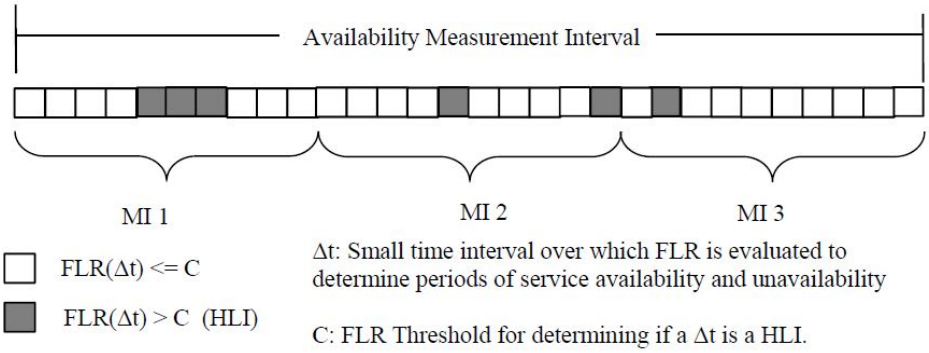
- Measurement interval Index
- Measurement interval start time
- Elapsed time for the measurement interval
- Suspect Status
- SLM transmitted
- SLR received
- Forward transmitted frames
- Forward received frames
- Minimum FLR Forward
- Maximum FLR Forward
- Average FLR Forward
- Backward transmitted frames
- Backward received frames
- Minimum FLR Backward
- Maximum FLR Backward
- Average FLR Backward

Copyright© 2022 Ciena® Corporation

SLM availability

SLM availability defines a way to determine periods of time when a service is available or unavailable. This is done by defining the availability measurement interval (AMI), an interval of time over which availability is evaluated. An AMI may or may not be the same length as the SLM session's normal measurement interval. The AMI can span multiple MIs, as shown in Figure 2-7.

Figure 2-7
SLM availability measurement interval



MEF 35 requires that all frame loss ratio PMs are adjusted to account for periods of unavailability.

The following availability PM statistics and related data are maintained for the current availability measurement interval (AMI) and stored in the session's availability history when each AMI completes.

- Measurement Interval Index
- Start time
- End time
- Elapsed time
- Suspect status
- Forward High Loss
- Backward High Loss
- Forward Consecutive High Loss
- Backward Consecutive High Loss
- Forward Available
- Backward Available
- Forward Unavailable
- Backward Unavailable
- Minimum FLR forward

Copyright© 2022 Ciena® Corporation

- Maximum FLR Forward
- Average FLR Forward
- Minimum FLR Backward
- Maximum FLR Backward
- Average FLR Backward

Session history

Legacy PM session history implementation is not compatible with MEF session history requirements. MEF requires that each session have a dedicated history with a configurable number of entries. Each history entry within a session must be assigned a permanent unique index that is not reused when old entries are removed from a history buffer.

Dedicated per history session history buffers

Legacy sessions store their history in a fixed sized history buffer allocated per local MEP. The number of history entries available for an individual session depends on session configurations for all MEP sessions of the same type.

When the history is full, a new entry overwrites the oldest entry resulting in one session overwriting the history of another when the MEP has multiple sessions of the same type.

Each session history in MEF 35 has a dedicated history with a configurable number of entries. Each history entry within a session is assigned a permanent unique index that is not reused when old entries are removed from a full history buffer. Session history buffers are isolated from each other, and one session can never overwrite entries in another session's history. The history buffer is freed when a session is deleted.The dedicated history buffer exists during the lifetime of the session only.

Session history indexing

MEF requires that the content of a history entry at a given index remains fixed when a new entry is added to a full history buffer, as follows:

- Each new entry is assigned a unique, permanent index from a continually increasing next index variable.
- The oldest history entry always has the lowest index.
- The newest history entry always has the highest index.
- When new entry is stored in a full history buffer, the oldest entry (lowest index) is removed. The newly added entry has the highest index. The contents of the entries for all the other indices is unchanged. As a result, when new entries are added to a full history, the index range continually changes. For example, if the history size is 56 and entries are indexed 200 to 255, the index range becomes 201 to 256 after the next entry is added.

Copyright© 2022 Ciena® Corporation

This dedicated MEF mode session history buffers are indexed using this type of indexing.

Session history backwards compatibility

MEF mode session history entries can only be stored in the MEP history if they have the same content as legacy mode history entries. This is not always the case. As a result, the current shared MEP history for legacy mode sessions is maintained, and a dedicated session history for MEF mode sessions only is allocated. MEF mode session history entries are stored in the dedicated session history only, but excluded from the existing legacy MEP history.

Threshold crossing alerts

Performance thresholds and threshold crossing alerts (TCA) can be configured for certain performance metrics. They can also be used to determine when service performance is degraded beyond a user configured level. If this occurs, a TCA alarm is generated.

Thresholds are always specific to a particular performance metric and a particular PM session. When the measured performance in a measured interval for that session exceeds the configured threshold level, a TCA can be generated and sent to the element management system (EMS) or network management system (NMS).

Performance data is normally collected from a network element by EMS or NMS periodically or on-demand. TCAs can be used as warning notifications to the EMS/NMS of possible service degradation which allows more timely action to resolve the problem. The process that takes a specific threshold configuration for a specific performance metric in a PM session and generates corresponding TCAs is a TCA function.

Note: MEF supports stateless and stateful TCA reporting.

Stateless TCA reporting

Stateless TCA reporting treats each measurement interval separately. Each TCA function has a single configured threshold. When the threshold is reached or crossed in a measurement interval for a specific performance metric, a TCA is generated.

Note: SAOS does not support stateless TCA reporting.

Copyright© 2022 Ciena® Corporation

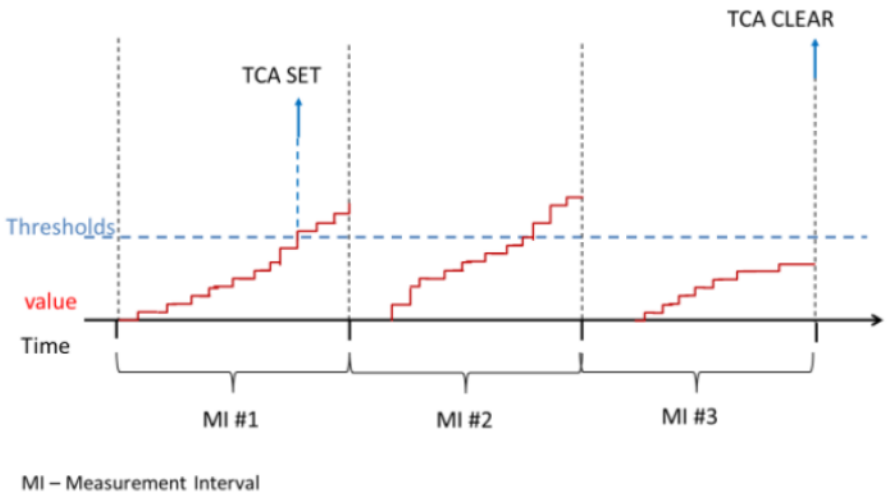
Stateful TCA reporting

Stateful TCA reporting provides notification when the degradation is initially encountered, followed by another notification when the problem is cleared. This type of reporting reduces the number of TCAs. Stateful TCA reporting differs from stateless TCA reporting where TCAs are generated continuously as long as the degradation lasts.

Note: SAOS only supports stateful TCA reporting.

Figure 2-8 shows how stateful TCA reporting works. A set TCA is generated in MI#1. In MI#2, the threshold is crossed again, but no set TCA is generated because a set TCA was generated for MI#1. MI#3 is the first subsequent measurement interval that the measured performance value is below the clear threshold. A clear TCA is generated at the end of MI#3.

Figure 2-8
TCA stateless reporting



TCA profiles

Users can enable TCA reporting for a delay or loss session by attaching a corresponding threshold profile while the session is created. Threshold profiles consist of all performance metrics which are supported for TCA. TCA profiles can only be attached to MEF sessions. TCA profiles cannot be attached with legacy sessions.

The following items must be met when configuring TCA profiles:

- A threshold profile must be uniquely identified by a user-defined name.
- A threshold profile consists of many performance metrics and their corresponding thresholds.

Copyright© 2022 Ciena® Corporation

- A session, the combination of service, local mep and session index, must be bound to a profile for threshold crossing alerts belonging to its respective performance metric.
- By default, there is no profile associated with the test session. Therefore there will be no TCA reporting for such sessions.

OAM system offloaded MEF session

MEF mode sessions can be offloaded to the system to enhance the scale of Y.1731 test sessions.

Platforms that have an OAM system process and generate Service OAM protocol data units and do not route them to the host CPU. This reduces the processing load at the CPU. The keyword “accelerate” is used to create MEF mode sessions and to offload them to the FPGA.

Note: Accelerated MEF mode delay measurement sessions are supported on the 3924, 3926, 3928, 3942, 5142-931, and 5160 platforms.

Copyright© 2022 Ciena® Corporation

Scalability

The Scalability table lists the maximum number of enhanced module offloaded MEF sessions that can be offloaded to the OAM enhanced module.

Table 2-13
Scalability

Platform	Interval	SLM initiator (S)	DMM initiator (D)	SLM responder (SR)	DMM responder (DR)	Maximum scale limit conditions
3942/ 5142-931	All intervals	2000	4000	4000	4000	S+D+SR+DR≤4000, where (0≤S+D≤4000, where 0≤S≤2000, 0≤D≤4000), 0≤SR≤4000, 0≤DR≤4000

Copyright© 2022 Ciena® Corporation

Table 2-13
Scalability

Platform	Interval	SLM initiator (S)	DMM initiator (D)	SLM responder (SR)	DMM responder (DR)	Maximum scale limit conditions
5160	All intervals	2000	4000	8000	8000	S+D+SR+DR≤16000, where (0≤S+D≤4000, where 0≤S≤2000, 0≤D≤4000), 0≤SR≤8000, 0≤DR≤8000
3924/ 3926/ 3928	10 ms or slower	2000	4000	4000	4000	S+D+SR+DR ≤8000, where 0≤S+D≤8000, where 0≤S≤2000, 0≤D≤4000, 0≤SR≤4000, 0≤DR≤4000
	3.3 ms	2000	3000	4000	4000	S+D+SR+DR ≤8000, where (0≤S+D≤3000, where 0≤S≤2000, 0≤D≤3000), 0≤SR≤4000, 0≤DR≤4000

Maintenance Association examples

This section provides the following examples for Maintenance Associations (MA):

- "Provider"
- "Operator"
- "Customer"

Copyright© 2022 Ciena® Corporation

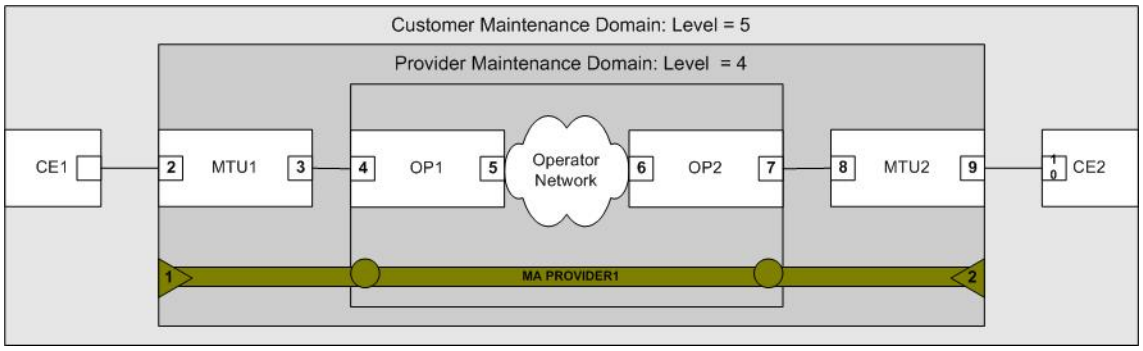
- “Physical Link”

Provider

In this example, a Provider has created a Maintenance Association (MA) to monitor a Service Instance on VLAN 10, associated with a data service sold to the Subscriber. This MA allows the Provider to determine whether or not the fault lies within its own network if a Subscriber reports that the service is down.

For simplicity, this example depicts only the relationship between two MEPs on two Service Delivery Switches in Multi-tenant Units (MTU1 and MTU2). Figure 2-9 depicts the MEP on MTU1, port 2, and MTU2 port 9. The Provider creates Maintenance Association PROVIDER1 at Maintenance Domain Level 4 on each MTU device. MEPs 1 and 2 on port 2 and port 9 respectively are then added to this Maintenance Association.

Figure 2-9
Provider Maintenance Association



In order for the Provider to monitor and troubleshoot service connectivity to the edge of the Operator network, the Operator must expose MIPs at the ports where the service connects to its network. Although the Provider is unable to administratively manage these MIPs, they allow the Provider to use CFM Loopback and Linktrace mechanisms to determine whether or not a service fault lies within the Operator network.

The Operator creates MIPs for VLAN 10 at MD Level 4 in ports 4 and 7. These MIPs are not associated with a specific Maintenance association, and are accessible by any Maintenance Association associated with its VLAN and MD Level. Thus, the Operator is able to provide MIPs to the Provider without specific knowledge of the Provider's Maintenance Association configuration.

Operator

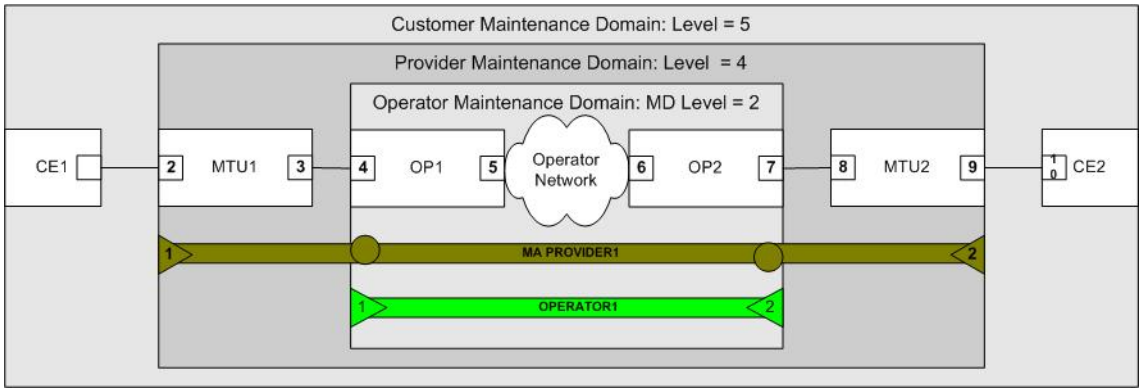
In this example, the Operator (OPERATOR1) and the Provider wish to use CFM to simultaneously monitor the service on VLAN 10. To this end, the Operator creates its own Maintenance Association for the service at

Copyright© 2022 Ciena® Corporation

Maintenance Domain Level 2. This MA allows the Operator to monitor and troubleshoot connectivity for the service within its own network without interfering with the operation of the Provider's Maintenance Association on the same VLAN, but at a higher MD Level.

As shown in Figure 2-10, configuration of this MA requires the creation of the OPERATOR1 Maintenance Association on devices OP1 and OP2, and MEPs on ports 4 and 7. Although not depicted in the diagram, the Operator could also create MIPs on any intermediate devices that transport the service.

Figure 2-10
Operator Maintenance Association



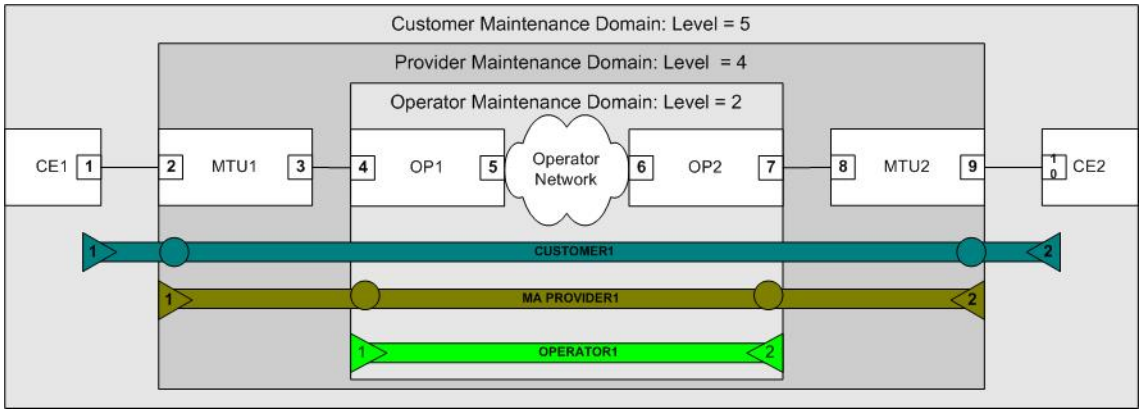
Customer

CFM can also monitor the VLAN 10 service between Subscriber devices in the Customer Maintenance Domain, independent of the Maintenance Associations in the Provider and Operator Maintenance Domains. Although a Customer MA will verify end-to-end service connectivity, the Customer is only able to isolate a fault to a specific link if the fault lies within the Customer Maintenance Domain. A fault can be isolated to the interior of the Provider network, but the Provider must be contacted to further troubleshoot the service disruption.

Figure 2-11 shows a Customer configured MA between the two CE devices. This configuration coexists with the previously defined PROVIDER1 and OPERATOR1 Maintenance Associations. The CUSTOMER1 MA is created on devices CE1 and CE2. MEPs are configured on CE1, port 1 and CE2, port 10. The MIPs shown on the Provider devices MTU1 and MTU2 must be created by the Provider.

Copyright© 2022 Ciena® Corporation

Figure 2-11
Customer Maintenance Association

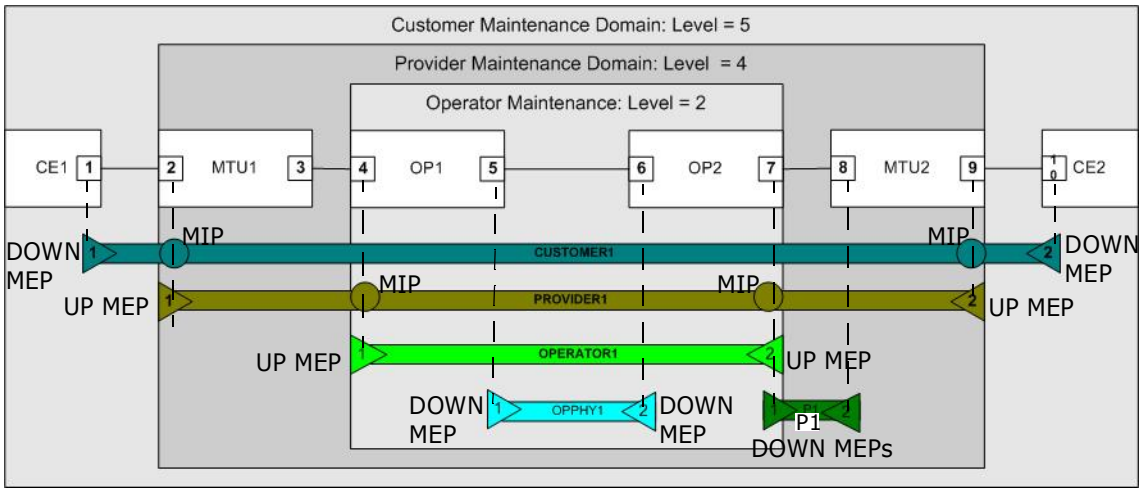


Physical Link

The Maintenance Domain Level 0 is typically reserved for Maintenance Associations that directly monitor physical links. A physical link MA may be associated with a link contained within a single Maintenance Domain, or a link that spans two MDs. Physical Link Maintenance Associations include a MEP on each port at both ends of the link.

In Figure 2-12, two physical link Maintenance Associations have been added to the configuration, OPPHY1 and P1. MA OPPHY1 monitors the link between OP1 port 5 and OP2 port 6. The Operator creates this MA at MD Level 0, so that it will not interfere with the operation of the higher-level Maintenance Associations. Down MEPs are then added to OPPHY1 for the ports at each end of the link.

Figure 2-12
Physical Link Maintenance Association



Copyright© 2022 Ciena® Corporation

Maintenance Association P1 is configured for the physical link connecting the Provider and Operator networks. Therefore, this requires that the Operator and Provider agree on a Maintenance Domain Level and a Maintenance Association name. The Operator and Provider must each create MA P1 on their respective devices. The Operator creates the down MEP for OP2 port 7, while the Provider creates the down MEP for MTU2 port 8. Once configured, MA P1 can be used by both Operator and Provider to monitor VLAN 10 connectivity across the link connecting their networks.

CFM on Ethernet type virtual switches

CFM is supported for Ethernet type Virtual Switches (VS) to provide:

- Service fault monitoring of a provider VLAN associated with an attached virtual circuit.
- Transmission and receipt of Q-in-Q encapsulated CFM frames over a virtual circuit for monitoring of subscriber VLANs.
- Ability to process and forward EVPL bundled CFM frames.

CFM on VS automatically creates an Up MEP on every C-VID on all subscriber ports. This allows connectivity between all service endpoints in the network to be monitored by creating CFM Services for corresponding virtual-switches on other devices in the service. Each device will automatically detect a Remote MEP for all non-local service endpoints. A VS-based CFM service is also dynamic, so if a new subscriber port is added to its associated VS, then a MEP is automatically added to the service for that port. The primary benefit of using a VS-based CFM services is to facilitate connectivity monitoring between all endpoints in a service network. You can also manually create down MEPs on provider ports to monitor provider VLANs.

VS-based CFM services monitor the active VLAN for service faults. If the virtual switch has an attached virtual circuit, the active VLAN is the provider VLAN associated with the virtual circuit. You can configure a CFM service to monitor the active VLAN directly along with a CFM service to monitor the VS as long as the services are at different MD levels.

CFM Over Q-in-Q

The partitioning of a VS into CFM interface groups allows CFM to operate over individual Subscriber VLANs by mimicking the frame transformations applied to data frames forwarded by the VS. Specifically, a CFM frame originating from a MEP in a Subscriber interface, is transmitted out Provider interfaces using Q-in-Q encapsulation, with a C-VID equal to the Subscriber interface VID, and the S-VID equal to the Provider interface VID. Similarly when a Q-in-Q encapsulated CFM frame is received on a Provider interface, it is forwarded to the interfaces in the interface group corresponding to the frame's C-VID tag, after removing the frame's outer S-VID tag.

Copyright© 2022 Ciena® Corporation

CFM Frame Origination

The interface type and VID of a MEP determine how the frames that it originates are initially encapsulated. Table 2-14 describes initial encapsulation at origination.

Table 2-14
Initial encapsulation at origination

Interface type	Initial frame encapsulation
Down MEP on any interface	Frame is single-tagged with interface VID.
Up MEP on Subscriber interface	Frame is single-tagged with interface VID.
Up MEP on Provider interface	Frame is untagged.

A frame transformation is then potentially applied at each egress interface, depending upon the interface type. Table 2-15 shows frame transformation at egress interface.

Table 2-15
Frame transformation at egress interface

Egress interface	Frame transformation
Subscriber egress interface	No transform
Provider egress interface	Push interface VID

Table 2-16 summarizes these Up MEP frame transformations and the resulting frame encapsulation for each possible combination of MEP and egress interface types.

Table 2-16
Encapsulation of Originated CFM Frames

Up MEP Interface Type	Up MEP Interface VID	MEP Frame Encapsulation	Egress Interface Type	Egress Interface VID	Egress Interface Transform	Egress Frame Encapsulation
Subscriber	10	802.1Q VID=10	Provider	300	Push Egress Interface VID	802.1ad S-VID=300 C-VID=10
Subscriber	20	802.1Q VID=20	Subscriber	20	None	802.1Q VID=20
Subscriber	0	Untagged	Subscriber	0	None	Untagged

Copyright© 2022 Ciena® Corporation

Up MEP Interface Type	Up MEP Interface VID	MEP Frame Encapsulation	Egress Interface Type	Egress Interface VID	Egress Interface Transform	Egress Frame Encapsulation
Subscriber	0	Untagged	Provider	200	Push Egress Interface VID	802.1Q VID=200
Provider	N/A	Untagged	Provider	100	Push Egress Interface VID	802.1Q VID=100
Provider	N/A	Untagged	Subscriber	40	None	802.1Q VID=40

Handling CFM Frames Received on a VS

When a CFM frame is received on a VS interface, it may be consumed by a MEP on that interface. If not, it is forwarded to other VS interfaces, each of which may either consume or forward the frame. A frame that is not consumed by the ingress interface is normalized by applying an frame transformation based on the ingress interface type, before it is forwarded. The result of this normalization determines the interface group used for forwarding the frame.

A CFM frame received on a Subscriber interface is not transformed, while the S-VID (outer) tag is popped off a frame that ingresses a Provider interface. If the transformed frame is tagged, then its VID determines the interface group for forwarding. If the frame is untagged, the interface group for VID=0 is used. Table 2-17 summarizes this behavior.

Copyright© 2022 Ciena® Corporation

Table 2-17
Transformation and Forwarding of CFM Frames Received on a VS

Ingress Interface Type	Ingress Interface VID	Ingress Frame Encapsulation	Ingress Transform	Transformed Frame Encapsulation	Action
Subscriber	10	802.1Q VID=10	None	802.1Q VID=10	Forward to all other Subscriber interfaces with VID = 10 and all Provider interfaces.
Subscriber	0	Untagged	None	Untagged	Forward to all other Subscriber interfaces with VID = 0 and all Provider interfaces.
Provider	100	802.1ad S-VID=100 C-VID=20	Pop S-VID	802.1Q VID=20	Forward to all other Provider interfaces and all Subscriber interfaces with VID=20.
Provider	200	802.1Q VID=200	Pop S-VID	Untagged	Forward to all other Provider interfaces and all Subscriber interfaces with VID=0.

CFM services on MPLS virtual switches

A CFM service can be created on an MPLS virtual switch. All MPLS interface types and modes are supported.

Up MEPs are created on attachment circuit virtual switch member ports.

CCMs and other CFM/Y.1731 messages mimic MPLS data frames and are transformed and forwarded/flooded on the virtual switch accordingly. Messages are originated locally by the up MEPs on the attachment circuits. Messages can be received at the virtual circuit or the attachment circuits. Table 2-18 shows how the frame is transformed on ingress and egress depending on the interface, frame type, the MEP type the frame originated from.

Copyright© 2022 Ciena® Corporation

Table 2-18
Transformation of CFM Frames on an MPLS VS

Interface Type	Frame Type	Frame Transform			
		Up MEP Originate	Down MEP Originate	Egress Transform	Ingress Transform
Attachment Circuit	Tagged	Push MEP VID	Push MEP VID	None	None
	Untagged	None	None	None	None
Virtual Circuit	Tagged	N/A	N/A	None	None
	Raw	N/A	N/A	None	None

Enhanced OAM module platforms

An enhanced OAM module allows transmit and receive frame processing for MEPs associated with all device ports to be offloaded to hardware. A frame transmitted by the OAM enhanced port can flood out single or multiple ports. Ingress frame processing supports MEP operations on ingress and egress ports. When an ingress frame classifies as OAM, it is directed to the OAM enhanced port. The enhanced port attempts to classify it to a specific OAM session. If the frame is not associated with an OAM session, they are processed by the software. OAM sessions associated with a single MEP can be distributed between hardware and software-based processing.

The following hardware-based Y.1731 features are supported:

- Up MEP
- Down MEP
- Delay measurement
- Synthetic loss measurement
- CFM over MPLS
- LAG-based MEPs

Note 1: Enhanced OAM module platforms are the 3924, 3926, 3928, 3942, 5142-931 and 5160.

Note 2: OAM enhanced port support for tunneled CFM is supported over MPLS.

OAM session resources

A Y.1731 session that is offloaded to an OAM enhanced port uses one session resource which comprises one transmit and/or one receive operation. Y.1731 sessions are software based by default.

Copyright© 2022 Ciena® Corporation

Table 2-19 describes the session resources required for each configurable session type, and the specific commands to offload each session type.

Table 2-19
OAM session resources

Session type	Protocol operation	OAM session resources	Configuration designed with "accelerate"
DMM initiator session	DMM transmit DMM receive	1 per session	Cfm delay send
DMM responder session	DMM receive DMR transmit	1 per session	Cfm delay-responder create
SLM initiator session	SLM transmit SLR receive	1 per session	Cfm synthetic-loss send
SLM responder session	SLM receive SLR transmit	1 per session	Cfm synthetic-loss-responder send

Offloading sessions to hardware

A session is offloaded to hardware by designating it with the "accelerate" configuration option.

Copyright© 2022 Ciena® Corporation

Table 2-20 describes what happens when sessions are offloaded to hardware.

Table 2-20
Offloading sessions

Offloading session	Description
DMM initiator	• DMM transmit and DMR receive processing for an accelerated delay session is offloaded to the OAM enhanced port. • If the OAM enhanced port does not have enough session resources for a new accelerated delay session, then session creation fails. • An accelerated delay session can be invoked for a MEP in a non-accelerated CFM service.
DMM responder	• DMM receive and DMR transmit processing for an accelerated delay-responder session is offloaded to the OAM enhanced port. • If the OAM enhanced port does not have enough resources for a new accelerated delay-responder session, then session creation fails. • DMMs received from a known remote MEP that are not associated with an accelerated responder session are processed in software.
SLM initiator	• SLM transmit and SLR receive processing for an accelerated synthetic session are offloaded to the enhanced OAM port. • If the enhanced OAM port does not have enough session resources for a new accelerated synthetic-loss session, then session creation fails. • An accelerated synthetic-loss session can be invoked for a MEP in a non-accelerated CFM session.
SLM responder	• SLM received and SLR transmit processing for an accelerated synthetic-loss responder session is offloaded to the OAM enhanced port. • If the OAM enhanced port does not have enough session resources for a new accelerated synthetic-loss-responder session, then session creation fails. • SLMs received from a known remote MEP that is not associated with an accelerated responder session is processed in software. A non-accelerated responder session is created, if required.

Copyright© 2022 Ciena® Corporation

Configuration constraints

Table 2-21 describes the configuration constraints are imposed on accelerated sessions.

Table 2-21
Configuration constraints

Accelerated	Configuration constraint
Up MEP CCM sessions	When multiple up MEPs exist in the same service network and at the same MD level, a multicast CCM floods to each MEP where it is processed independently. The OAM enhanced port cannot support this scenario because a CCM can only classify to a single session. The CFM implementation supports multiple CFM services at the same MD level within a service network, each with its own set of local and remote MEPs. Since the enhanced OAM port cannot accommodate all possible MEP configurations for each CFM sessions, the following restriction is enforced in addition to existing configuration constraints: • An up MEP cannot be created in a CFM service when another MEP in a different CFM service already exists at the same MD level in the service network, unless the new MEP is created on a unique CVLAN. Multiple up MEPs at the same MD level and on a common CVLAN are allowed if they belong to the same CFM service.
TestID range restrictions	The OAM enhanced port supports a 12-bit TestID value to differentiate simultaneous Y.1731 sessions of the same type between a common local and remote MEP pair. The TestID for an accelerated Y.1731 session is restricted to the range: 0-4095.
Test session creation restrictions	On 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved before creating test sessions. Any attempt to create these test sessions without reserving the enhanced CFM port will result in failure.
Accelerated CFM service creation	On 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved before creating offloaded CFM service. Attempts to create the accelerated CFM service without reserving the enhanced CFM port will be rejected. ***Note:*** On 3924, 3926 and 3928 platforms, the accelerate option cannot be set until the enhanced CFM port is reserved on the 3924, 3926 and 3928 platforms.

Copyright© 2022 Ciena® Corporation

Table 2-21
Configuration constraints

Accelerated	Configuration constraint
MIPs disallowed on MD levels with an accelerated CFM service	The following restrictions are enforced to prevent the OAM enhanced port from terminating CCMs that also require MIP processing: • An attempt to create a MIP in a service network that already contains an accelerated CFM service at the same MD level is rejected. • An attempt to create an accelerated CFM service in a service network that already contains a MIP at the same MD level is rejected. An attempt to change to existing CFM service to accelerated when the service network also contains a MIP at the same MD level is rejected.

System scale limits

The total OAM session scale supported by a system comprises the maximum number of sessions supported, and the maximum frame rate of OAM frames that can be processed. The enhanced OAM port offloads frame processing for a subset of sessions from software processes. It does not increase the maximum number of sessions supported by the system. Sessions offloaded to the OAM enhanced port do not consume frame budget resources. Software base sessions continue to be constrained by the CFM frame budget limit.

Table 2-22 lists the maximum number of OAM sessions supported per system with the actual number of sessions that can be offloaded per OAM enhanced port. The OAM enhanced port session resource pool is shared by all session types.

Table 2-22
Maximum OAM sessions

Session type	System maximum	Maximum OAM enhanced port sessions		
		5160	3942, 5142-931	3924,3926,3928
DMM initiator	4000	16000	4000	8000
DMM responder	8192			
SLM initiator	4000			
SLM responder	8192			
Total sessions	48768	16000	4000	8000

Copyright© 2022 Ciena® Corporation

OAM frame rate scale limits

Offloading an OAM session to the OAM enhanced port reduces the CPU resources required for transmit and receive frame processing. Accelerated sessions are exempt from the CFM frame budget, and can be supported independently from the message interval. As a result, the system can process a higher overall OAM frame rate.

An example deployment has each CFM service with four simultaneous delay sessions and four simultaneous synthetic-loss sessions running. The message interval for all session types is 10 milliseconds. Table 2-23 shows a comparison of the maximum number of CFM services with this configuration that the system can support for all software based (non-accelerated) and all enhanced OAM module platform based (accelerated) sessions. Non-accelerated sessions are constrained by the CFM frame budget, while accelerated sessions are constrained by enhanced OAM module platform session resources.

Table 2-23
Example comparison of accelerated and non-accelerated sessions

CFM Service Configuration	Non-accelerated		Accelerated	
	Frame Budget	Enhanced OAM module platforms	Frame Budget	Enhanced OAM module platform
4 x Y.1731 delay	800	0	0	4
4 x Y.1731 synthetic-loss	800	0	0	4
Resources required per CFM service	1600	0	0	8
CFM services supported per system	5000 frame-budget / 1600 resources per service = 3 services		4000 sessions / 8 resources per service = 500 services	

CFM service statistics

CFM Service connectivity can be continually monitored for a set of configured MEP and remote MEP pairs by means of Y.1731 Delay Measurement Message (DMM) or Loss Measurement Message (LMM) test sequences. This is done by specifying a repeat, in minutes between test runs. If a repeat is not specified, the test is only run once. Optional thresholds can also be specified for Delay and Jitter that cause a trap to be generated.

Copyright© 2022 Ciena® Corporation

Thresholds can be set for far-end frame loss, near-end frame loss, delay, and jitter. When a threshold is exceeded, an event/trap is generated. If a test continually exceeds the configured threshold it will not generate continuous events, only when the threshold is crossed, either in rising or falling. Alarms are based on the user-defined normal and peak values.

A continuously-running Y.1731 DMM or LMM test can also be scheduled for a MEP and remote MEP pair that has not yet been discovered. Also, Y.1731 delay and loss tests with a repeat interval specified will be saved in the configuration (during a configuration save) and restored when the configuration is applied.

The storage of Y.1731 delay binning metrics in the history MIB is supported. You can retrieve the following Delay Measurement bin statistics for prior test iterations for all delay sessions using the CLI and SNMP-MIB session history tables:

- Delay Bin Threshold and Result Counter
- Two-way Jitter Bin Threshold and Result Counter
- Forward Jitter Bin Threshold and Result Counter
- Backward Jitter Bin Threshold and Result Counter

DMM/DMR Hardware Assist (3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, 5160 only)

To support sub-ms accuracy for DMM/DMR latency/jitter measurements, 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 switches automatically support hardware-assisted time stamping. With these switches, the ASIC time stamps DMM/DMR transmitted and received messages. The CPU sends and processes the DMM/DMR messages. This capability is available on all ports of the switch, so CPU load increases as the number of DM sessions increases. However, since the local and remote message processing time is discarded from the delay calculation, the measurements obtained using the ASIC supported DM are more accurate than those obtained from the software-based solution.

Note 1: Hardware-assisted time stamping interoperates with software-based solutions and conforms to the Y.1731 standard.

Note 2: Hardware-assisted time stamping is supported for configurations with the standard Y.1731 Ethertype 0x8902.

Copyright© 2022 Ciena® Corporation

Understanding Ingress CFM Frame Classification

CFM global configuration includes attributes for frame classification type, MD level, and mode. These attributes are automatically managed by the system software.

Table 2-24
Single-tagged CFM Frame Format

DA	SA	0x8100	VID	0x8902	MD Level	Version	OpCode	Flags	FTO	Message Content
		VLAN Tag		**EtherType**	**CFM Header**					

Note: A MEP is considered active when it and its associated service are enabled. A MIP is always considered active.

This chapter provides the following procedures for CFM:

- “Configuring and displaying CFM global settings” on page 2-57
- “Configuring maintenance domains” on page 2-62
- “Displaying maintenance domains” on page 2-64
- “Creating and deleting CFM services” on page 2-66
- “Setting attributes for CFM services” on page 2-68
- “Enabling and disabling a CFM service” on page 2-73
- “Displaying CFM services” on page 2-74
- “Configuring a hardware-based service” on page 2-79
- “Moving a CFM service between hardware and software” on page 2-81
- “Moving a CFM service between software and hardware” on page 2-82
- “Configuring MEPs” on page 2-83
- “Setting MEP attributes” on page 2-86
- “Deleting a MEP” on page 2-88
- “Enabling and disabling a MEP” on page 2-89
- “Displaying MEPs” on page 2-91
- “Creating a remote MEP” on page 2-94
- “Deleting a remote MEP” on page 2-96
- “Enabling and disabling remote MEPs and MEP discovery” on page 2-97
- “Displaying remote MEPs” on page 2-99
- “Creating MIPs” on page 2-102
- “Deleting MIPs” on page 2-103
- “Enabling and disabling the MIP database” on page 2-104

Copyright© 2022 Ciena® Corporation

- "Displaying MIP configuration and MIP database" on page 2-105
- "Sending and displaying loopback messages" on page 2-106
- "Sending and displaying linktrace messages" on page 2-109
- "Configuring Y.1731 DMMs" on page 2-114
- "Configuring DMM responders" on page 2-121
- "Displaying statistics" on page 2-124
- "Configuring Y.1731 LMMs" on page 2-133
- "Configuring LMM responders" on page 2-140
- "Configuring single-ended synthetic frame loss measurement" on page 2-143
- "Displaying and clearing CFM statistics" on page 2-148
- "Displaying CFM port stack information" on page 2-156
- "Configuring a VLAN CFM service" on page 2-157
- "Configuring CFM services for a virtual switch service" on page 2-159
- "Configuring CFM over MPLS" on page 2-161
- "Displaying SLM frame loss test results" on page 2-168
- "Configuring a MEF 35 compliant delay session" on page 2-169
- "Configuring a MEF 35 compliant synthetic loss measurement session" on page 2-172
- "Deleting a MEF 35 compliant delay session" on page 2-176
- "Deleting a MEF 35 compliant synthetic loss measurement session" on page 2-177
- "Disabling a MEF 35 compliant delay measurement session" on page 2-178
- "Disabling a MEF 35 compliant synthetic loss measurement session" on page 2-179
- "Configuring a MEF 35 compliant frame delay range" on page 2-180
- "Configuring a MEF 35 frame delay range bins lower threshold" on page 2-181
- "Deleting a MEF 35 frame delay range binning profile" on page 2-182
- "Displaying MEF 35 delay measurement information" on page 2-183
- "Displaying MEF 35 synthetic loss session information" on page 2-189
- "Displaying MEF 35 SOAM sessions on a MEP sorted by session index" on page 2-196
- "Displaying MEF 35 frame relay range profiles" on page 2-197

Copyright© 2022 Ciena® Corporation

- “Creating a MEF 35 compliant threshold profile” on page 2-199
- “Deleting a MEF 35 compliant threshold profile” on page 2-200
- “Configuring parameters to a MEF 35 compliant threshold profile” on page 2-201
- “Attaching a threshold profile to MEF 35 compliant sessions” on page 2-204
- “Displaying MEF 35 compliant threshold profiles” on page 2-206

Copyright© 2022 Ciena® Corporation

Procedure 2-1
Configuring and displaying CFM global settings

You can

- enable CFM
- disable CFM (default state)
- set CFM attributes
- display CFM attributes, resources, and statistics

Step	Action
To enable CFM	
1	Enable CFM: `cfm enable`
To disable CFM	
2	Disable CFM: `cfm disable`
To set CFM attributes	
3	Configure CFM attributes: `cfm set {dot1ad-strict <on|off>} {ethertype <NUMBER: 2048..65535>} {l2-loop-detect <on|off>} {lbm-default-count <NUMBER: 1..3000>} {lbm-default-interval <NUMBER: 10..60000>} {lbm-default-timeout <NUMBER: 2000..10000>} {slm-default-count <NUMBER: 2..4294967295>} {slm-default-interval <2|3|4|5|6|7|10ms|100ms|1sec|10sec|1min| 10min>} {slm-default-timeout <MILLISECONDS: 2000..10,000>} {mip-level-enforcement <on|off>} {vs-automatic-meps <on|off>} {y1731ethertype <NUMBER: 2048-65535>}{dmm-default-count <2..65535>} {dmm-default-interval < dmm-interval-enum>}{dmm-default-timeout <MILLISECONDS: 2000..10,000>}{lmm-default-count <2..65535>} {lmm-default-interval <lmm-interval-enum>{lmm-default-timeout <MILLISECONDS: 2000..10,000>}`

Copyright© 2022 Ciena® Corporation

where

dot1ad-strict <on|off>	when enabled, only CFM frames that contain a single VLAN tag or are untagged are recognized as CFM frames. A double-tagged CFM frame will be forwarded as a normal data frame on interfaces containing MEPs and/or MIPs, and CFM processing is bypassed. By default, strict compliance is turned on.
ethertype <NUMBER: 2048..65535>	is the Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal). ***Note:*** Ensure that the CFM EtherType is unique Setting the CFM EtherType to the same value an EtherType in use by another protocol can cause other protocol packets to be classified as CFM.
l2-loop-detect <on|off>	enables or disables Layer 2 loop detection. When Layer 2 loop detection is enabled, the device detects, counts, and discards received frames that it originally sent.
lbm-default-count <NUMBER: 1..3000>}	is the global default number of LBMs to send. The default value is 1.
lbm-default-interval <NUMBER: 10..60000>	is the global default LBM interval. The default value is 100ms.
lbm-default-timeout <NUMBER: 2000..10000>	is the global default LBM timeout. The default value is 5000 ms (5 seconds).
slm-default-count <NUMBER: 2..4294967295>	is the global default number of SLMs to send. The default value is 2.
slm-default-interval <2|3|4|5|6|7|10ms |100ms|1sec|10sec|1min| 10min>	is the global default SLM interval. Default value is 100ms.
slm-default-timeout <MILLISECONDS : 2000..10,000>	is the global default SLM timeout. The default value is 5000 ms (5 seconds).

Copyright© 2022 Ciena® Corporation

where

mip-level-enforcement <on|off>	When MIP level enforcement is turned on, the MIP processes CFM frames received on an MD level equal to the MIP's configured level. When MIP level enforcement is set to off, the MIP processes CFM frames received on an MD Level equal to or less than the MIP's configured value. Frames at higher MD levels are forwarded in hardware and are not visible to the MIP.
vs-automatic-meps <on|off>	is automatic UNI up MEP creation. The default value is on.
y1731ethertype <NUMBER: 2048..65535>	is the Y.1731 Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal). ***Note:*** On 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 switches, changing the Y.1731 EtherType to a non-default value disables support for hardware assisted time stamping, and a warning message is displayed accordingly.
dmm-default-count <2..65535>	is the global default number of DMMs to send. The default value is 100.
dmm-default-interval <dmm-interval-enum>	is the global default DMM interval. The default value is 100ms.
dmm-default-timeout <MILLISECONDS : 2000..10,000>	is the global default DMM timeout. The default value is 5000 ms (5 seconds).
lmm-default-count <2..65535>	is the global default number of LMMs to send. The default value is 100.
lmm-default-interval <lmm-interval-enum>	is the global default LMM interval. The default value is 100ms.
lmm-default-timeout <MILLISECONDS : 2000..10,000>	is the global default LMM timeout. The default value is 5000 ms (5 seconds)

To restore CFM attributes to default values

4 Restore CFM attributes to default values:

```
cfm unset {dot1ad-strict} {l2-loop-detect} {lbm-default-
count} {lbm-default-interval} {lbm-default-timeout}
{slm-default-count} {slm-default-interval} {slm-default-
timeout} {mip-level-enforcement} {y1731ethertype}{dmm-
```


Copyright© 2022 Ciena® Corporation

```
default-count} {dmm-default-interval}{dmm-default-
timeout}{lmm-default-count} {lmm-default-interval} {lmm-
default-timeout}
```

where

dot1ad-strict	when enabled, only CFM frames that contain a single VLAN tag or are untagged are recognized as CFM frames. A double-tagged CFM frame will be forwarded as a normal data frame on interfaces containing MEPs and/or MIPs, and CFM processing is bypassed. By default, strict compliance is turned on.
ethertype	is the Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal).
l2-loop-detect	enables or disables Layer 2 loop detection. When Layer 2 loop detection is enabled, the device detects, counts, and discards received frames that it originally sent.
lbm-default-count	is the global default number of LBMs to send. The default value is 1.
lbm-default-interval	is the global default LBM interval. The default value is 100ms.
lbm-default-timeout	is the global default LBM timeout. The default value is 5000 ms (5 seconds).
slm-default-count	is the global default number of SLMs to send. The default value is 2.
slm-default-interval	is the global default SLM interval. Default value is 100ms.
slm-default-timeout	is the global default SLM timeout. The default value is 5000 ms (5 seconds).
mip-level-enforcement	When MIP level enforcement is turned on, the MIP processes CFM frames received on an MD level equal to the MIP's configured level. Frames at higher MD levels are forwarded in hardware and are not visible to the MIP. By default, MIP level enforcement is turned on.
vs-automatic-meps	is automatic UNI up MEP creation. The default value is on.
y1731ethertype	is the Y.1731 Ethertype value sent in CFM frames entered in decimal or hexadecimal format. The default is 35074 (0x8902 hexadecimal).
dmm-default-count	is the global default number of DMMs to send. The default value is 100.
dmm-default-interval	is the global default DMM interval. The default value is 100ms.
dmm-default-timeout	is the global default DMM timeout. The default value is 5000 ms (5 seconds).

Copyright© 2022 Ciena® Corporation

where

lmm-default-count	is the global default number of LMMs to send. The default value is 100.
lmm-default-interval	is the global default LMM interval. The default value is 100ms.
lmm-default-timeout	is the global default LMM timeout. The default value is 5000 ms (5 seconds)

To display configuration, resources, and statistics

5 Display global CFM configuration, resources, and statistics:

```
cfm show [statistics]
```

where

statistics	displays statistics.

—end—

Example

The following example configures CFM.

```
cfm set ethertype 35272 mep-hold-time 300000 dot1ad-strict on
mip-level-enforcement on
```


Copyright© 2022 Ciena® Corporation

Procedure 2-2
Configuring maintenance domains

You can:

- change the name of a maintenance domain
- create a maintenance domain

Step	Action

To change the name of a maintenance domain

1 Change the name of a maintenance domain

```
cfm md set level <NUMBER: 0-7> name <String[31]>
```

where

level <NUMBER: 0-7>	is the Maintenance Domain level to configure.
name <String[31]>	is the name for the Maintenance Domain. If a Maintenance Domain name is changed, it must be changed on all other units. The name must be the same on each end point.

To create a maintenance domain

2 Create a maintenance domain:

```
cfm md create {md <md>} [level <NUMBER: 0-7>] [md-name-
format <none|dns|mac-int|string>] [md-name-mac-addr
<MacAddress>] [md-name-integer <#>] [md-name-string
<String>]
```

where

md <md>	sets the Maintenance Domain management name, a locally unique name used as an identifier for configuration purposes.
level <NUMBER: 0-7>	is the MD level.
md-name-format <none|dns|mac-int|string>	the Maintenance Domain name is based on domain name, a MAC address + 2 octet integer, or a character-based string. Specifying None allows for compatibility with a Y.1731 MEGID. If not specified, the MD name will be set to the same as the management name.

Copyright© 2022 Ciena® Corporation

where

md-name-mac-addr <MacAddress>	specifies the MAC address when using the mac-int MD name format.
md-name-integer <#>	specifies the 2 octet integer to use with the MAC address when using the mac-int MD name format
md-name-string <String>	is the name of the MD.

—end—

Example

The following example changes the name of a maintenance domain.

```
cfm md set level 7 name CustomerMD7
```

In this example, the first CFM service at MD Level 4 is named *servVPLS:30103-4* and the MD Name component of its MAID is set to *serv*. This CFM service uses the default MD for level 4:

```
cfm md create md diag level 4
cfm service create vlan 20 name VPLS:30203-4 md diag
```

> ***Note:*** Since the second CFM service belongs to a different MD, its MAID can use a different MD Name without impacting the MAID of the first CFM service.

In this example an MD is created, and its MD name is set to a new string, then its format and value are changed.

```
cfm md create md diag level 4

md set md md4 md-name-string serv

cfm md set md md4 md-name-format mac-int md-name-mac
00:02:a1:01:23:45 md-name-int 1000
```


Copyright© 2022 Ciena® Corporation

Procedure 2-3
Displaying maintenance domains

You can:

- display a list of maintenance domains
- display maintenance domain information by level
- display maintenance domain information by name

Step	Action

To display a list of maintenance domains

1 Display a list of maintenance domains:

```
cfm md show
```

To display maintenance domain information by level

2 Display maintenance domain information by level:

```
cfm md show [level <NUMBER: 0-7>] [services] [agent]
```

where

level <NUMBER: 0-7>	shows a summary for the specific Maintenance Domain level.
services	shows service information
agent	retrieves from agent.

To display maintenance domain information by name:

3 Display maintenance domain information by name:

```
cfm md show md [<CfmMd>] [services]
```

where

md [<String>]	is a specific Maintenance Domain.
services	shows service information.

—end—

Example

The following example displays a list of maintenance domains:

```
> cfm md show

+------------------------ CFM MAINTENANCE DOMAINS ------------------------+
|Level |Management Name               |Services|MD Name                    |
+------+------------------------------+--------+---------------------------+
|0     |md0                           |0       |md0                        |
|1     |md1                           |0       |md1                        |
|2     |md2                           |0       |md2                        |
|3     |md3                           |1       |md3                        |
```


Copyright© 2022 Ciena® Corporation

```
|4      |md4                            |0        |md4                            |
|5      |md5                            |0        |md5                            |
|6      |md6                            |0        |md6                            |
|7      |md7                            |0        |md7                            |
|4      |diag                           |0        |diag                           |
|3      |test                           |0        |test                           |
+-------+-------------------------------+---------+-------------------------------+
```

The following example displays maintenance domain information by level.

```
cfm md show level 3

+------------- CFM MAINTENANCE DOMAIN INFO ---------------+
| Parameter             | Value                           |
+-----------------------+---------------------------------+
| Level                 | 3                               |
| Name                  | md3                             |
| Index                 | 4                               |
| Number of Services    | 2                               |
| MD Name               | md3                             |
| MD Name Length        | 3                               |
| MD Name Format        | String                          |
+-----------------------+---------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-4
Creating and deleting CFM services

You can:

- Create CFM services for virtual switches, and VLANs. Multiple CFM services can be created at the same MD level in a common VS or VLAN. Only a single MEP or MIP is allowed per interface MD level, but MEPs at the same MD level can belong to different CFM services.
- Delete a CFM service.

Step	Action

To create a CFM service

1 Create a CFM service:

```
cfm service create {static-backup-pbt <static-backup-pbt>
|static-pbt <static-pbt> | vlan <VlanList> |vs
<VirtualSwitchName>} [accelerate] [default-mep-type
<up|down>] [level <NUMBER: 0-7>] [ma-name-format <icc-
based|integer|string|vid|vpnid>] [ma-name-integer
<NUMBER: 0-65535>] [ma-name-string <String>] [ma-name-vid
<VlanId>] [ma-name-vpn-oui <Oui>] [ma-name-vpn-index
<NUMBER>] [md <CfmMdName>] [name <String[45]>] [next-
mepid <NUMBER:1-8191>]
```

where

{static-backup-pbt <static-backup-pbt> | static-pbt <static-pbt> | vlan <VlanList> |vs <VirtualSwitch Name[15]>}	is the name or ID of the VLAN(s), or virtual switch to monitor.
accelerate	identifies the service as a hardware-assisted service.
default-mep-type <up|down>	determines the type of MEP to create for a service when the type is left unspecified. Default is none.
level <NUMBER: 0-7>	is the Maintenance Domain Level for the service. The default is 3.
ma-name-format <icc-based| integer| string|vid|vpnid>	is the short Maintenance Association (MA) name format. The default is “string.”

Copyright© 2022 Ciena® Corporation

where

ma-name-integer <NUMBER: 0-65535>	is the short MA name 2 octet integer.
ma-name-string <String>	is the short MA name character string.
ma-name-vid <VlanId>]	is the short MA name primary VLAN ID.
ma-name-vpn-oui <Oui>	is the short MA name VPN Organizationally Unique Identifier (OUI).
ma-name-vpn-index <NUMBER>	is the short MA name VPN index.
md <CfmMdName>	is the Maintenance Domain name.
name <String[45]>	is a unique name for the service. By default, the name matches the virtual switch or VLAN associated with the service. This identifier will be used as the Short MA Name of its associated MA. The link partner associated with the same service on the far end must be configured with the same identifier for CFM to function correctly.
next-mepid <NUMBER:1-8191>	CFM has a configurable nextMepid value, with the range 1-8191, which is used to determine default MEPIDs. When a MEP is created without a specified MEPID, the current value of nextMepid will be used as the MEPID of the new MEP, and then incremented by one. If the resulting value of nextMepid is already used by an existing MEP, nextMepid will be continually incremented until a unique value is found. The purpose of nextMepid is to provide a mechanism for generating MEPIDs that are unique in the MA across all devices in the Service network. Be sure to assign each device a nextMepid value that will guarantee MEPID uniqueness across all MEPs.

To delete a CFM service

2 Delete a CFM service: Deleting CFM on a tunnel will result in the deletion of its dedicated MA and associated MEPs. Also, if any fault states exist on the associated Virtual Switch or VLAN, they are cleared.

```
cfm service delete service <service>
```

where

service <service>	is the service to be deleted.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-5
Setting attributes for CFM services

You can set attributes for CFM services, such as alarm, message transmission intervals, MEP, fault, and remote MEP settings.

Table 2-25 lists priority levels and corresponding defect types for the alarm priority attribute.

Table 2-25
Alarm Priority

Priority Level	Defect Type	Service Fault
1	RDI – Remote Defect Indicator shows that the remote MEP is not receiving CCMs from some other MEP in the service.	RD
2	MAC Status Defect indicates the remote MEP transmitted CCM for a non-forwarding interface.	MS
3	Remote MEP CCM Defect indicates that the local MEP is not receiving CCMs from Remote MEP(s).	RM
4	Error CCM Defect indicates misconfiguration of MEPID or ccm-interval.	CC
5	CCM Cross Connect Defect indicates misconfiguration of MAID or MD Level. When a CCM has an incorrectly configured MAID or MD level, it triggers a Cross Connect Defect (XC) fault. However, this CCM is still counted as a valid CCM, and will increment the valid received (Rx) statistics counter.	XC
6	A new service initially has the Instability (IS) service fault until a stable remote MEP is detected. The service should not have any faults after the remote MEP is detected and determined to be stable. This fault cannot be suppressed by the alarm priority setting, and will always be reported.	IS

Copyright© 2022 Ciena® Corporation

Table 2-26 lists valid CCM, DMM, and LMM intervals.

Table 2-26
CCM, DMM, and LMM Intervals

Interval	Periods
0 or off	Disables CCM transmission from all MEPs in a given Maintenance Association.
3.3ms (DMM, LMM)	3.33 milliseconds. Setting the DMM or LMM Interval to 3.33 milliseconds in software-based CFM services is not recommended, as the results may not be reliable. Use hardware-based CFM services to use this interval. Also, note that faster rates are more CPU-intensive.
3.3ms (CCM)	3.33 milliseconds. Setting the CCM Interval to 3.33 milliseconds in software-based CFM services is not recommended, as the results may not be reliable. Use hardware-based CFM services to use this interval. Also, note that faster CCM rates are more CPU-intensive.
2 or 10ms	10 milliseconds
3 or 100ms	100 milliseconds
4 or 1sec	1 second (Default)
5 or 10sec	10 seconds
6 or 1min	60 seconds. Not supported for hardware-based services.
7 or 10min	10 minutes. Not supported for hardware-based services.

Step	Action
1	Set CFM service attributes:

```
cfm service set service <service> [accelerate]
{[alarm-priority <NUMBER: 1-5>][alarm-time <NUMBER: 0-
36000>][ccm-interval <NUMBER: 0-
7|off|3.3ms|10ms|100ms|1sec|10sec|1min|10min>][csf-
interval <NUMBER: 1-
7|3.3ms|10ms|100ms|1sec|10sec|1min|10min>][csf-loss-
num <NUMBER: 1..255>][csf-dci-num <NUMBER:
1..255>][ccm-loss-bucket-size <NUMBER: 1-60>], [ccm-
loss-num <NUMBER: 1-255>], [ccm-loss-stats
<enable|disable>], [level <NUMBER: 0-7>], [name
<String[31]>], [next-mepid <NUMBER: 1 - 8191>],
[remote-mep-aging-time <NUMBER: 0-3600000>], remote-
```


Copyright© 2022 Ciena® Corporation

```
mep-discovery <enable|disable> [reset-time <NUMBER:
10-36000>], [sender-id-type
<none|chassis|manage|chassis-manage>]}
```

where

service <service>	is the service name.
accelerate	identifies the service as a hardware-assisted service.
alarm-priority <NUMBER: 1-5>	determines what priority level will be used to trigger an alarm. For each fault event, CFM reports a defect type that corresponds to a priority level. If a detected fault's priority level is lower than the alarm priority setting, it will not be reported. The range is 1-5, and the default is 3. For more information, refer to Table 2-25 on page 2-68.
alarm-time <NUMBER: 0-36000>	is the time (in milliseconds) that defects must be present before issuing a Fault Alarm. The Alarm Time starts whenever a fault greater than the Alarm Priority is detected. The range is 0 – 36000 milliseconds. Default = 1000 ms (1 second). The lower the value, the faster a fault alarm is issued.
ccm-interval <NUMBER: 0-7|off|3.3ms|10ms|100ms|1sec|10sec|1min|10min>	is the frequency at which CCM messages are transmitted. The default value is 1 second.
csf-interval <NUMBER: 1-7|3.3ms|10ms|100ms|1sec|10sec|1min|10min>	is the CSF transmission interval index of time. Default is 1 second.
csf-loss -num <NUMBER: 1..255>	is the CSF loss number. Default is 3.
csf-dci-num <NUMBER: 1..255>	is the CSF Dci number. Default is 3.
ccm-loss-bucket-size <NUMBER: 1-60>	is the CCM loss bucket size for CCM loss statistics ranging from 1-60 minutes. The default bucket duration is 15 minutes, which provides a default history of 24 hours.
ccm-loss-num <NUMBER: 1-255>	is the CCM loss number ranging from 1-255.
ccm-loss-stats <enable|disable>	enables or disables CCM loss statistics collection. When enabled, the history of CCM frame sequence errors for a remote MEP are saved. Each sequence error is used to compute the number of CCM frames that have been lost. This number is then added to the current history bucket. SAOS has a total of 96 history buckets. Changes to the enable/disable state or bucket duration flush the history.

Copyright© 2022 Ciena® Corporation

where

level <NUMBER: 0-7>	is the Maintenance Domain Level for the service. The default is 3.
name <String[31]>	is the name for the service. By default, the name matches the virtual switch or VLAN associated with the service.This identifier will be used as the Short MA Name of its associated MA. The link partner associated with the same service on the far end must be configured with the same identifier for CFM to function correctly.
next-mepid <NUMBER: 1 - 8191>	CFM has a configurable nextMepid value, with the range 1-8191, which is used to determine default MEPIDs. When a MEP is created without a specified MEPID, the current value of nextMepid will be used as the MEPID of the new MEP, and then incremented by one. If the resulting value of nextMepid is already used by an existing MEP, nextMepid will be continually incremented until a unique value is found. The purpose of nextMepid is to provide a mechanism for generating MEPIDs that are unique in the MA across all devices in the Service network. Be sure to assign each device a nextMepid value that will guarantee MEPID uniqueness across all MEPs.
remote-mep-aging-time <NUMBER: 0-3600000>	is the time period in milliseconds that a Remote MEP in the service can stay in an RMEP fault state before it is deleted. For example, if it is set to 60000, a Remote MEP will be deleted one minute after CCMs are no longer received from it. The default value is 0, which disables remote MEP aging.
remote-mep-discovery <enable|disable>	enables or disables Remote MEP Discovery for the service. When disabled, Remote MEPs must be explicitly configured and will not be discovered through CCM reception. Since a remote MEP will not be automatically added to the service, if CCMs that are received by one of its MEPs contain an unknown MEPID an Error CCM service fault is triggered.
reset-time <NUMBER: 10-36000>	is the time period for which there should be no fault identified before clearing previous faults.
sender-id-type <none|chassis|manage|chassis-manage>	is the sender ID TLV type.

—end—

Example

The following example disables remote MEP discovery for a service named v100l5.

```
cfm service set service vl100l5 remote-mep-discovery disable
```


Copyright© 2022 Ciena® Corporation

The following example enables remote MEP discovery for a service named v100l5.

```
cfm service set service v100l5 remote-mep-discovery enable
```


Copyright© 2022 Ciena® Corporation

Procedure 2-6
Enabling and disabling a CFM service

When you create a CFM service, it is disabled by default.

After a CFM service is disabled, any fault states will be cleared.

Step	Action

To enable a CFM service

1 Enable a CFM service:

```
cfm service enable service <service>
```

where

service <service> is the service to be enabled.

To disable a CFM service

2 Disable a CFM service:

```
cfm service disable service <service>
```

where

service <service> is the service to be disabled.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-7
Displaying CFM services

You can display:

- Display all CFM services
- Display a specific CFM service
- Display MEPs for a specific CFM service
- Display remote MEP for a specific CFM service

Table 2-27 lists the service faults that are indicated with an "X" for the following service faults.

Table 2-27
Service faults indicated with an X

Service fault	Description
XC (Cross-connect)	Indicates that a CCM was received with an incorrect MAID (MEGID), or was for an MD Level different than the service MD Level. When a CCM has an incorrectly configured MAID or MD level, it triggers a Cross Connect Defect (XC) fault. However, this CCM is still counted as a valid CCM, and will increment the valid received (Rx) statistics counter in the global statistics as shown on page 5-52 for the “RX Total CCM” value.
CC (Error CCM)	Indicates that a CCM was received with an incorrect ccm-interval, or that the Remote MEP's MEPID equals the MEPID of a local MEP in the service. Under certain circumstances, an Error CCM does not register a CC service fault for the service, but does for global CFM statistics. To confirm whether or not this type of fault has occurred, check the global statistics as shown on page 5-52 for the “RX Total CCM-Interval Error CCM” value.
RM (RMEP Error)	Indicates that a CCM not been received from a Remote MEP within 3.5 * ccm-interval.
MS (MAC Status)	Indicates that one or more Remote MEPs report a Port Status fault and are not forwarding.
RDI (RDI)	Indicates that one or more Remote MEPs have detected service faults.
IS (Instability)	Indicates that the service is yet to discover a stable Remote MEP.

Faults indicated here may not have been reported through a service fault event, as that requires a fault to have a priority greater than the service alarm-priority and be present for a period of time longer than the service alarm-time.

Copyright© 2022 Ciena® Corporation

A CFM service that is completely healthy will not have any Service Fault indicators. Some service fault conditions may be expected. For example, if a service has a Remote MEP in a port that is disabled, then the MS fault will always be present.

CFM service configuration includes attributes for frame classification type, MD To create a MEP on a subscriber port C-VID:level, and mode. These attributes are automatically managed by the system software and are described in detail in “Understanding Ingress CFM Frame Classification” on page 2-54.

Step	Action

To display all CFM services

1 Display all CFM services:

```
cfm service show
```

To display a specific CFM service

2 Display a specific CFM service to confirm that the service has no faults.

```
cfm service show service <service>
```

where

service <service> is the CFM service that you want to display.

To display MEPs for a specific CFM service

3 Display MEPs for a specific CFM service:

```
cfm service show service <service> mep
```

where

service <service> is the CFM service that you want to display MEPs for.

To display remote MEPs for a specific CFM service

4 Display remote MEPs for a specific CFM service to confirm that the remote MEPs associated with the service have no faults.

```
cfm service show service <service> remote-mep
```

where

service <service> is the CFM service that you want to display remote MEPs for.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example shows sample output for displaying a specific CFM service. The service VLAN#2005 does not have faults.

```
> cfm service show service VLAN#2005

+--------------------------- CFM SERVICE INFO ---------------------------+
| Parameter             | Value                                          |
+-----------------------+------------------------------------------------+
| CFM Service Name      | VLAN#2005                                      |
| Index                 | 1                                              |
| Service Type          | VLAN                                           |
| Vs or VLAN Name       | VLAN#2005                                      |
| Service Network       | 2005                                           |
| Maint. Domain Level   | 4                                              |
| Maint. Domain Name    | md4                                            |
| MAID                  | md4VLAN#2005                                   |
|   MD Name Format      | Character String                               |
|   MD Name Length      | 3                                              |
|   MD Name             | md4                                            |
|   MA Name Format      | Character String                               |
|   MA Name Length      | 9                                              |
|   Short MA Name       | VLAN#2005                                      |
|   MAID Hex Dump       | Total Length: 16                               |
|                       | 04 03 6D 64 34 02 09 56 4C 41 4E 23 32 30 30 35|
| Admin State           | enabled                                        |
| Oper State            | enabled                                        |
| CCM Interval          | 4 or 1sec                                      |
| VLLI Fault State      | None                                           |
| VLLI Notification     | disabled                                       |
| CCM Loss Number       | 3                                              |
| Alarm Priority        | 2                                              |
| Alarm Time            | 3000                                           |
| Reset Time            | 3000                                           |
| Default MEP Type      | Up                                             |
| Remote MEP Aging Time | 0                                              |
| Remote MEP Discovery  | Enabled                                        |
| Next MEPID            | 161                                            |
| Total MEPs            | 1                                              |
| Active Meps           | 1                                              |
| Total Remote MEPs     | 2                                              |
| Service Faults        |                                                |
| CSF Interval          | 4 or 1sec                                      |
| CSF Loss Number       | 3                                              |
| CSF Dci Number        | 3                                              |
| Last Fault CCM        | [none]                                         |
| CCM Loss Statistics   | Disabled                                       |
| CCM Loss Bucket Size  | 15                                             |
| Frame Classification  | MD Level 4 SvlanOnly                           |
| Accelerated           | No                                             |
+-----------------------+------------------------------------------------+
```

If an "XC" or "CC" fault condition is present, a raw hex dump of the last CCM frame that triggered the fault is shown in the detailed display for the CFM service.

```
> cfm service show service vl10012
```


Copyright© 2022 Ciena® Corporation

```
+-------------------- CFM SERVICE INFO ---------------------------------+
| Parameter             | Value                                         |
+-----------------------+-----------------------------------------------+
| CFM Service Name      | vl100l2                                       |
...
| Service Faults        | XCON                                          |
| Last Fault CCM        | Frame Length: 112                             |
|                       | 01 80 C2 00 00 31 00 02                       |
|                       | A1 31 23 C7 81 00 E0 64                       |
|                       | 89 02 20 01 03 46 00 00                       |
|                       | 02 62 00 3A 04 03 6D 64                       |
|                       | 31 02 07 76 6C 31 30 30                       |
|                       | 6C 31 00 00 00 00 00 00                       |
|                       | 00 00 00 00 00 00 00 00                       |
|                       | 00 00 00 00 00 00 00 00                       |
|                       | 00 00 00 00 00 00 00 00                       |
|                       | 00 00 00 00 00 00 00 00                       |
|                       | 00 00 00 00 00 00 00 00                       |
|                       | 00 00 00 00 01 00 08 06                       |
|                       | 04 00 02 A1 31 23 C7 02                       |
|                       | 00 01 02 04 00 01 01 00                       |
| CCM Loss Statistics   | Disabled                                      |
| CCM Loss Bucket Size  | 15                                            |
| DMM Interval          | 3 or 100ms                                    |
| LMM Interval          | 3 or 100ms                                    |
|-----------------------------------------------------------------------|
```


Copyright© 2022 Ciena® Corporation

The following example shows MEPs for a CFM service named VLAN#1001.

```
> cfm service show service VLAN#1001 mep

+------------------------------- CFM MEPs ----------------------------+
|                |        |     |    |                  |Admin|CCM  |CCM|
|Service         |Port    |Mepid|Type|   Mac Address    |State|State|Pri|
+----------------+--------+-----+----+------------------+-----+-----+---+
|VLAN#1001       |1       |1    |down|00:02:A1:24:0E:32|en   |on   |7  |
+----------------+--------+-----+----+------------------+-----+-----+---+
```

The following example shows remote MEPs for a CFM service named CFM_VLAN_777.

```
> cfm service show service CFM_VLAN_777 remote-mep

+------------------------- CFM REMOTE MEPS ------------------------------+-----------+
|            |     |                 |State|Total |Seq  |Last   |  Fault  |Accelerated|
|Service     |Mepid|Mac Address      |Ad|Op|Rx CCM|Error|Seq Num|F|M|P|I|R|           |
+------------+-----+-----------------+--+--+------+-----+-------+-+-+-+-+-+-----------+
|CFM_VLAN_777|101  |00:02:A1:07:94:00|en|en|1249  |0    |1249   | | | | | |NO         |
+------------+-----+-----------------+--+--+------+-----+-------+-+-+-+-+-+-----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-8
Configuring a hardware-based service

Configure a hardware-based service.

Note: Only MEPs of type down can be hardware-accelerated.

Step	Action
1	Create the CFM service without the “accelerate” attribute. `cfm service create`
2	Set the CFM service attributes. `cfm service set`
3	Enable the CFM service.
4	Create a down MEP on the network facing port: `cfm mep create service <service> port <Port> type down mepid <NUMBER>` where service <service> is the hardware-based CFM service. port <Port> is the port. mepid <NUMBER> is the MEP identifier.
5	Confirm that the service has no faults: `cfm service show service <service>` where service <service> is the CFM service.
6	Confirm that the remote MEPs associated with the service have no faults. `cfm service show service <service> remote-mep` where service <service> is the CFM service.
7	Disable the CFM service: `cfm service disable service <service>` where service <service> is the CFM service that you want to be hardware-assisted.

Copyright© 2022 Ciena® Corporation

8 Set the accelerate attribute:

```
cfm service set service <service> accelerate
```

where

service <service> is the CFM service that you want to be hardware-assisted.

9 Enable the CFM service:

```
cfm service enable service <service>
```

where

service <service> is the CFM service that you want to be hardware-assisted.

10 Confirm that the service has no faults:

```
cfm service show service <service>
```

where

service <service> is the CFM service.

11 Confirm that the remote MEPs associated with the service have no faults.

```
cfm service show service <service> remote-mep
```

where

service <service> is the CFM service.

—end—

Example

The following example creates a hardware-based service.

```
cfm service create vlan 100 name vl100
cfm service set service vl100 ccm-interval 3.33ms
cfm service enable service vl100
cfm mep create service vl100 port 11 type down mepid 10
cfm service show service v1100
cfm service show service v1100 remote-mep
cfm service disable service v1100
cfm service set service v1100 accelerate
cfm service enable service v1100
cfm service show service v1100
```


Copyright© 2022 Ciena® Corporation

Procedure 2-9
Moving a CFM service between hardware and software

Move a CFM service between hardware and software when you no longer want the CFM service to be hardware-assisted.

Step	Action

1 Disable the CFM service:

```
cfm service disable service <service>
```

where

service <service> is the hardware-based CFM service that you want to move to software.

2 Unset the accelerate attribute:

```
cfm service unset service <service> accelerate
```

where

service <service> is the hardware-based CFM service that you want to move to software.

3 Enable the CFM service:

```
cfm service enable service <service>
```

where

service <service> is the hardware-based CFM service that you want to move to software.

—end—

Example

The following example moves a CFM service between hardware and software.

```
cfm service disable service vl100
cfm service unset service vl100 accelerate
cfm service enable service vl100
```


Copyright© 2022 Ciena® Corporation

Procedure 2-10
Moving a CFM service between software and hardware

On the 3924, 3926 and 3928 platforms, CFM service cannot be moved from software to hardware until the enhanced CFM port is reserved. Move a CFM service between software and hardware when you want the CFM service to be hardware-assisted.

Step	Action
1	Disable the CFM service: `cfm service disable service <service>` where service <service> is the CFM service that you want to be hardware-assisted.
2	Set the accelerate attribute: `cfm service set service <service> accelerate` where service <service> is the CFM service that you want to be hardware-assisted.
3	Enable the CFM service: `cfm service enable service <service>` where service <service> is the CFM service that you want to be hardware-assisted.

—end—

Example

The following example moves a CFM service between software and hardware.

```
cfm service disable service vl100
cfm service set service vl100 accelerate
cfm service enable service vl100
```


Copyright© 2022 Ciena® Corporation

Procedure 2-11
Configuring MEPs

Configure MEPs for the CFM service in order for CCM messages to be generated and processed.

CFM over Q-in-Q

When you create a CFM service for Q-in-Q virtual switches, an up MEP is automatically created for each subscriber port by default. A separate MEP is created for each customer VLAN (C-VID) on every subscriber port. You can disable automatic creation of MEPs with the *cfm set vs-automatic-meps* command to accommodate different deployment models and create MEPs manually. For example, you can create a down MEP on a subscriber port for monitoring within the customer network or a down MEP on a provider port to monitor the provider network.

CFM also supports the ability to manually create Up MEPs for EVPL-based VS services using the CVLAN to provide:

- SVLAN service monitoring between subscriber interfaces across the provider network using single-tagged CFM. A port-based Up MEP originates untagged CFM frames that are transmitted single-tagged with the SVLAN out NNIs.

  Note: Configuring an Up MEP on a specific CVLAN injects double-tagged CFM frames into the provider network.

- SVLAN service monitoring between subscriber interfaces on ports that do not actually have a port-based attachment to the VS. A VS that only has specific VLAN members for given subscriber port may require an Up MEP that monitors the entire port and not a single CVLAN.
- Support for a single MEP or MIP that is associated with all CVLANs when CFM frames are double-tagged in the provider network. In this case, a port-based MEP can be configured to originate frames tagged on an arbitrary CVLAN.
- Support for exchanging untagged CFM frames with the customer network.

For manual creation of MEPs, CFM supports the following:

- Multiple port-based MEPs (VLAN 0) on the same subscriber port and same MD level are supported as long as each MEP is associated with a different virtual switch service.
- A port-based MEP can be created on a virtual switch subscriber port that has been added to the virtual switch as a port-based member or if one or more VLANs on the port is a member of the virtual switch.

Copyright© 2022 Ciena® Corporation

- CFM frames received directly on a subscriber port can only be processed by port-based MEPs that are associated with the virtual switch where the ingress port has been added as a port-based member.
- A port-based MEP can process CFM frames forwarded to it from any other interface in the virtual switch service, unless the virtual switch has a VLAN-based interface on the port that is able to handle the frame instead.

The VLAN parameter is specified when creating a MEP on a subscriber port, and cannot be modified for an existing MEP.

Step	Action

To create a MEP

1 Create a MEP:

```
cfm mep create service <service> port <PortName> [vlan
<VlanId] [type <up|down>] [mepid <NUMBER: 1-8191>]
```

where

service <service>	is the CFM service.
port <PortName>	is the port.
vlan <VlanId>	is the customer VLAN ID specified for MEPs on ports that are members of a virtual switch. The default is 0.
type <up|down>	determines whether CFM Messages processed by a MEP ingress and egress through its associated logical interfaces (down), or are logically forwarded to and from its logical interface from other logical interfaces in the service instance (up). The default type is up.
mepid <NUMBER: 1-8191>	is a numeric identifier unique for every MEP in the Maintenance Association. The default MEPID is the next MEP ID available.

To create a MEP on a subscriber port C-VID:

2 Create a MEP on a subscriber port C-VID:

```
cfm mep create service <service> port <PortName> [vlan
<VlanId] [mepid <NUMBER: 1-8191>]
```

where

service <service>	is the CFM service.

Copyright© 2022 Ciena® Corporation

where	
port <PortName>	is the port.
vlan <VlanId]	is the customer VLAN ID specified for MEPs on ports that are members of a virtual switch. The default is 0.
mepid <NUMBER: 1-8191>	is a numeric identifier unique for every MEP in the Maintenance Association. The default MEPID is the next MEP ID available.

—end—

CFM over MPLS

When you create a CFM service for MPLS virtual switches, an up MEP is automatically created for each member port of the attachment circuit.

Example

The following example creates a MEP.

```
cfm mep create service CFM_VLAN_777 port 10 type down mepid 2
```


Copyright© 2022 Ciena® Corporation

Procedure 2-12
Setting MEP attributes

Set MEP attributes for MEPs.

Step	Action

1 Set MEP attributes:

```
cfm mep set {service <service>} {local-mepid <NUMBER: 1-
8191> | port <PortName> [vlan <Vlan>]} [block-opposite-
fault-threshold <NUMBER>] [block-opposite-fault-time
<NUMBER: 1-3600>] [ccm-comment <String[32]>] [ccm-
priority <NUMBER: 0-7>] [ccm-state <on|off>] [csf-
priority <NUMBER: 0..7>][csf-state <String>][mepid
<NUMBER: 1-8191>] [tag-mode <on|off>] [tag-vid <0-4094>]
[tag-priority <0-7>] [type <up|down>] [transparency-state
<on|off>] [transparency-md-level <NUMBER: 0-7>]
```

where

service <service>	is the CFM service that you want to set MEP attributes for.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>]	is the VLAN.
block-opposite-fault-threshold <NUMBER>	CFM counts the number of frames blocked by a MEP of the opposite type and incorrect level for their direction of travel. A block opposite fault is generated when the block opposite fault frame threshold is exceeded during the configured time window. Default is 0.
block-opposite-fault-time <NUMBER: 1-3600>	is the time window in minutes for generating a block opposite MEP fault. The threshold range is 1- 3600 minutes. Default is 5 minutes.
ccm-comment <String[32]>	is an up to 32 character string used to send an Organizationally Unique Identifier (OUI) TLV with CCMs and to be checked for in received CCMs. The default setting does not include the OUI. The CCM comment is a proprietary feature that is displayed in the Remote MEP details of received CCMs
ccm-priority <NUMBER: 0-7>	is the CCM message priority. Valid values are 0-7. Default is 3.

Copyright© 2022 Ciena® Corporation

where

ccm-state <on|off>	Default is on. For troubleshooting purposes, you can set the state to off, and the MEP will process the CCMs that it receives, but will not transmit any.
csf-priority <NUMBER: 0..7>	is the CSF message priority. Default is 7.
csf-state <String>	is the CSF state. Default is off.
mepid <NUMBER: 1-8191>	is the new MEP Identifier for the specified MEP. Default is the next MEP ID available in the Maintenance Association.
tag-mode <on|off>	enables Customer VLAN ID support for VLAN CFM services.
tag-vid <0-4094>	is the VLAN ID of the additional tag for 802.1ad CFM traffic. Setting the tag-vid to 0 associates the MEP with all VLANs of an EVPL member port.
tag-priority <0-7>	is the dot1p priority encoded in the additional tag.
type <up|down>	is the MEP type. Default is down.
transparency-state <on | off>	enables MEP transparency to frame MD levels that are less than or equal to the transparency-md-level. Default setting is off.
transparency-md-level <NUMBER: 0-7>	sets the CCM MD level at and below which MEP transparency applies. Default value is 0.

—end—

Example

The following example sets the service name to CFM_VLAN_777

```
cfm mep set service CFM_VLAN_777 port 10 mepid 201
```

The following example enables MEP transparency and sets the MD transparency level to 3. The MEP will be transparent to CCMs with MD level 0, 1, 2 or 3.

```
cfm mep set service mse-data transparency-state on

cfm mep set service mse-data transparency-md-level
transparency-md-level 3
```


Copyright© 2022 Ciena® Corporation

Procedure 2-13
Deleting a MEP

Delete MEPs that are no longer in use for a CFM service.

Step	Action

1 Delete a MEP:

```
cfm mep delete service <service> {mepid <NUMBER: 1-8191>
| port <PortName> [vlan <Vlan>]}
```

where

service <service>	is the CFM service name.
mepid <NUMBER: 1-8191>	is the MEP identifier for the MEP that you want to delete.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

Example

The following example deletes the MEP on port 10.

```
cfm mep delete service CFM_VLAN_777 port 10
```


Copyright© 2022 Ciena® Corporation

Procedure 2-14
Enabling and disabling a MEP

Newly created MEPs are automatically enabled. If you disabled a MEP, you can enable it when it is required.

For troubleshooting, you can disable a MEP to prevent processing of CFM messages.

Step	Action

To enable a MEP

1 Enable a MEP:

```
cfm mep enable service <service> {mepid <NUMBER: 1-8191>
| port <PortName> [vlan <Vlan>]}
```

where

service <service>	is the CFM service name.
mepid <NUMBER: 1-8191>	is the MEP identifier for the MEP that you want to enable.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

To disable a MEP

2 Disable a MEP:

```
cfm mep disable service <service> {mepid <NUMBER: 1-8191>
| port <PortName> [vlan <Vlan>]}
```

where

service <service>	is the CFM service name.
mepid <NUMBER: 1-8191>	is the MEP identifier for the MEP that you want to disable.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

—end—

Example

The following example enables the MEP on port 10.

```
cfm mep enable service CFM_VLAN_777 port 10
```


Copyright© 2022 Ciena® Corporation

The following example disables the MEP on port 10.

```
cfm mep disable service CFM_VLAN_777 port 10
```


Copyright© 2022 Ciena® Corporation

Procedure 2-15
Displaying MEPs

You can display:

- a summary of all MEPs
- detailed MEP information for a specific CFM service

Step	Action

To display all MEPs

1 Display all MEPs:

```
cfm mep show
```

To display detailed MEP information for a specific CFM service

2 Display detailed MEP information for a specific CFM service:

```
cfm mep show [service <service> {mepid <NUMBER: 1-8191> |
port <PortName> [vlan <Vlan>]} [order-by-mepid][exclude-
evpl]
```

where

service <service>	is the CFM service name.
mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
order-by-mepid	orders results by mepid.
exclude-evpl	excludes EVPL interfaces.

—end—

Example

The following example displays MEP information for CFM service VLAN#2005 and MEP identifier 160.

```
cfm mep show service VLAN#2005 mepid 160

+------------------------------- CFM MEP INFO -------------------------------------+
| Parameter                          | Value                                       |
+------------------------------------+---------------------------------------------+
| Service                            | VLAN#2005                                   |
| Service Type                       | VLAN                                        |
| VLAN Name                          | VLAN#2005                                   |
| Service Network                    | 2005                                        |
| Port                               | 8                                           |
| VLAN                               | 2005                                        |
| MEPID                              | 160                                         |
| Mac Address                        | 00:03:18:D7:E7:D9                           |
| Type                               | Up                                          |
| Admin State                        | enabled                                     |
```


Copyright© 2022 Ciena® Corporation

```
| Accelerated                          | No                                  |
| CCM State                            | on                                  |
| CCM Priority                         | 7                                   |
| Tag Mode                             | off                                 |
| Tag VID                              | 0                                   |
| Tag Priority                         | 7                                   |
| Block Opposite Fault Threshold       | 0                                   |
| Block Opposite Fault Time            | 5                                   |
| Transparency State                   | off                                 |
| Transparency MD Level                | 0                                   |
| CSF Admin State                      | on                                  |
| CSF Priority                         | 7                                   |
| CSF Tx Type                          | Los                                 |
| CSF Rx Type                          | Dci                                 |
| Next Loopback Sequence Number        | 1                                   |
| Next Linktrace Sequence Number       | 1                                   |
| Rx Total Valid Frames                | 1569758848                          |
| Rx Total Invalid Frames              | 0                                   |
| Rx Invalid Message Overflow          | 0                                   |
| Rx Invalid Port Status TLV           | 0                                   |
| Rx Invalid Interface Status TLV      | 0                                   |
| Rx Invalid Sender ID TLV             | 0                                   |
| Rx Invalid Blocked by Opposite MEP   | 0                                   |
| Rx Transparent Active Side           | 0                                   |
| Rx Transparent Passive Side          | 0                                   |
| Tx CCM                               | 3109156                             |
| Rx Valid CCM                         | 5903692                             |
| Rx CCM In Sequence                   | 1569741449                          |
| Rx CCM Sequence Errors               | 14075                               |
| Rx MD Level Xcon CCM                 | 0                                   |
| Rx MAID Xcon CCM                     | 0                                   |
| Rx MEPID Error CCM                   | 3324                                |
| Rx CCM-Interval Error CCM            | 0                                   |
| Rx Invalid CCM                       | 0                                   |
| Tx Loopback Message                  | 0                                   |
| Tx Loopback Reply                    | 0                                   |
| Rx In-order Loopback Reply           | 0                                   |
| Rx Out-of-order Loopback Reply       | 0                                   |
| Rx Content Mismatch Loopback Reply   | 0                                   |
| Rx Unexpected Loopback Reply         | 0                                   |
| Rx Invalid Loopback Reply            | 0                                   |
| Rx Valid Loopback Message            | 0                                   |
| Rx Invalid Loopback Message          | 0                                   |
| Tx Linktrace Message                 | 0                                   |
| Rx Valid Linktrace Message           | 0                                   |
| Rx Invalid Linktrace Message         | 0                                   |
| Rx Valid Linktrace Reply             | 0                                   |
| Rx Invalid Linktrace Reply           | 0                                   |
| Rx Unexpected Linktrace Reply        | 0                                   |
| Rx Invalid Linktrace Relay Action    | 0                                   |
| Tx Linktrace Reply                   | 0                                   |
| Delay Measurement Repeats            | Disabled                            |
| Delay Measurement Delay (min)        | 0                                   |
| Tx Delay Measurement Message         | 2781894465                          |
| Rx Valid Delay Measurement Message   | 100                                 |
| Rx Invalid Delay Measurement Message | 0                                   |
| Tx Delay Measurement Reply           | 100                                 |
| Rx Valid Delay Measurement Reply     | 2780196315                          |
| Rx Invalid Delay Measurement Reply   | 0                                   |
| Rx Unexpct Delay Measurement Reply   | 0                                   |
| Rx Delay Measurement Reply Timeout   | 0                                   |
| Frame Loss Measurement Repeats       | Disabled                            |
| Frame Loss Measurement Delay (min)   | 0                                   |
| Tx Frame Loss Measurement Message    | 0                                   |
| Rx Valid Frame Loss Message          | 0                                   |
| Rx Invalid Frame Loss Message        | 0                                   |
| Tx Frame Loss Measurement Reply      | 0                                   |
| Rx Valid Frame Loss Reply            | 0                                   |
| Rx Invalid Frame Loss Reply          | 0                                   |
| Rx Frame Loss Measure Reply Timeout  | 0                                   |
| Tx Synthetic Loss Measurement Msg    | 3080786091                          |
| Rx Valid Synthetic Loss Message      | 0                                   |
| Rx Invalid Synthetic Loss Message    | 0                                   |
| Tx Synthetic Loss Message Reply      | 0                                   |
| Rx Valid SLM Reply                   | 3078626026                          |
| Rx Invalid SLM Message Reply         | 0                                   |
| Rx SLM Message Reply Timeout         | 0                                   |
| Tx Total Client Signal Fail          | 982                                 |
| Tx Client Signal Fail - Los          | 982                                 |
| Tx Client Signal Fail - Dci          | 0                                   |
| Rx Valid Client Signal Fail          | 0                                   |
| Rx Invalid Client Signal Fail        | 0                                   |
| Rx Client Signal Fail - Los          | 0                                   |
| Rx Client Signal Fail - Dci          | 0                                   |
+------------------------- Last Loopback Message ----------------------------------+
```


Copyright© 2022 Ciena® Corporation

```
| Target Remote MEPID                  | 0                                          |
| Target Mac Address                   | 00:00:00:00:00:00                          |
| Priority:                            | 7                                          |
| Count:                               | 0                                          |
| First Sequence Number                | 0                                          |
| LBMs Sent                            | 1                                          |
| LBMs To Send                         | 0                                          |
| Rx In-order Loopback Reply           | 0                                          |
| Rx Out-of-order Loopback Reply       | 0                                          |
| Rx Content Mismatch                  | 0                                          |
+-------------------- Last Delay Measurement Message -------------------------------+
| Target Remote MEPID                  | 0                                          |
| Target Mac Address                   | 00:00:00:00:00:00                          |
| Test ID                              | 0                                          |
| Iteration                            | 0                                          |
| Priority                             | 0                                          |
| DMM Interval                         | 0                                          |
| Repeat Delay                         | 0                                          |
| Iteration Count                      | 0                                          |
| Timeout                              | 0                                          |
| CFM Frame Size                       | 0                                          |
| Frame Count Tx                       | 0                                          |
| Frame Count Rx                       | 0                                          |
| Min Delay in us                      | 0                                          |
| Ave Delay in us                      | 0                                          |
| Max Delay in us                      | 0                                          |
| Min Jitter in us                     | 0                                          |
| Ave Jitter in us                     | 0                                          |
| Max Jitter in us                     | 0                                          |
| Total Jitter in us                   | 0                                          |
| Forward Min Jitter in us             | 0                                          |
| Forward Ave Jitter in us             | 0                                          |
| Forward Max Jitter in us             | 0                                          |
| Forward Total Jitter in us           | 0                                          |
| Backward Min Jitter in us            | 0                                          |
| Backward Ave Jitter in us            | 0                                          |
| Backward Max Jitter in us            | 0                                          |
| Backward Total Jitter in us          | 0                                          |
+------------------- Last Frame Loss Measurement Message ----------------------------+
| Target Remote MEPID                  | 0                                          |
| Target Mac Address                   | 00:00:00:00:00:00                          |
| Test ID                              | 0                                          |
| Iteration                            | 0                                          |
| Priority                             | 0                                          |
| LMM Interval                         | 0                                          |
| Repeat Delay                         | 0                                          |
| Iteration Count                      | 0                                          |
| Timeout                              | 0                                          |
| Frame Count Tx                       | 0                                          |
| Frame Count Rx                       | 0                                          |
| Frame Loss Near                      | 0                                          |
| Frame Loss Far                       | 0                                          |
| Bad Sequence Number                  | 0                                          |
| Missing Sequence Number              | 0                                          |
| Frame Loss Near Fault Threshold      | 0                                          |
| Frame Loss Far Fault Threshold       | 0                                          |
| Frame Loss Bad Seq Fault Threshold   | 0                                          |
+----------------- Last Synthetic Loss Measurement Message --------------------------+
| Target Remote MEPID                  | 0                                          |
| Target Mac Address                   | 00:00:00:00:00:00                          |
| Test ID                              | 0                                          |
| Iteration                            | 0                                          |
| Frame Count Tx                       | 0                                          |
| Frame Count Rx                       | 0                                          |
| Priority                             | 0                                          |
| SLM Interval                         | 0                                          |
| Repeat Delay                         | 0                                          |
| Iteration Count                      | 0                                          |
| Timeout                              | 0                                          |
| CFM Frame Size                       | 0                                          |
| Frame Delivery Ratio                 | 0.00%                                      |
| Frame Loss Near                      | 0                                          |
| Frame Loss Far                       | 0                                          |
+------------------------- Last Linktrace Message ----------------------------------+
| Target Remote MEPID                  | 0                                          |
| Target Mac Address                   | 00:00:00:00:00:00                          |
| Priority                             | 7                                          |
| Sequence Number                      | 0                                          |
| Initial TTL                          | 0                                          |
| Use FDB Only                         | No                                         |
+------------------------------------------------- Linktrace Responses ------------------------------------------------------+
|   |Ttl|          |  Remote MP      | Relay |Flags|                                |                                    |
|Ttl|Idx|Trans Id  | Mac Address     |Action |FY|TM| Ingress TLV                     | Egress TLV                         |
+---+---+----------+-----------------+-------+--+--+--------------------------------+------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-16
Creating a remote MEP

A manually created MEP must be assigned a MEPID that is not equal to the MEPID of any local or remote MEP already associated with the service. Manually created Remote MEPs are administratively disabled by default, and will persist in the system. The MAC address associated with a Remote MEP can be configured to a fixed value, and the MAC address is uninitialized until it is either explicitly configured or a CCM containing the MEPID associated with that Remote MEP is processed.

You can:

- create a remote MEP
- set remote MEP attributes

Step	Action

To create a remote MEP

1 Create a remote MEP:

```
cfm remote-mep create [service <service> mepid <NUMBER:1-8191>]
```

where

service <service> is the CFM service name.

mepid <NUMBER: 1-8191> is the MEP identifier.

To set remote MEP attributes

2 Set remote MEP attributes:

```
cfm remote-mep set [service <service> mepid <NUMBER:1-8191>][hold-state <enabled|disabled|lock>] [mac <MacAddress>]
```

where

service <service> is the CFM service name.

Copyright© 2022 Ciena® Corporation

where

mepid <NUMBER: 1-8191>	is the MEP identifier.
hold-state <enabled| disabled|lock>	holds after enabled until stable.
mac <MacAddress>	is the mac address.

—end—

Example

The following example creates a remote MEP with a service name of VLAN#1001, a mepid of 100, and a hold-state of lock.

```
cfm remote-mep create service VLAN#1001 mepid 100 hold-state
lock
```

The following example sets the service name to CFM-1 and the hold-state to disabled.

```
cfm remote-mep set service CFM-1 hold-state disabled
```


Copyright© 2022 Ciena® Corporation

Procedure 2-17
Deleting a remote MEP

Delete a remote MEP.

Step	Action
1	Delete a remote MEP: `cfm remote-mep delete [service <service> mepid <NUMBER:1-8191>]` where service <service> is the CFM service name. mepid <NUMBER:1-8191> is the remote MEP identifier.

—end—

Example:

The following example deletes a remote MEP named CFM-1 that has a mepid of 100.

```
cfm remote-mep delete service CFM-1 mepid 100
```


Copyright© 2022 Ciena® Corporation

Procedure 2-18
Enabling and disabling remote MEPs and MEP discovery

You can:

- enable a remote MEP
- disable a remote MEP
- disable remote MEP discovery
- enable remote MEP discovery

When a new remote MEP is discovered, it is added to MEP CCM Database in a hold state. If valid CCMs are continuously received from the remote MEP for the time specified in the rmep-hold-time and the MEP is administratively enabled, the remote MEP automatically transitions to the enabled operational state. If the MEP has been administratively disabled, it will remain in the hold state indefinitely. You can enable remote MEPs that have not been discovered by CFM.

When you disable a remote MEP, it cannot trigger a service fault. You can disable remote MEPs that have not been discovered by CFM.

Step	Action

To enable a remote MEP

1 Enable a remote MEP:

```
cfm remote-mep enable service <service> mepid <NUMBER:1-8191>
```

where

service <service>	is the CFM service name.
mepid <NUMBER:1-8191>	is the remote MEP identifier.

Copyright© 2022 Ciena® Corporation

To disable a remote MEP

2 Disable a remote MEP:

```
cfm remote-mep enable service <service> mepid <NUMBER:1-8191>
```

where

service <service>	is the CFM service name.
mepid <NUMBER:1-8191>	is the remote MEP identifier.

—end—

Example

The following example enables a remote MEP for a service named VS-CFM that has a mepid of 2.

```
cfm remote-mep enable service VS-CFM-1 mepid 2
```

The following example disables a remote MEP for a service named VS-CFM that has a mepid of 2.

```
cfm remote-mep disable service VS-CFM-1 mepid 2
```


Copyright© 2022 Ciena® Corporation

Procedure 2-19
Displaying remote MEPs

Display remote MEPs to verify CCM reception and display faults.

You can display:

- remote MEPs
- information about remote MEPs

Table 2-28 lists the fields displayed in the CFM Remote MEPs summary table.

Table 2-28
Fields in the CFM Remote MEPs summary table

Field	Description
Service	Identifies the CFM service.
Mepid	Identifies the remote MEP.
Mac Address	Identifies the MAC address of the MAC Relay Entity.
State	Indicates whether the MEP is enabled. • Ad: Indicates whether the MEP is administratively enabled. • Op: Indicates whether the MEP is operationally enabled.
Total Rx CCM	Specifies the total number of CCM messages received.
Seq Error	Specifies the number of CCM sequence errors. A sequence error occurs when the sequence number of a CCM is not one greater than the sequence number of the last CCM received from the Remote MEP, and indicates that a CCM is lost or received out of order. ***Note:*** If the CFM service is accelerated, the value for this field is 0.

Copyright© 2022 Ciena® Corporation

Table 2-28
Fields in the CFM Remote MEPs summary table

Field	Description
Last Seq Num	Provides the last sequence number. ***Note:*** If the CFM service is accelerated, the value for this field is 0. MIPs and non-accelerated remote MEPs on peer devices show a value of 0 in the Last Seq Num field.
Fault	Remote MEP fault indicators. All defects currently in effect for a Remote MEP are designated with an "X": • F: Remote MEP Fault. A CCM has not been received from the Remote MEP within ccm-interval*3.5. • M: Mac Status. The combined values of Port Status and Mac Status constitute a Mac Status fault. • P: Port Status. The last CCM received from the Remote MEP indicated a Port Status fault. • I: Interface Status. Last CCM received indicates an Interface Status fault. • R: RDI. The last CCM received from the Remote MEP indicated an RDI fault.
Accelerated	Indicates whether the CFM service is accelerated.

In a healthy service, Remote MEPs will typically not have any fault indicators. A non-zero value for "Seq Error" indicates that one or more CCMs from the Remote MEP were lost in transit. CCMs that are delayed for a period of time greater than ccm-interval*3.5 are not reflected in the "Seq Error" field, although such a condition may trigger and RMEP Fault (F).

Step	Action

To display remote MEPs

1 Display remote MEPs:

```
cfm remote-mep show agent y1731
```

where

agent	retrieve from agent.
y1731	displays a summary of Y.1731 delay and frame-loss test results for all remote MEPs.

Copyright© 2022 Ciena® Corporation

To display information about remote MEPs

2 Display information about remote MEPs:

```
cfm remote-mep show [service <service>] [mepid <mepid>]
agent
```

where

service <service>	is the CFM service name.
mepid <mepid>	is the remote MEP identifier.
agent	retrieve from agent.

—end—

Example

The following example shows sample output for the cfm remote-mep show command where the MAC status defect is reported due to a port status fault.

```
cfm remote-mep show

+------------------------------------ CFM REMOTE MEPS ---------------------------------------+
|              |      |                  |State|Total     |Seq  |Last      |  Fault   |Accelerated|
|Service       |Mepid|Mac Address       |Ad|Op|Rx CCM    |Error|Seq Num   |F|M|P|I|R|           |
+--------------+-----+-----------------+--+--+---------+-----+---------+-+-+-+-+-+-----------+
|VLAN#100      |10   |02:03:18:58:27:61|en|en|1034978  |1    |1109556  | |X|X| | |No         |
+--------------+-----+-----------------+--+--+---------+-----+---------+-+-+-+-+-+-----------+
```

The following example shows sample output for the cfm remote-mep show command where the MAC status defect is reported due to an interface status fault.

```
cfm remote-mep show

+---------------------------------- CFM REMOTE MEPS ---------------------------------------+
|             |      |                  |State|Total     |Seq  |Last      |  Fault   |Accelerated|
|Service      |Mepid|Mac Address       |Ad|Op|Rx CCM    |Error|Seq Num   |F|M|P|I|R|           |
+------------+-----+-----------------+--+--+---------+-----+---------+-+-+-+-+-+-----------+
|VLAN#100    |10   |02:03:18:58:27:61|en|en|1034978  |1    |1109556  | |X| |X| |No         |
+------------+-----+-----------------+--+--+---------+-----+---------+-+-+-+-+-+-----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-20
Creating MIPs

Create a MIP when you have intermediate devices in a VLAN service. Intermediate devices are the devices between the devices containing service MEPs. Similar to MEPs, MIPs can be created on individual C-VIDs of a VS subscriber port. Also, you can create multiple MIPs for the same VLAN and port at different MD levels.

Step	Action
1	Create a MIP: `cfm mip create {vlan <VlanList>} {port <PortName>} [level <NUMBER: 0-7>]` where vlan <VlanList> is the VLAN. port <PortName> is the port. level <NUMBER: 0-7> is the maintenance domain level.

—end—

Example

The following example creates MIPs for the VLAN 1001 and port 1 at level 3 and level 5.

```
cfm mip create vlan 1001 port 1 level 3
cfm mip create vlan 1001 port 1 level 5
```


Copyright© 2022 Ciena® Corporation

Procedure 2-21
Deleting MIPs

Delete MIPs when they are no longer required.

Step	Action
1	Delete a MIP: `cfm mip delete {vlan <VlanList>} {port <PortName>} [level <NUMBER: 0-7>]` where vlan <VlanList> is the VLAN. port <PortName> is the port. level <NUMBER: 0-7> is the maintenance domain level. If no level is specified, then MIPs at all levels on the VLAN/port are deleted.

—end—

Example

The following example deletes MIPs from level 5 of port 1 on VLAN 1001.

```
cfm mip delete vlan 1001 port 1 level 5
```


Copyright© 2022 Ciena® Corporation

Procedure 2-22
Enabling and disabling the MIP database

You can:

- enable the MIP database
- disable the MIP database

Step	Action

To enable the MIP database

1 Enable the MIP database:

```
cfm mip-ccm-db enable
```

To disable the MIP database:

2 Disable the MIP database:

```
cfm mip-ccm-db disable
```

—end—

Example

The following example disables the MIP database.

```
cfm mip-ccm-db disable
```


Copyright© 2022 Ciena® Corporation

Procedure 2-23
Displaying MIP configuration and MIP database

You can display:

- MIP configuration
- MIP database

Step	Action

To display MIP configuration

1 Display MIP configuration:

```
cfm mip show [vlan <VlanList> port <PortName>]
```

where

vlan <VlanList> is the VLAN.

port <PortName> is the port.

To display the MIP database

2 Display the MIP database:

```
cfm mip-ccm-db show
```

—end—

Example

The following example shows sample output for the cfm mip show command.

```
cfm mip show

+------------------------ CFM MIPs ----------------------------+
| Service Instance |Vlan Id |Port    |Level |Mac Address       |
|------------------+--------+--------+------+------------------|
|VLAN#1001         |1001    |1       |3     |00:02:A1:24:0E:32 |
|------------------+--------+--------+------+------------------|
```

The following example shows sample output for the cfm mip-ccm-db show command.

```
cfm mip-ccm-db show

+--------------------------- MIP CCM Database ---------------------------+
|    |                    |     |Total    |      Last CCM Information      |
|VLAN|   MAC Address      |Port |CCM Rx   |Seq Num   |Time   |Lv|Mepid| PS |RDI|
+----+--------------------+-----+---------+----------+-------+--+-----+----+---|
|777 |00:02:A1:30:A1:78|9    |101      |2784      |0      |3 |200  |Up  | X |
+----+--------------------+-----+---------+----------+-------+--+-----+----+---|
```


Copyright© 2022 Ciena® Corporation

Procedure 2-24
Sending and displaying loopback messages

Send and display loopback messages for troubleshooting purposes. You can:

- send a loopback message to a MEP
- send a loopback message to a MAC address
- display loopback replies

Loopback is a unicast CFM frame sent from a MEP to specific MEPs or MIPs. Multiple loopback messages (LBMs) may be sent to the same destination and loopback catalogs the responses by how many were received in order and how many were out of order.

Table 2-29 lists the fields in the loopback reply (LBR).

Table 2-29
Fields in the loopback reply

Field	Description
Tx	Number of LBMs transmitted
ToTx	Number of LBMs for transmission remaining
Io	Number of In Order LBRs received
Ooo	Number of Out of Order LBRs received
Con	Number of LBRs received having a Content Mismatch with the corresponding LBM.
Loss	The loss count is the difference of the number of LBMs transmitted from the sum of the In Order LBRs and Out of Order LBRs received (Tx - (Io + Ooo)).

Normally, the Tx LBM value is equal to the LBR in Order value to indicate that an LBR was received for each LBM, and that all LBRs were received in the expected order. If LBR Out of Order is greater than 0, then some LBRs were

Copyright© 2022 Ciena® Corporation

not received in the same order as their associated LBMs were transmitted. If Tx LBM is greater than the LBR In Order value plus the LBR Out of Order value, then an LBR was not received for every LBM transmitted.

Step	Action

To send a loopback message to a MEP

1 Send a loopback message to a MEP:

```
cfm loopback send service <service> {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mepid <NUMBER: 1-8191>} [count <NUMBER: 1-255>] [priority <NUMBER: 0-7>] [data <String [128]>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier to send to.
count <NUMBER: 1-255>	is the number of Loopback messages to send.
priority <NUMBER: 0-7>	is the priority value used in the VLAN tag of the transmitted frame
data <String [128]>	is the loopback data to be included in each.

To send a loopback message to a MAC address

2 Send a loopback message to a MAC address:

```
cfm loopback send-mac service <String[16]> {local-mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mac <MacAddress>} [count <NUMBER: 1-255>] [priority <NUMBER: 0-7>] [data <String [128]>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.

Copyright© 2022 Ciena® Corporation

where

vlan <Vlan>	is the VLAN.
mac <MacAddress>	is the mac address.
count <NUMBER: 1-255>	is the number of Loopback messages to send.
priority <NUMBER: 0-7>	is the priority value used in the VLAN tag of the transmitted frame
data <String [128]>	is the loopback data to be included in each.

To display loopback replies

3 Display loopback replies:

```
cfm loopback show [service <service>] [order-by-mepid]
[exclude-evpl]
```

where

service <service>	is the CFM service name.
order-by-mepid	orders results by mepid.
exclude-evpl	excludes EVPL interfaces.

—end—

Example

The following example sends a loopback message to a MEP specified by MEP ID.

```
cfm loopback send service vl10015 local-mepid 59 mepid 1 count
100
```

The following example sends multiple messages to obtain an order count.

```
cfm loopback send service cfmvlan port 1 mepid 100 count 10
```

The following example sends messages to a specific MAC address.

```
cfm loopback send-mac service cfmvlan port 1 mac
00:02:A1:15:56:E0
```


Copyright© 2022 Ciena® Corporation

Procedure 2-25
Sending and displaying linktrace messages

Send and display linktrace messages for troubleshooting purposes. You can:

- send a linktrace to another MEP
- send a linktrace to a MAC address
- display linktrace replies

Linktrace is a multicast CFM frame originated from a MEP. When received by a MIP, the MIP checks its forwarding table and responds that the message was received on port X and forwarded out of port Y. In the case of a MEP to MEP message, all intermediate MIPs on the path will respond on a per box basis. All linktrace responses (LTRs) are unicast back to the originator.

> ***Note:*** Linktrace messages (LTMs) may also be sent to any arbitrary MAC address, not necessarily a MEP/MIP. This feature can be used to trace paths, even those outside of a given Maintenance Association.

Copyright© 2022 Ciena® Corporation

Table 2-30 lists the fields in the linktrace replies.

Table 2-30
Fields in linktrace replies

Field	Description
Ttl - Time to Live	An LTR is received from each CFM aware node that handles and propagates the LTM. Each node decrements the LTM Ttl by one and encodes the resulting value in the LTR. Normally, the Ttl values in the LTR list start at the initial LTM Ttl - 1, and decrease by one for each row in the table. Non-sequential Ttl values indicate that not all LTRs send by intermediate nodes were received, or that the LTM Ttl was incorrectly decremented at some point.
Ttl Idx - Time to Live Index	A locally assigned value used to differentiate multiple LTRs received with the same Ttl value. Normally, one LTR is received for each Ttl, and its Ttl index is 1. Multiple LTR entries for the same Ttl indicate an error condition, as it is the result of the LTM being handled on multiple forwarding paths through the network to the target DA.
Relay Action	Indicates how the LTM was handled by the MEP or MIP as follows: • Hit - The LTM reached the target MEP or MIP. • FDB - The egress port for forwarding to the LTM target MAC was resolved using the MAC learn table. • MFDB - The egress port for forwarding to the LTM target MAC was resolved using the MEP or MIP CCM Database. • undef - Undefined. This value should never be present in an LTR Relay Action.
Ingress Port	Name of the port on which the LTM was received. The name is either a port number or aggregation name.
Ingress Action	Reports how a data frame to the LTM target MAC would be handled at the ingress port as follows: • Ok - The frame would be accepted for forwarding • Down - The ingress port is not operational. • Blocked - The ingress port is blocked by topology enforcement. • VID - The ingress port is not a member of the LTM's VID, and ingress filtering is enabled. • undef - Undefined. Receiving an LTR that has no reply ingress TLV results in the undefined value for the Ingress Action.

Copyright© 2022 Ciena® Corporation

Table 2-30
Fields in linktrace replies

Field	Description
Egress Port	Name of the port that is the target of the LTM, or the port that a data frame to the LTM target MAC would be transmitted out when forwarded. The name is either a port number or aggregation name.
Egress Action	Reports how a frame to the LTM target MAC would be handled as it passes through the egress port as follows: • Ok - The frame would be forwarded. • Down - The frame would be discarded because the egress port is not operational. • Blocked - The frame would be discarded because the egress port is blocked by topology enforcement. • VID - The frame would be discarded because the egress port is not a member of the LTM VID and egress filtering is enabled. • undef - Undefined. This indicates that the frame would not reach the egress port.
Flags	Reports two flags in the linktrace responses: • FY - FwdYes. • TM - TerminalMEP.

A normal linktrace result is to receive one LTR for each intermediate MIP (if any) along the forwarding path to the target MAC, and a LTR from the target MEP or MIP, or the Remote MEP that handles an LTM targeted at an arbitrary destination address.

Failure to receive any LTRs indicates one or more of the following conditions:

- The LTM was not handled by any MEP or MIP that could resolve how to forward to the target MAC.
- The LTM did not traverse any MEPs or MIPs as it was multicast through the network.
- All LTRs were lost in transit.
- The LTR Ttl values should be consecutive. A Ttl value that is more than one less than Ttl value of the LTR immediately above it in the output typically indicates that one or more LTRs were lost in transit.

Copyright© 2022 Ciena® Corporation

Step	Action

To send a linktrace to another MEP

1 Send a linktrace to another MEP:

```
cfm linktrace send service <service> {local-mepid
<NUMBER:1-8191> | port <PortName> [vlan <Vlan>]} {mepid
<NUMBER: 1-8191>} [ttl <NUMBER: 1-255>] [priority
<NUMBER: 0-7>] [fdb-only]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER:1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier to send to.
ttl <NUMBER: 1-255>	is the initial value for the Time To Live (TTL) field, which limits the number of hops that the Linktrace Request message can propagate through the network.
priority <NUMBER: 0-7>	is the priority value used in the VLAN tag of the transmitted frame.
fdb-only	is a flag indicating that only the normal forwarding database should be used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise

To send a linktrace to a MAC address

2 Send a linktrace to a MAC address:

```
cfm linktrace send-mac service <service> {local-mepid
<NUMBER:1-8191> | port <PortName> [vlan <Vlan>]} {mac
<MacAddress>} [ttl <NUMBER: 1-255>] [priority <NUMBER: 0-
7>] [fdb-only]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER:1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

Copyright© 2022 Ciena® Corporation

where

mac <MacAddress>	is the mac address.
ttl <NUMBER: 1-255>	is the initial value for the Time To Live (TTL) field, which limits the number of hops that the Linktrace Request message can propagate through the network.
priority <NUMBER: 0-7>	is the priority value used in the VLAN tag of the transmitted frame.
fdb-only	is a flag indicating that only the normal forwarding database should be used to look up the target MAC, and not the MEP CCM and MIP CCM databases that would also be used otherwise

To display linktrace replies

3 Display linktrace replies:

```
cfm linktrace show [service <service>] [order-by-mepid]
[exclude-evpl]
```

where

service <service>	is the CFM service name.
order-by-mepid	orders results by mepid.
exclude-evpl	excludes EVPL interfaces.

—end—

Example

The following example sends a linktrace to a Remote MEP with one LTR received.

```
cfm linktrace send service vl100 port 5 mepid 600
```

The following example sends a linktrace to a MAC address with no LTRs received.

```
cfm linktrace send-mac service vl100 port 5 mac
00:11:22:33:44:55
```


Copyright© 2022 Ciena® Corporation

Procedure 2-26
Configuring Y.1731 DMMs

Send and display Y.1731 DMMs for troubleshooting purposes. You can:

- send DMMs to a remote MEP
- send DMMs to a MAC address
- cancel remote MEP DMM transmission
- cancel MAC address DMMs transmission
- clear delay measurement statistics for all or a specific service local MEP ID
- clear delay measurement statistics for a specific MEP in a service
- delete a DMM session from the local MEP

DM frames with an MD Level lower than that of the receiving MEP are discarded. DM frames with an MD Level equal to and a DA not equal to that of the receiving MEP are discarded.

Step	Action

To send DMMs to a remote MEP

1 Send DMMs to a remote MEP:

```
cfm delay send {service <service>} {local-mepid <NUMBER:
1-8191> | port <PortName> [vlan <Vlan>]} {mepid <NUMBER:
1-8191> | mac <remote-mac-address>} [test-id <INTEGER:
0..4294967295>] [count <NUMBER: 2-65535> | duration
<SECONDS: 1.. 65535 >] [dmm-interval <dmm-interval-enum>]
[priority <NUMBER: 0-7>] [iterate <NUMBER: 0..60> |
repeat-delay <MINUTES:0-1440>] [timeout <MILLISECONDS:
2000..10000>] [frame-size <NUMBER:140..1400 >] [delay-
threshold <MICROSECONDS: 0..2147483647>] [jitter-
threshold <MICROSECONDS: 0..2147483647>] [max-delay-
threshold <MICROSECONDS: 0..2147483647>] [max-jitter-
threshold <MICROSECONDS: 0..2147483647>] [accelerate |
non-accelerate] [delay-bins <CFM Delay Profile Name>]
```


Copyright© 2022 Ciena® Corporation

```
[jitter-bins <CFM Jitter Profile Name>] [forward-jitter-
bins <CFM Jitter Profile Name>] <backward-jitter-bins
<CFM Jitter Profile Name>] [cos-mode]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the local MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
mac <remote-mac-address>	is the unicast MAC address of the remote MEP.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)
count <NUMBER: 2-65535>	is the number of DMM frames to transmit per delay measurement test (count). Valid range is 2 - 65535 and the default value is 2. (Optional)
duration <SECONDS: 1..65535 >	is the amount of time in seconds that the test iteration runs. This attribute is mutually exclusive with count.
[dmm-interval <dmm-interval-enum>]	is the DMM interval, specified as an index or time. The permitted values are 1 (3.33ms), 2 (10ms), 3 (100ms), 4 (1sec), 5 (10sec), 6 (1min) and 7 (10min). If the DMM interval is not specified, then the service level setting for the DMM interval is used.
priority <NUMBER: 0-7>	is the priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). The default value is 7. (Optional)
iterate <NUMBER: 0..60>	is the number of discrete tests invoked within a test session. Iterate=0 means continuous test. The default value is 1.
repeat-delay <MINUTES:0-1440>	is the amount of time to wait in minutes between each test iteration.
timeout <MILLISECONDS: 2000..10,000>	is the DMM timeout. The default value is 5000 ms.
frame-size <NUMBER:140..1400 >	is the base CFM frame size.

Copyright© 2022 Ciena® Corporation

where	
delay-threshold <MICROSECONDS: 0..2147483647>	is the delay error threshold in microseconds. (Optional)
jitter-threshold <MICROSECONDS: 0..2147483647>	is the jitter error threshold in microseconds. (Optional)
max-delay-threshold <MICROSECONDS: 0..2147483647>	is the maximum delay threshold in microseconds. (Optional)
max-jitter-threshold <MICROSECONDS: 0..2147483647>	is the maximum jitter threshold in microseconds. (Optional)
accelerate | non-accelerate	For the sessions configured with *accelerate*, the Delay session is offloaded to FPGA. Both Tx/Rx and timestamping is done by FPGA. For the session configured with *non-accelerate*, SW does Tx/Rx of the DMM/DMR frames and are timestamped by HW (BCM). ***Note:*** On the 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved to use the accelerate option.
delay-bins <CFM Delay Profile Name>	is the delay profile name.
jitter-bins <CFM Jitter Profile Name>	is the jitter profile name.
forward-jitter-bins <CFM Jitter Profile Name>	is the forward jitter profile name.
backward-jitter-bins <CFM Jitter Profile Name>	is the backward jitter profile name.
cos-mode	indicates that DMR p-bits are to be substituted for test-id when TestId TLV is missing.

Copyright© 2022 Ciena® Corporation

To send DMMs to a MAC address

2 Send DMMs to a MAC address:

```
cfm delay send-mac {service <service>} {local-mepid
<NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mac
<MacAddress>} [count <NUMBER: 2-600>] [priority <NUMBER:
0-7>] [repeat <NUMBER: 1-1440>] [delay-threshold
<NUMBER>] [jitter-threshold <NUMBER>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mac <MacAddress>	is the mac address.
count <NUMBER: 2-600>	is the number of DMM frames to transmit per delay measurement test (count). Valid range is 2 - 600 and the default value is 2. (Optional)
priority <NUMBER: 0-7>	is the priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). Default is 7. (Optional)
repeat <NUMBER: 1-1440>	indicates whether the test should be repeated. Valid range 0 - 1440 minutes. By default a test will not be auto-repeated. A value of 0 indicates that the test should run continuously. (Optional)
delay-threshold <NUMBER>	in microseconds to generate an event and trap when test results continuously exceed the value. (Optional)
jitter-threshold <NUMBER>	in microseconds to generate an event and trap when test results continuously exceed the value. (Optional)

To cancel remote MEP DMM transmission

3 Cancel remote MEP DMM transmission:

```
cfm delay cancel {service <service>} {local-mepid
<NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mepid
<NUMBER: 1-8191> | mac <remote-mac-address>} [test-id
<INTEGER: 0..4294967295>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.

Copyright© 2022 Ciena® Corporation

where

vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
mac <remote-mac-address>	is the unicast MAC address of the remote MEP.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)

To cancel MAC address DMMs transmission

4 Cancel MAC address DMMs transmission:

```
cfm delay cancel-mac {service <service>} {local-mepid
<NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mac
<MacAddress>}
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mac <MacAddress>	is the mac address.

To clear delay measurement statistics

5 Clear delay measurement statistics:

```
cfm delay clear [statistics]
```

where

statistics	clears statistics.

To clear delay measurement statistics for a service

6 Clear delay measurement statistics for a service:

```
cfm delay clear service <service> {port <Port>} {vlan
<Vlan>} {local-mepid <NUMBER: 1-8191>} {statistics}
{history}
```

where

service <service>	is the CFM service name.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

Copyright© 2022 Ciena® Corporation

where

local-mepid <NUMBER: 1-8191>	is the local MEP identifier.
statistics	clears statistics.
history	clears history.

To delete a DMM session from the local MEP

7 Delete a DMM session from the local MEP:

```
cfm delay delete service <service> {local-mepid <NUMBER:
1-8191> | port <PortName> [vlan <Vlan>]} {mepid < <NUMBER:
1..8191>} [test-id <INTEGER: 0..4294967295>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)

—end—

Example

The following example sends DMMs to a remote MEP.

```
cfm delay send service CFM_VLAN_10 local-mepid 2 remote-mepid 1
```

The following example sends DMMs to a MAC address.

```
cfm delay send-mac service CFM_VLAN_10 local-mepid 2 mac
01:02:03:04:05:06
```

The following example configures the delay, jitter, forward jitter and backward jitter attributes.

```
cfm delay send service cfm-3200 local-mepid 2 mepid 12 test-id
1 non-accelerate count 50 delay-bins delay-long jitter-bins
jitter-long forward-jitter-bins jitter-long backward-jitter-
bins jitter-long
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the cfm delay show command.

```
> cfm delay show
```

MEP DELAY MEASUREMENT MESSAGE INFORMATION

Service	Local Mepid	Remote Mac Address	Remote Mepid	TestId	Iteration	DMM	DMR	Delay in us		Jitter in us		Rep Time	Acc
cfm-3000-1Q	1	00:02:5A:01:C0:92	2	1	10	54	54	Two-way		Two-way		0	No
								Min:	219	Min:	1		
								Avg:	252	Avg:	16		Stamp: Sw
								Max:	354	Max:	113		
										Tot:	855		
								Forward		Forward			
								Min:	81	Min:	0		
								Avg:	111	Avg:	7		
								Max:	130	Max:	21		
										Tot:	375		
								Backward		Backward			
								Min:	113	Min:	0		
								Avg:	141	Avg:	15		
								Max:	243	Max:	115		
										Tot:	800		

The following example cancels remote MEP DMM transmission.

```
cfm delay cancel service CFM_VLAN_10 local-mepid 2 mepid 1
```

The following example cancels MAC address DMMs transmission.

```
cfm delay cancel-mac service CFM_VLAN_10 local-mepid 1 mac
01:02:03:04:05:06
```

The following example clears delay measurement statistics for all or a specific service local MEP ID.

```
cfm delay clear
```


Copyright© 2022 Ciena® Corporation

Procedure 2-27
Configuring DMM responders

You can:

- create a DMM responder
- delete a DMM responder
- display a DMM responder
- clear statistics for a DMM responder

Note: DMM responder is supported on the 3924, 3926, 3928 and 5160.

Step	Action

To create a DMM responder

1 Create a DMM responder in hardware from the local MEP to a remote MEP:

```
cfm delay-responder create service <service> {port<port-
list> [vlan [<VLAN>] {local-mepid <NUMBER: 1..8191>}
[mepid <NUMBER: 1..8191] {accelerate | non-accelerate
[test-id <NUMBER: 0..4294967295>]}
```

where

service <service>	is the CFM service.
port<port-list>	is the port.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid <NUMBER: 1..8191>	is the remote MEP identifier.
accelerate | non-accelerate [test-id <	accelerate is the hardware assisted dmm-responder session. non-accelerate is the software time-stamped dmm-responder session ***Note:*** On the 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved to use the accelerate option.
test-id <NUMBER: 0..4294967295>	is the Test ID.

Copyright© 2022 Ciena® Corporation

To delete a DMM responder

2 Delete a DMM responder:

```
cfm delay-responder delete service <service> {port <port-
list> [vlan [<VLAN>] {local-mepid< <NUMBER: 1..8191>}
[mepid < <NUMBER: 1..8191][test-id <NUMBER:
0..4294967295>]
```

where

service <service>	is the CFM service.
port<port-list>	is the port.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid <NUMBER: 1..8191>	is the remote MEP identifier.
test-id <NUMBER: 0..4294967295>	is the Test ID (optional).

To display DMM responders

3 Display configured DMM responders:

```
cfm delay-responder show service <service> {port <port-
list> [vlan [<VLAN>]{local-mepid <NUMBER: 1..8191>}
```

where

service <service>	is the CFM service.
port<port-list>	is the port.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.

To clear statistics associated with a DMM responder

4 Clear statistics associated with a DMM responder:

```
cfm delay-responder clear service <service> {port <port-
list> [vlan <VLAN>] {local-mepid <NUMBER: 1..8191>}
[mepid <NUMBER: 1..8191>] [test-id <NUMBER:
0..4294967295>]
```

where

service <service>	is the CFM service.
port<port-list>	is the port.
vlan<VLAN>	is the VLAN.

Copyright© 2022 Ciena® Corporation

where

local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid <NUMBER: 1..8191>	is the remote MEP identifier.
test-id <NUMBER: 0..4294967295>	is the Test ID (optional).

—end—

Example

The following example shows the output for the cfm delay-responder show command.

```
> cfm delay-responder show
```

CFM DELAY RESPONDERS

Service	Local Mepid	Local Mac Address	Remote Mepid	Remote Mac Address	TestId	Acc	Total DMM Received	Total DMR Transmitted	Timestamp
cfm-200	40	00:03:18:D4:F4:F2	30	00:03:18:D0:2B:32	0	Yes	0	0	Hardware
cfm-500	60	00:03:18:D4:F4:F2	50	00:03:18:D0:2B:32	1	No	0	0	Software
cfm-500	60	00:03:18:D4:F4:F2	50	00:03:18:D0:2B:32	2	No	300	300	Software

Copyright© 2022 Ciena® Corporation

Procedure 2-28
Displaying statistics

You can display:

- DMM statistics
- DMM statistics for a service
- LMM statistics
- SLM statistics for a service

Step	Action

To display DMM statistics

1 Display DMM statistics:

```
cfm delay show [order-by-mepid] [exclude-evpl] [bins]
```

where

order-by-mepid	indicates that results are ordered by MEP identifier.
exclude-evpl	indicates that EVPL interfaces are excluded.
bins	indicates that results are broken down into bins.

To display DMM statistics for a service

2 Display DMM statistics for a service:

```
cfm delay show service <service> [order-by-
mepid][exclude-evpl] [bins] {local-mepid <NUMBER:1-
8191>}[mepid <NUMBER: 1-8191>} [test-id <INTEGER:
0..4294967295>] {history}
```

where

service <service>	is the CFM service name.
order-by-mepid	indicates that results are ordered by MEP identifier.
exclude-evpl	indicates that EVPL interfaces are excluded.
bins	indicates that results are broken down into bins.
local-mepid <NUMBER:1-8191>	is the local MEP identifier.

Copyright© 2022 Ciena® Corporation

where

mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)
history	displays history.

To display LMM statistics

3 Display LMM statistics:

```
cfm frame-loss show [service <service>] <mep-object>
[mepid <remote-mep-id>] [test-id <INTEGER:
0..4294967295>] [history]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER:1-8191>	is the local MEP identifier.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)
history	displays history

To display SLM statistics for a service

4 Display SLM statistics for a service:

```
cfm synthetic-loss show service <service> [order-by-
mepid] [exclude-evpl] {local-mepid <NUMBER:1-
8191>}[mepid <NUMBER: 1-8191>} {test-id <NUMBER: 1-
4294967295>} {history}
```

where

service <service>	is the CFM service name.
order-by-mepid	indicates that results are ordered by MEP identifier.
exclude-evpl	indicates that EVPL interfaces are excluded.
local-mepid <NUMBER:1-8191>	is the local MEP identifier.

Copyright© 2022 Ciena® Corporation

where

mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <NUMBER: 1-4294967295>	is the test identifier.
history	displays history.

—end—

Example

The following example displays DMM statistics for a service.

```
cfm delay show service cfm-3000-1Q local-mepid 1 mepid 2 test-id 1
```

```
+-------------------------- CFM DELAY SESSION INFO ---------------------------------+
| Parameter                          | Value                                       |
+------------------------------------+---------------------------------------------+
| Service Name                       | cfm-3000-1Q                                 |
| Service Index                      | 1                                           |
| Local Mepid                        | 1                                           |
| Remote Mepid                       | 2                                           |
| Test ID                            | 1                                           |
| Priority                           | 7                                           |
| Source MAC Address                 | 00:02:5A:01:C1:12                           |
| Target MAC Address                 | 00:02:5A:01:C0:92                           |
| DMM Interval                       | 10sec                                       |
| Count                              | 100                                         |
| Duration (sec)                     | 990                                         |
| Iteration Count                    | Continuous                                  |
| Repeat Delay (minutes)             | 0                                           |
| Repeat Flag                        | 1                                           |
| Rx Timeout                         | 5000                                        |
| Device TYpe                        | 0                                           |
| Configured Frame Size              | 64                                          |
| Delay Threshold                    | -1                                          |
| Jitter Threshold                   | -1                                          |
| Max Delay Threshold                | -1                                          |
| Max Jitter Threshold               | -1                                          |
| Accelerated                        | No                                          |
| Config Accelerated                 | No                                          |
| Timestamp                          | Software                                    |
| CoS Mode                           | No                                          |
+---------------------------- Last Test Result ---------------------------------------+
| Iteration                          | 11                                          |
| Start                              | 06/22/2017 00:14:17                         |
| End                                | 06/22/2017 00:14:26                         |
| Duration (ms)                      | 8912                                        |
| DMM Tx                             | 1                                           |
| DMR Rx                             | 1                                           |
| Avg Delay                          | 302                                         |
| Min Delay                          | 302                                         |
| Max Delay                          | 302                                         |
| Forward Avg Delay                  | 113                                         |
| Forward Min Delay                  | 113                                         |
| Forward Max Delay                  | 113                                         |
| Backward Avg Delay                 | 189                                         |
| Backward Min Delay                 | 189                                         |
| Backward Max Delay                 | 189                                         |
| Avg Jitter                         | 0                                           |
| Min Jitter                         | 0                                           |
| Max Jitter                         | 0                                           |
| Total Jitter                       | 0                                           |
| Forward Avg Jitter                 | 0                                           |
| Forward Min Jitter                 | 0                                           |
| Forward Max Jitter                 | 0                                           |
| Forward Total Jitter               | 0                                           |
| Backward Avg Jitter                | 0                                           |
| Backward Min Jitter                | 0                                           |
| Backward Max Jitter                | 0                                           |
| Backward Total Jitter              | 0                                           |
| Frame Size                         | 68                                          |
| Status                             | Start                                       |
+------------------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

```
+---------------------------- DELAY MEASUREMENT RESULT BINS ----------------------------+
|      |          Delay Result                |      |          Jitter Result               |
| Bin  | Threshold (us)      | Count          | Bin  | Threshold (us)      | Count          |
+------+---------------------+----------------+------+---------------------+----------------+
| 0    | 0                   | 50             | 0    | 0                   | 49             |
| 1    | 10                  | 0              | 1    | 10                  | 0              |
| 2    | 20                  | 0              | 2    | 20                  | 0              |
| 3    | 30                  | 0              | 3    | 30                  | 0              |
| 4    | 40                  | 0              | 4    | 40                  | 0              |
| 5    | 50                  | 0              | 5    | 50                  | 0              |
| 6    | 60                  | 0              | 6    | 60                  | 0              |
| 7    | 70                  | 0              | 7    | 70                  | 0              |
| 8    | 80                  | 0              | 8    | 80                  | 0              |
| 9    | 90                  | 0              | 9    | 90                  | 0              |
| 10   | 100                 | 0              | 10   | 100                 | 0              |
|      |                     |                +------+---------------------+----------------+
|      |                     |                |              Forward                        |
|      |                     |                +------+---------------------+----------------+
|      |                     |                | 0    | 0                   | 49             |
|      |                     |                | 1    | 10                  | 0              |
|      |                     |                | 2    | 20                  | 0              |
|      |                     |                | 3    | 30                  | 0              |
|      |                     |                | 4    | 40                  | 0              |
|      |                     |                | 5    | 50                  | 0              |
|      |                     |                | 6    | 60                  | 0              |
|      |                     |                | 7    | 70                  | 0              |
|      |                     |                | 8    | 80                  | 0              |
|      |                     |                | 9    | 90                  | 0              |
|      |                     |                | 10   | 100                 | 0              |
|      |                     |                +------+---------------------+----------------+
|      |                     |                |              Backward                       |
|      |                     |                +------+---------------------+----------------+
|      |                     |                | 0    | 0                   | 49             |
|      |                     |                | 1    | 10                  | 0              |
|      |                     |                | 2    | 20                  | 0              |
|      |                     |                | 3    | 30                  | 0              |
|      |                     |                | 4    | 40                  | 0              |
|      |                     |                | 5    | 50                  | 0              |
|      |                     |                | 6    | 60                  | 0              |
|      |                     |                | 7    | 70                  | 0              |
|      |                     |                | 8    | 80                  | 0              |
|      |                     |                | 9    | 90                  | 0              |
|      |                     |                | 10   | 100                 | 0              |
+------+---------------------+----------------+------+---------------------+----------------+
```

The following example displays DMM history for a service.

```
cfm delay show service cfm-3000-1Q local-mepid 1mepid 2 history
```

```
+-------------- MEP DMM INFORMATION --------------+
|                 |Local  |      Local       |Test  |
|Service          |MEP ID |   Mac Address    |Results|
+-----------------+-------+------------------+------+
|cfm-3000-1Q      |1      |00:02:5A:01:C1:12|30    |
+-----------------+-------+------------------+------+
```

```
+------------------------------------------------ MEP DELAY MEASUREMENT HISTORY ------------------------------------+
|                            |                          |         |     |     |                |                |      |
|    Session Parameters      |           Time           |Iteration| DMM | DMR |   Delay in us  | Jitter in us   |Status|
+----------------------------+--------------------------+---------+-----+-----+----------------+----------------+------+
|RMEP ID: 2                  |Start: 06/21/2017 21:28:14|1        |100  |100  |Two-way         |Two-way         |Done  |
|TestId: 1                   |End:   06/21/2017 21:44:56|         |     |     |Min:        222 |Min:          0 |      |
|Priority: 7                 |Duration (ms): 1001712    |         |     |     |Ave:        257 |Avg:         17 |      |
|Interval: 10sec             |                          |         |     |     |Max:        392 |Max:        158 |      |
|RMEP MAC: 00:02:5A:01:C0:92 |                          |         |     |     |                |Tot:       1742 |      |
|Frame Size: 68              |                          |         |     |     |Forward         |Forward         |      |
|Accelerate: No              |                          |         |     |     |Min:         96 |Min:          0 |      |
|Timestamp: Software         |                          |         |     |     |Avg:        124 |Avg:         10 |      |
|                            |                          |         |     |     |Max:        177 |Max:         53 |      |
|                            |                          |         |     |     |                |Tot:       1037 |      |
|                            |                          |         |     |     |Backward        |Backward        |      |
|                            |                          |         |     |     |Min:        101 |Min:          0 |      |
|                            |                          |         |     |     |Avg:        132 |Avg:         14 |      |
|                            |                          |         |     |     |Max:        255 |Max:        149 |      |
|                            |                          |         |     |     |                |Tot:       1387 |      |
+----------------------------+--------------------------+---------+-----+-----+----------------+----------------+------+
|                                                    DELAY MEASUREMENT RESULT BINS                                   |
+----+-----------------------+----+-----------------------+----+-----------------------+----+-----------------------+
|    Delay Result            |    Jitter Result           |    Forward Jitter Result   |    Backward Jitter Result  |
|Bin | Threshold | Count     |Bin | Threshold | Count     |Bin | Threshold | Count     |Bin | Threshold | Count     |
|    |   (us)    |           |    |   (us)    |           |    |   (us)    |           |    |   (us)    |           |
+----+-----------+-----------+----+-----------+-----------+----+-----------+-----------+----+-----------+-----------+
| 0  | 0         | 100       | 0  | 0         | 99        | 0  | 0         | 99        | 0  | 0         | 99        |
| 1  | 5000      | 0         | 1  | 5000      | 0         | 1  | 5000      | 0         | 1  | 5000      | 0         |
| 2  | 10000     | 0         | 2  | 10000     | 0         | 2  | 10000     | 0         | 2  | 10000     | 0         |
| 3  | 15000     | 0         |    |           |           |    |           |           |    |           |           |
+----+-----------+-----------+----+-----------+-----------+----+-----------+-----------+----+-----------+-----------+
```


Copyright© 2022 Ciena® Corporation

The following example displays jitter results from the MEP.

```
cfm mep show service cfm-3200 mepid 2
```

```
+------------------------------- CFM MEP INFO -------------------------------------+
| Parameter                          | Value                                       |
+------------------------------------+---------------------------------------------+
| Service                            | cfm-3200                                    |
| Service Type                       | Virtual Switch                              |
| Virtual Switch Name                | vs3200                                      |
| Service Network                    | 3200                                        |
| Port                               | 3                                           |
| VLAN                               | 200                                         |
| MEPID                              | 2                                           |
| Mac Address                        | 00:02:5A:01:E0:2D                           |
| Type                               | Up                                          |
| Admin State                        | enabled                                     |
| Accelerated                        | No                                          |
| CCM State                          | on                                          |
| CCM Priority                       | 7                                           |
| Tag Mode                           | off                                         |
| Tag VID                            | 0                                           |
| Tag Priority                       | 7                                           |
| Block Opposite Fault Threshold     | 0                                           |
| Block Opposite Fault Time          | 5                                           |
| Next Loopback Sequence Number      | 1                                           |
| Next Linktrace Sequence Number     | 1                                           |
| Rx Total Valid Frames              | 5054                                        |
| Rx Total Invalid Frames            | 0                                           |
| Rx Invalid Message Overflow        | 0                                           |
| Rx Invalid Port Status TLV         | 0                                           |
| Rx Invalid Interface Status TLV    | 0                                           |
| Rx Invalid Sender ID TLV           | 0                                           |
| Rx Invalid Blocked by Opposite MEP | 0                                           |
| Tx CCM                             | 4954                                        |
| Rx Valid CCM                       | 4954                                        |
| Rx CCM In Sequence                 | 5054                                        |
| Rx CCM Sequence Errors             | 0                                           |
| Rx MD Level Xcon CCM               | 0                                           |
| Rx MAID Xcon CCM                   | 0                                           |
| Rx MEPID Error CCM                 | 0                                           |
| Rx CCM-Interval Error CCM          | 0                                           |
| Rx Invalid CCM                     | 0                                           |
| Tx Loopback Message                | 0                                           |
| Tx Loopback Reply                  | 0                                           |
| Rx In-order Loopback Reply         | 0                                           |
| Rx Out-of-order Loopback Reply     | 0                                           |
| Rx Content Mismatch Loopback Reply | 0                                           |
| Rx Unexpected Loopback Reply       | 0                                           |
| Rx Invalid Loopback Reply          | 0                                           |
| Rx Valid Loopback Message          | 0                                           |
| Rx Invalid Loopback Message        | 0                                           |
| Tx Linktrace Message               | 0                                           |
| Rx Valid Linktrace Message         | 0                                           |
| Rx Invalid Linktrace Message       | 0                                           |
| Rx Valid Linktrace Reply           | 0                                           |
| Rx Invalid Linktrace Reply         | 0                                           |
| Rx Unexpected Linktrace Reply      | 0                                           |
| Rx Invalid Linktrace Relay Action  | 0                                           |
| Tx Linktrace Reply                 | 0                                           |
| Delay Measurement Repeats          | Disabled                                    |
| Delay Measurement Delay (min)      | 0                                           |
| Tx Delay Measurement Message       | 100                                         |
| Rx Valid Delay Measurement Message | 0                                           |
| Rx Invalid Delay Measurement Message | 0                                         |
| Tx Delay Measurement Reply         | 0                                           |
| Rx Valid Delay Measurement Reply   | 100                                         |
| Rx Invalid Delay Measurement Reply | 0                                           |
| Rx Unexpct Delay Measurement Reply | 0                                           |
| Rx Delay Measurement Reply Timeout | 0                                           |
| Frame Loss Measurement Repeats     | Disabled                                    |
| Frame Loss Measurement Delay (min) | 0                                           |
| Tx Frame Loss Measurement Message  | 0                                           |
| Rx Valid Frame Loss Message        | 0                                           |
| Rx Invalid Frame Loss Message      | 0                                           |
| Tx Frame Loss Measurement Reply    | 0                                           |
| Rx Valid Frame Loss Reply          | 0                                           |
| Rx Invalid Frame Loss Reply        | 0                                           |
| Rx Frame Loss Measure Reply Timeout | 0                                          |
| Tx Synthetic Loss Measurement Msg  | 0                                           |
| Rx Valid Synthetic Loss Message    | 0                                           |
| Rx Invalid Synthetic Loss Message  | 0                                           |
| Tx Synthetic Loss Message Reply    | 0                                           |
| Rx Valid SLM Reply                 | 0                                           |
| Rx Invalid SLM Message Reply       | 0                                           |
| Rx SLM Message Reply Timeout       | 0                                           |
+------------------------- Last Loopback Message ---------------------------------+
| Target Remote MEPID                | 0                                           |
| Target Mac Address                 | 00:00:00:00:00:00                           |
| Priority:                          | 7                                           |
| Count:                             | 0                                           |
| First Sequence Number              | 0                                           |
| LBMs Sent                          | 1                                           |
| LBMs To Send                       | 0                                           |
| Rx In-order Loopback Reply         | 0                                           |
| Rx Out-of-order Loopback Reply     | 0                                           |
| Rx Content Mismatch                | 0                                           |
+--------------------- Last Delay Measurement Message -------------------------------+
| Target Remote MEPID                | 12                                          |
| Target Mac Address                 | 00:23:8A:EF:C0:44                           |
| Test ID                            | 1                                           |
| Iteration                          | 1                                           |
| Priority                           | 7                                           |
```


Copyright© 2022 Ciena® Corporation

```
| DMM Interval                        | 3                                                |
| Repeat Delay                        | 0                                                |
| Iteration Count                     | 1                                                |
| Timeout                             | 5000                                             |
| CFM Frame Size                      | 68                                               |
| Frame Count Tx                      | 50                                               |
| Frame Count Rx                      | 50                                               |
| Min Delay in us                     | 4                                                |
| Ave Delay in us                     | 6                                                |
| Max Delay in us                     | 8                                                |
| Min Jitter in us                    | 0                                                |
| Ave Jitter in us                    | 0                                                |
| Max Jitter in us                    | 3                                                |
| Total Jitter in us                  | 45                                               |
| Forward Min Jitter in us            | 0                                                |
| Forward Ave Jitter in us            | 0                                                |
| Forward Max Jitter in us            | 2                                                |
| Forward Total Jitter in us          | 26                                               |
| Backward Min Jitter in us           | 0                                                |
| Backward Ave Jitter in us           | 0                                                |
| Backward Max Jitter in us           | 1                                                |
| Backward Total Jitter in us         | 19                                               |
+-------------------- Last Frame Loss Measurement Message ----------------------------+
| Target Remote MEPID                 | 0                                                |
| Target Mac Address                  | 00:23:8A:EF:C0:44                                |
| Test ID                             | 0                                                |
| Iteration                           | 0                                                |
| Priority                            | 0                                                |
| LMM Interval                        | 0                                                |
| Repeat Delay                        | 0                                                |
| Iteration Count                     | 0                                                |
| Timeout                             | 0                                                |
| Frame Count Tx                      | 0                                                |
| Frame Count Rx                      | 0                                                |
| Frame Loss Near                     | 0                                                |
| Frame Loss Far                      | 0                                                |
| Bad Sequence Number                 | 0                                                |
| Missing Sequence Number             | 0                                                |
| Frame Loss Near Fault Threshold     | 0                                                |
| Frame Loss Far Fault Threshold      | 0                                                |
| Frame Loss Bad Seq Fault Threshold  | 0                                                |
+------------------ Last Synthetic Loss Measurement Message --------------------------+
| Target Remote MEPID                 | 0                                                |
| Target Mac Address                  | 00:23:8A:EF:C0:44                                |
| Test ID                             | 0                                                |

| Iteration                           | 0                                                |
| Frame Count Tx                      | 0                                                |
| Frame Count Rx                      | 0                                                |
| Priority                            | 0                                                |
| SLM Interval                        | 0                                                |
| Repeat Delay                        | 0                                                |
| Iteration Count                     | 0                                                |
| Timeout                             | 0                                                |
| CFM Frame Size                      | 0                                                |
| Frame Loss Near                     | 0                                                |
| Frame Loss Far                      | 0                                                |
| Synthetic Loss Near Fault Threshold | 0                                                |
| Synthetic Loss Far Fault Threshold  | 0                                                |
+--------------------------- Last Linktrace Message ----------------------------------+
| Target Remote MEPID                 | 0                                                |
| Target Mac Address                  | 00:00:00:00:00:00                                |
| Priority                            | 7                                                |
| Sequence Number                     | 0                                                |
| Initial TTL                         | 0                                                |
| Use FDB Only                        | No                                               |
+------------------------------------------------------- Linktrace Responses -----------------------------------------------------+
|   |Ttl|          |   Remote MP      | Relay |Flags|                                      |                                   |
|Ttl|Idx|Trans Id  | Mac Address      |Action |FY|TM| Ingress TLV                          | Egress TLV                        |
+---+---+----------+------------------+-------+--+--+--------------------------------------+-----------------------------------+
```

The following example displays delay and jitter results broken down by bins.

```
cfm show service cfm-3200 local-mepid 2 mepid 12 test-id 1 bins
+---------------------------- DELAY MEASUREMENT RESULT BINS ----------------------------+
| Service Name                              | cfm-3200                                   |
| Service Index                             | 1                                          |
| Local Mepid                               | 2                                          |
| Remote Mepid                              | 12                                         |
| Test ID                                   | 1                                          |
+-----+--------------------------------------------------------------------------------+
|     |             Delay Result              |     |            Jitter Result             |
| Bin | Threshold (us)     | Count            |Bin  | Threshold (us)      | Count          |
+-----+--------------------+------------------+-----+---------------------+----------------+
| 0   | 0                  | 50               | 0   | 0                   | 49             |
| 1   | 10                 | 0                | 1   | 10                  | 0              |
| 2   | 20                 | 0                | 2   | 20                  | 0              |
| 3   | 30                 | 0                | 3   | 30                  | 0              |
| 4   | 40                 | 0                | 4   | 40                  | 0              |
| 5   | 50                 | 0                | 5   | 50                  | 0              |
| 6   | 60                 | 0                | 6   | 60                  | 0              |
| 7   | 70                 | 0                | 7   | 70                  | 0              |
| 8   | 80                 | 0                | 8   | 80                  | 0              |
| 9   | 90                 | 0                | 9   | 90                  | 0              |
| 10  | 100                | 0                | 10  | 100                 | 0              |
|     |                    |                  +-----+---------------------+----------------|
|     |                    |                  |              Forward                      |
```


Copyright© 2022 Ciena® Corporation

			0	0	49
			1	10	0
			2	20	0
			3	30	0
			4	40	0
			5	50	0
			6	60	0
			7	70	0
			8	80	0
			9	90	0
			10	100	0
			Backward		
			0	0	49
			1	10	0
			2	20	0
			3	30	0
			4	40	0
			5	50	0
			6	60	0
			7	70	0
			8	80	0
			9	90	0
			10	100	0

The following example displays delay and jitter results for the CFM service cfm-3200, local MEP identifier 2, MEP identifier 12 and Test ID 1 broken down by bins.

```
cfm delay show service cfm-3200 local-mepid 2 mepid 12 test-id 1 bins
```

DELAY MEASUREMENT RESULT BINS

Service Name	cfm-3200
Service Index	1
Local Mepid	2
Remote Mepid	12
Test ID	1

Delay Result			Jitter Result		
Bin	Threshold (us)	Count	Bin	Threshold (us)	Count
0	0	50	0	0	49
1	10	0	1	10	0
2	20	0	2	20	0
3	30	0	3	30	0
4	40	0	4	40	0
5	50	0	5	50	0
6	60	0	6	60	0
7	70	0	7	70	0
8	80	0	8	80	0
9	90	0	9	90	0
10	100	0	10	100	0
			Forward		
			0	0	49
			1	10	0
			2	20	0
			3	30	0
			4	40	0
			5	50	0
			6	60	0
			7	70	0
			8	80	0
			9	90	0
			10	100	0
			Backward		
			0	0	49
			1	10	0
			2	20	0
			3	30	0
			4	40	0
			5	50	0
			6	60	0
			7	70	0
			8	80	0
			9	90	0
			10	100	0

Copyright© 2022 Ciena® Corporation

The following example displays SLM statistics for all services.

```
cfm synthetic-loss show
+------------------------------------ SYNTHETIC LOSS MEASUREMENT MESSAGE INFORMATION ------------------------------------+
|              |Local|Remote           |Remote|          |          |     |     | FD    |             |             |Rep |   |
|Service       |Mepid|Mac Address      |Mepid |  TestId  |Iteration | SLM | SLR | Ratio |Near Loss    |Far Loss     |Time|Acc|
+--------------+-----+-----------------+------+----------+----------+-----+-----+-------+-------------+-------------+----+---+
|cfm-3200      |2    |00:23:8A:EF:C0:44|12    |1         |1         |94   |48   | 51.06%|           0|           0|N/A |No |
|              |     |                 |      |          |          |     |     |       |Ratio:  0.00%|Ratio:  0.00%|    |   |
|              |     |                 |      |          |          |     |     |       |Min:        0|Min:        0|    |   |
|              |     |                 |      |          |          |     |     |       |Avg:        0|Avg:        0|    |   |
|              |     |                 |      |          |          |     |     |       |Max:        0|Max:        0|    |   |
+--------------+-----+-----------------+------+----------+----------+-----+-----+-------+-------------+-------------+----+---+
```

The following example displays SLM history for a service.

```
cfm synthetic-loss show service cfm-3200 local-mepid 2 mepid 12 test-id 1
history
+-------------- MEP SLM INFORMATION --------------+
|                |Local |      Local      |Test   |
|Service         |MEP ID|   Mac Address   |Results|
+----------------+------+-----------------+-------+
|cfm-3200        |2     |00:02:5A:01:E0:2D|1      |
+----------------+------+-----------------+-------+

+------------------------------------------------ MEP SYNTHETIC LOSS MEASUREMENT HISTORY ------------------------------------+
|                          |                          |          |     |     | FD    |                |                |      |
|    Session Parameters    |           Time           |Iteration| SLM | SLR | Ratio |   Near Loss    |   Far Loss     |Status|
+--------------------------+--------------------------+----------+-----+-----+-------+----------------+----------------+------+
|RMEP ID: 12               |Start: 06/20/2016 17:27:09|1         |94   |48   | 51.06%|             0|             0|Tout  |
|TestId: 1                 |End:   06/20/2016 17:27:23|          |     |     |       |Ratio:    0.00%|Ratio:    0.00%|      |
|Priority: 7               |Duration (ms): 14387      |          |     |     |       |Min:          0|Min:          0|      |
|Interval: 100ms           |                          |          |     |     |       |Avg:          0|Avg:          0|      |
|RMEP MAC: 00:23:8A:EF:C0:44|                         |          |     |     |       |Max:          0|Max:          0|      |
|Frame Size: 64            |                          |          |     |     |       |                |                |      |
|Accelerate: No            |                          |          |     |     |       |                |                |      |
+--------------------------+--------------------------+----------+-----+-----+-------+----------------+----------------+------+
```

The following example displays SLM statistic history for a service with counters.

```
cfm synthetic-loss show service cfm-3200 local-mepid 2 mepid 12 test-id 1
history-with-counters

+-------------- MEP SLM INFORMATION --------------+
|                |Local |      Local      |Test   |
|Service         |MEP ID|   Mac Address   |Results|
+----------------+------+-----------------+-------+
|cfm-3200        |2     |00:02:5A:01:E0:2D|1      |
+----------------+------+-----------------+-------+

+------------------------------------ MEP SYNTHETIC LOSS MEASUREMENT HISTORY ------------------------------------+
|                          |                |          |     |     | FD    |                |                |      |
|    Session Parameters    |   counters     |Iteration| SLM | SLR | Ratio |   Near Loss    |   Far Loss     |Status|
+--------------------------+----------------+----------+-----+-----+-------+----------------+----------------+------+
|RMEP ID: 12               |Start:          |1         |94   |48   | 51.06%|             0|             0|Tout  |
|TestId: 1                 |txFCf:         1|          |     |     |       |Ratio:    0.00%|Ratio:    0.00%|      |
|Priority: 7               |txFCb:       507|          |     |     |       |Min:          0|Min:          0|      |
|Interval: 100ms           |rxFCl:         1|          |     |     |       |Avg:          0|Avg:          0|      |
|RMEP MAC: 00:23:8A:EF:C0:44|End:            |          |     |     |       |Max:          0|Max:          0|      |
|Frame Size: 64            |txFCf:        48|          |     |     |       |                |                |      |
|Start: 06/20/2016 17:27:09|txFCb:       554|          |     |     |       |                |                |      |
|End:   06/20/2016 17:27:23|rxFCl:        48|          |     |     |       |                |                |      |
|Duration (ms): 14387      |                |          |     |     |       |                |                |      |
+--------------------------+----------------+----------+-----+-----+-------+----------------+----------------+------+
```

The following example displays SLM statistics for a service and a particular test ID.

```
cfm synthetic-loss show service cfm-3200 local-mepid 2 mepid 12 test-id 1
+---------------------- CFM SYNTHETIC LOSS SESSION INFO ----------------------------+
| Parameter                                | Value                                    |
+------------------------------------------+------------------------------------------+
| Service Name                             | cfm-3200                                 |
| Service Index                            | 1                                        |
```


Copyright© 2022 Ciena® Corporation

```
| Local Mepid                          | 2                                          |
| Remote Mepid                         | 12                                         |
| Test ID                              | 1                                          |
| Priority                             | 7                                          |
| Source MAC Address                   | 00:02:5A:01:E0:2D                          |
| Target MAC Address                   | 00:23:8A:EF:C0:44                          |
| SLM Interval                         | 100ms                                      |
| Count                                | 94                                         |
| Duration (sec)                       | 9                                          |
| Iteration Count                      | 1                                          |
| Repeat Delay (minutes)               | 0                                          |
| Repeat Flag                          | 0                                          |
| Rx Timeout                           | 5000                                       |
| Device TYpe                          | 0                                          |
| Configured Frame Size                | 64                                         |
| Fln Threshold                        | -1                                         |
| Flf Threshold                        | -1                                         |
| Accelerated                          | N/A                                        |
| Config Accelerated                   | No                                         |
+---------------------------- Last Test Result ---------------------------------------+
| Iteration                            | 1                                          |
| Start                                | 06/20/2016 17:27:09                        |
| End                                  | 06/20/2016 17:27:23                        |
| Duration (ms)                        | 14387                                      |
| SLM Tx                               | 94                                         |
| SLR Rx                               | 48                                         |
| Frame Delivery Ratio                 | 51.06%                                     |
| Far Loss                             | 0                                          |
|    Ratio                             | 0.0000%                                    |
|    Minimum                           | 0                                          |
|    Average                           | 0                                          |
|    Maximum                           | 0                                          |
| Near Loss                            | 0                                          |
|    Ratio                             | 0.0000%                                    |
|    Minimum                           | 0                                          |
|    Average                           | 0                                          |
|    Maximum                           | 0                                          |
| Frame Size                           | 64                                         |
| Status                               | Tout                                       |
+-------------------------------------+----------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-29
Configuring Y.1731 LMMs

Send and display Y.1731 LMMs for troubleshooting purposes. You can:

- send LMMs to a remote MEP
- send LMMs to a MAC address
- cancel remote MEP LMM transmission
- cancel MAC address LMMs transmission

Table 2-31 provides descriptions for the MEP Frame Loss message information fields.

Table 2-31
Fields in the MEP Frame Loss message

Field	Description
Local Mepid	The local MEP ID.
Remote Mac Address	MAC address of the peer MEP.
Remote Mepid	MEP ID of the peer.
Loss Near	Frame loss associated with ingress data frames.
Loss Far	Frame loss associated with egress data frames.
Bad Seq	"Bad Sequence Identifier": Number of received LMRs that contained a Sequence Identifier TLV, but its value did not match the expected sequence identifier for the test iteration.
Seq Miss	"Sequence Identifier Missing": Number of received LMRs that did not contain a Sequence Identifier TLV.
Rep Time	Time interval in minutes between subsequent iterations of a repeating frame-loss test.

Copyright© 2022 Ciena® Corporation

Step	Action

To send LMMs to a remote MEP

1 Send LMMs to a remote MEP:

```
cfm frame-loss send service <service> {local-mepid
<NUMBER: 1-8191>|port <PortName> [vlan <Vlan>]} {mepid
<NUMBER: 1-8191>|mac <remote-mac-address>} [test-id
<INTEGER: 0..4294967295>] [count <NUMBER: 2-600>|
duration <SECONDS: 1.. 65535 >][priority <NUMBER: 0-
7>][fln-threshold <NUMBER: 0-600>] [flf-threshold <0-
600>] [lmm-interval <lmm-interval-enum>] [iterate
<NUMBER: 0..60> repeat-delay <MINUTES:0-1440>] [timeout
<MILLISECONDS: 2000..10,000>] [accelerate] [data-
priority<String: 0..7|all>]
```

where

service <service	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
mac <remote-mac-address>	is the unicast MAC address of the remote MEP.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)
count <NUMBER: 2-600>	is the number of LMM frames to transmit per loss measurement test (count). Valid range is 2 - 600 and the default value is 2. (Optional)
duration <SECONDS: 1.. 65535 >	is the amount of time in seconds the test iteration should run and is mutually exclusive with count.
priority <NUMBER: 0-7>	is the priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). Default is 7. (Optional)
fln-threshold <NUMBER: 0-600>	is the near loss threshold to generate an event and trap when test results continuously exceed the value. (Optional)
flf-threshold <0-600>	is the far loss threshold to generate an event and trap when test results continuously exceed the value. (Optional). In SAOS 6.13, this threshold is not supported while initiated in hardware. The value will always be 0.

Copyright© 2022 Ciena® Corporation

where

lmm-interval <lmm-interval-enum>	is the interval at which LMMs are sent. If the LMM interval is not specified, then service level setting for the LMM interval will be used.
iterate <NUMBER: 0..60>	is the number of discrete tests invoked within a test session. Setting the iterate attribute to 0 establishes continuous test.
repeat-delay <MINUTES:0-1440>	is the amount of time to wait between each test iteration, in minutes.
timeout <MILLISECONDS : 2000..10,000>	is the timeout.
accelerate	indicates that the test is hardware-based. ***Note:*** Frame-loss sessions do not need the enhanced CFM port to be reserved. Frame-loss sessions work with or without the enhanced CFM port reserved on 3924, 3926 and 3928 platforms.
data-priority<String: 0..7|all>	is the priority at which the traffic is counted.

To send LMMs to a MAC address

2 Send LMMs to a MAC address:

```
cfm frame-loss send-mac {service <service>} {local-mepid
<NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} {mac
<MacAddress>} [count <NUMBER: 2-600>] [priority <NUMBER:
0-7>] [repeat <NUMBER: 0-1440>] [fln-threshold <NUMBER:
0-600>] [flf-threshold <0-600>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mac <MacAddress>	is the mac address.
count <NUMBER: 2-600>	is the number of LMM frames to transmit per loss measurement test (count). Valid range is 2 - 600 and the default value is 2. (Optional)
priority <NUMBER: 0-7>	is the priority and drop eligible values to be used in the VLAN tag of the transmitted frame (priority). Default is 7. (Optional)

Copyright© 2022 Ciena® Corporation

where

repeat <NUMBER: 0-1440	is the Auto-Repeat Interval (repeat), if the test should be repeated. Valid range 0 - 1440 minutes. By default a test will not be auto-repeated. A value of 0 indicates that the test should run continuously. (Optional)
fln-threshold <NUMBER: 0-600>	is the near loss threshold to generate an event and trap when test results continuously exceed the value. (Optional)
flf-threshold <0-600>	is the far loss threshold to generate an event and trap when test results continuously exceed the value. (Optional) In SAOS 6.13, this threshold is not supported while initiated in hardware. The value will always be 0.

To cancel remote MEP LMM transmission

3 Cancel remote MEP LMM transmission:

```
cfm frame-loss cancel {service <service>} {local-mepid
<NUMBER: 1-8191>|port <PortName> [vlan <Vlan>]} {mepid
<NUMBER: 1-8191>|mac <remote-mac-address>} [test-id
<INTEGER: 0..4294967295>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
mac <remote-mac-address>	is the unicast MAC address of the remote MEP.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)

Copyright© 2022 Ciena® Corporation

To cancel MAC address LMMs transmission

4 Cancel MAC address LMMs transmission:

```
cfm frame-loss cancel-mac {service <service>} {local-
mepid <NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]}
{mac <MacAddress>}
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mac <MacAddress>	is the mac address.

To delete an LMM session test

5 Delete an LMM session test:

```
cfm frame-loss delete service <service> {port <port-list>
vlan<VLAN>|local-mepid< <NUMBER: 1..8191>} {mepid <
<NUMBER: 1..8191>} [test-id <INTEGER: 0..4294967295>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)

To free resources for LMM

6 Set the VC statistics resource classifier count:

```
resource-manager pool set feature vc-statistics resource
classifier count 0
```

7 Set the VC statistics resource counter;

```
resource-manager pool set feature vc-statistics resource
counter count 0
```


Copyright© 2022 Ciena® Corporation

8 Set the loss-measurement classifier count:

```
resource-manager pool set feature loss-measurement
resource classifier count 256
```

9 Validate the settings:

```
resource manager validate
```

10 Save the configuration:

```
configuration save
```

11 Reboot the chassis:

```
chassis reboot
```

—end—

Example

The following example sends LMMs to a remote MEP.

```
cfm frame-loss send service CFM_VLAN_10 local-mepid 2 mepid 1
```

The following example sends LMMs to a MAC address.

```
cfm frame-loss send-mac service CFM-VLAN_10 local-mepid 2 mac
01:02:03:04:05:06 repeat 1 count 250 fln-threshold 200 flf-
threshold 400
```

The following example displays LMM test results.

```
> cfm frame-loss show

+---------- MEP FRAME LOSS MEASUREMENT MESSAGE INFORMATION ------------------+
|         |Local|Remote           |Remote|     |     |Loss|Loss|Bad |Seq  |Rep |
|Service  |Mepid|Mac Address      |Mepid |LMM  |LMR  |Near|Far |Seq |Miss |Time|
+---------+-----+-----------------+------+-----+-----+----+----+----+-----+----+
|v1001    |119  |00:02:A1:4A:66:E0|6     |20   |20   |0   |0   |0   |20   |    |
+---------+-----+-----------------+------+-----+-----+----+----+----+-----+----+
```

The following example cancels remote MEP LMM transmission.

```
cfm frame-loss cancel service CFM_VLAN_10 local-mepid 2 mepid 1
```

The following example cancels MAC address LMMs transmission:

```
cfm frame-loss send-mac service CFM_VLAN_10 local-mepid 2 mac
01:02:03:04:05:06
```

The following example shows that the resources are not free for that feature:

```
> resource-manager show

+-------------------------+-----------+----------+------+----------+-----------+
|                        ACTIVE RESOURCE CONFIGURATION                          |
+-------------------------+-----------+----------+------+----------+-----------+
| feature                 | resource  | reserved | used | increment| pltfm max |
+-------------------------+-----------+----------+------+----------+-----------+
| broadcast-containment   | classifier| 256      | 1    | 256      | 256       |
```


Copyright© 2022 Ciena® Corporation

	meter	256	0	256	256
	counter	256	0	256	256
loss-measurement	classifier	0	0	256	768
	meter	0	0	256	768
	counter	0	0	256	768
traffic-profiling	classifier	1024	20	256	1536
	meter	1792	0	256	2048*
	counter	1024	40	256	1536
transport-oam	classifier	0	0	256	256
	meter	0	0	256	256
	counter	0	0	256	256
vc-statistics	classifier	256	0	256	1536
	meter	0	0	256	1536
	counter	256	0	256	1536
vs-enhanced-l2-transform	classifier	0	0	256	256
	meter	0	0	256	256
	counter	0	0	256	256

Copyright© 2022 Ciena® Corporation

Procedure 2-30
Configuring LMM responders

You can:

- create an LMM responder
- delete an LMM responder
- display LMM responders

Step	Action

To create an LMM responder

1 Create an LMM responder in hardware from the local mep identified by the local-mepid or port and vlan combination to a remote mep identified by the mepid:

```
cfm frame-loss-responder create service <service> {port
<port-list> vlan<VLAN>|local-mepid< <NUMBER: 1..8191>}
{mepid <NUMBER: 1..8191>} accelerate [data- priority
<String: 0..7|all>]>]
```

where

service <service>	is the CFM service name.
port<port-list>	is the port or ports.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid < <NUMBER: 1..8191>	is the remote MEP identifier.
accelerate	identifies the service as a hardware-assisted service. ***Note:*** This option does not need the enhanced CFM port to be reserved on the 3924, 3926 and 3928 platforms. The enhanced CFM port is only needed for DM/SLM initiator responders' CLI.
data-priority<String: 0..7 | all>	is the priority at which the traffic should be counted.

Copyright© 2022 Ciena® Corporation

To delete an LMM responder

2 Delete an LMM responder in hardware from the local mep identified by the local-mepid or port and vlan combination to a remote mep identified by the mepid:

```
cfm frame-loss-responder delete service <service> {port
<port-list> vlan<VLAN>|local-mepid< <NUMBER: 1..8191>}
{mepid <NUMBER: 1..8191>}
```

where

service <service>	is the CFM service name.
port<port-list>	is the port or ports.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid < <NUMBER: 1..8191>	is the remote MEP identifier.

To display LMM responders

3 Display LMM responders in hardware for a service:

```
cfm frame-loss-responder clear service <service> {port
<port-list> vlan <VLAN>|local-mepid< <NUMBER: 1..8191>}
{mepid <NUMBER: 1..8191>}
```

where

service <service>	is the CFM service name.
port<port-list>	is the port or ports.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid < <NUMBER: 1..8191>	is the remote MEP identifier.

Copyright© 2022 Ciena® Corporation

To clear statistics associated with an LMM responder

4 Clear statistics associated with the LMM responder in hardware from the local mep identified by the local-mepid or port and vlan combination to a remote mep identified by the mepid:

```
cfm frame-loss-responder clear service <service>
{port<port-list> vlan<VLAN>|local-mepid <NUMBER:
1..8191>} {mepid <NUMBER: 1..8191>}
```

where

service <service>	is the CFM service name.
port<port-list>	is the port or ports.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid < <NUMBER: 1..8191>	is the remote MEP identifier.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-31
Configuring single-ended synthetic frame loss measurement

Configure single-ended synthetic frame loss measurement to:

- initiate a synthetic loss measurement test between a local and remote MEP
- calculate and store test results

When a synthetic frame loss measurement session is canceled, the session in progress is terminated for repeating and single iterations. The session remains visible. The continuous test is still written to the system configuration file.

When a synthetic frame loss measurement session is deleted for a test that is active, the session is permanently deleted. The session is no longer visible. The test results remain in MEP history. The continuous test is no longer written to the system configuration file.

CFM maintains a history of Synthetic Loss test results for each local MEP. Each history entry corresponds to a session iteration. The history can contain results from multiple sessions, that is, current and past sessions. When the history is full, a new entry replaces the oldest entry.

You can

- configure single-ended synthetic frame loss measurement
- configure a single-ended synthetic loss responder session
- cancel synthetic frame loss auto-test to a remote MEP
- delete all synthetic frame loss measurement sessions
- delete a specific synthetic frame loss measurement session
- clear SLM statistics

Step	Action

To configure single-ended synthetic frame loss measurement

1 Configure single-ended synthetic frame loss measurement on the sender using the MEP ID:

```
cfm synthetic-loss send service <service> {port <Port>}
{vlan <VLAN>} {local-mepid <NUMBER: 1-8191>} {mepid
<NUMBER: 1-8191>} {test-id <NUMBER: 1-4294967295>} {count
<NUMBER: 2-65535>|duration <INTEGER: 1.. 65535 >]} {slm-
interval <2 | 3 | 4 | 5 | 6 | 7 | 10ms | 100ms | 1sec |
```


Copyright© 2022 Ciena® Corporation

```
10sec | 1min | 10min>} {priority <NUMBER: 0-7>} {repeat-
delay <NUMBER: 0-1440>} {iterate <NUMBER: 0-60>} {timeout
<MILLISECONDS: 2000-10000>} [accelerate] {frame-size
<NUMBER: 47-1400>} {fln-threshold <NUMBER: 0-65535>}
{flf-threshold <NUMBER: 0-65535>}
```

where

service <service>	is the service name.
port <Port>	is the port.
vlan <VLAN>	is the VLAN.
local-mepid <NUMBER: 1-8191>	is the local MEPID.
mepid <NUMBER: 1-8191>	is the MEP ID.
test-id <NUMBER: 1-4294967295>	is the test ID.
count <NUMBER: 2-65535>	is the number of SLMs to send. The default value is 2.
duration <INTEGER: 1.. 65535 >]	is the amount of time in seconds that the test iteration runs. Duration is mutually exclusive with count.
slm-interval <2 | 3 | 4 | 5 | 6 | 7 | 10ms | 100ms | 1sec | 10sec | 1min | 10min>}	is the SLM transmission interval index or time. The default value is 1000ms.
priority<NUMBER: 0-7>	is the SLM message priority. The default value is 7.
repeat-delay <NUMBER: 0-1440>	is the delay in minutes between consecutive iterations. The default value is 0.
iterate <NUMBER: 0-60>	is the number of times the SLM test has to iterate. The default value is 1. The value for continuous test is 0.
timeout <MILLISECONDS: 2000-10000>	is the SLM timeout. The default value is 5000.
frame-size <NUMBER: 64-1400>	is the base CFM frame size, without encapsulation.

Copyright© 2022 Ciena® Corporation

where

accelerate	indicates that the test is hardware-based (optional). ***Note:*** On the 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved before using the accelerate option.
fln-threshold <NUMBER: 0-65535>	is the Frame Loss Near error threshold.
flf-threshold <NUMBER: 0-65535>	is the Frame Loss Far error threshold.

To create a synthetic-loss-responder session

2 Create a synthetic-loss-responder session in hardware from the local mep identified by the local-mepid or port and vlan combination to a remote mep identified by the mepid:

```
cfm synthetic-loss-responder create service <service>
{port <port-list> vlan<VLAN>|local-mepid< <NUMBER:
1..8191>} {mepid <NUMBER: 1..8191>} [accelerate]
```

where

service <service>	is the CFM service name.
port<port-list>	is the port or ports.
vlan<VLAN>	is the VLAN.
local-mepid< <NUMBER: 1..8191>	is the local MEP identifier.
mepid < <NUMBER: 1..8191>	is the remote MEP identifier.
accelerate	identifies the service as a hardware-assisted service (optional).

To cancel synthetic frame loss auto-test to a remote MEP

3 Cancel synthetic frame loss auto-test to a remote MEP:

```
cfm synthetic-loss cancel service <service> {port <Port>}
{vlan <VLAN>} {local-mepid <NUMBER: 1-8191>} {mepid
<NUMBER: 1-8191>} {test-id <NUMBER: 1-4294967295>}
```

where

service <service>	is the service name.
port <Port>	is the port.
vlan <VLAN>	is the VLAN.

Copyright© 2022 Ciena® Corporation

where

local-mepid <NUMBER: 1-8191>	is the local MEPID.
mepid <NUMBER: 1-8191>	is the remote MEPID.
test-id <NUMBER: 1-4294967295>	is the test ID.

To delete all synthetic frame loss measurement sessions

4 Delete all synthetic frame loss measurement sessions:

```
cfm synthetic-loss delete
```

To delete a specific synthetic frame loss measurement session

5 Delete a specific synthetic frame loss measurement session:

```
cfm synthetic-loss delete service <service> {port <Port>}
{vlan <VLAN>} {local-mepid <NUMBER: 1-8191>} {mepid
<NUMBER: 1-8191>} {test-id <NUMBER: 1-4294967295>}
```

where

service <service>	is the service name.
port <Port>	is the port.
vlan <VLAN>	is the VLAN.
local-mepid <NUMBER: 1-8191>	is the local MEPID.
mepid <NUMBER: 1-8191>	is the remote MEPID.
test-id <NUMBER: 1-4294967295>	is the test ID.

Copyright© 2022 Ciena® Corporation

To clear SLM statistics

6 Clear SLM statistics:

```
cfm synthetic-loss clear service <service> {port <Port>}
{vlan <VLAN>} {local-mepid <NUMBER: 1-8191>} {mepid
<NUMBER: 1-8191>} {test-id <NUMBER: 1-4294967295>}
{statistics} {history}
```

where

service <service>	is the CFM service.
port <Port>	is the port.
vlan <VLAN>	is the VLAN.
local-mepid <NUMBER: 1-8191>	is the local MEPID.
mepid <NUMBER: 1-8191>	is the remote MEPID.
test-id <NUMBER: 1-4294967295>	is the test ID.
statistics	clears statistics.
history	clears history.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-32
Displaying and clearing CFM statistics

Display and clear CFM statistics for troubleshooting purposes. You can:

- display global CFM statistics
- display CFM statistics for a specific service
- clear global CFM statistics
- clear CFM statistics for all services
- clear CFM statistics for a specific service
- clear CFM statistics for all MEPs
- clear CFM statistics for a specific MEP
- clear CFM statistics for all remote MEPs
- clear CFM statistics for a specific remote MEP
- clear delay measurement statistics for all or a specific service local MEP ID
- clear loss measurement statistics for all or a specific service local MEP ID

Step	Action

To display global CFM statistics

1 Display global CFM statistics:

```
cfm show statistics
```

To display CFM statistics for a specific service

2 Display CFM statistics for a specific service:

```
cfm service show service <service> statistics
```

where

service <service> is the CFM service name.

To clear global CFM statistics

3 Clear global CFM statistics:

```
cfm clear statistics
```

To clear CFM statistics for all services

4 Clear CFM statistics for all services:

```
cfm service clear statistics
```


Copyright© 2022 Ciena® Corporation

To clear CFM statistics for a specific service

5 Clear CFM statistics for a specific service:

```
cfm service clear service <service> statistics
```

where

service <service> is the CFM service name.

To clear CFM statistics for all MEPs

6 Clear CFM statistics for all MEPs:

```
cfm mep clear statistics
```

To clear CFM statistics for a specific MEP

7 Clear CFM statistics for a specific MEP:

```
cfm mep clear service <service> {mepid <NUMBER: 1-8191> |
port <PortName> [vlan <Vlan>]} statistics
```

where

service <service> is the CFM service name.

mepid <NUMBER: 1-8191> is the MEP identifier.

port <PortName> is the port.

vlan <Vlan> is the VLAN.

To clear CFM statistics for all remote MEPs

8 Clear CFM statistics for all remote MEPs:

```
cfm remote-mep clear statistics
```

To clear CFM statistics for a specific remote MEP

9 Clear CFM statistics for a specific remote MEP:

```
cfm remote-mep clear service <service> mep-id <NUMBER: 1-
8191> statistics
```

where

service <service> is the CFM service name.

mepid <NUMBER: 1-8191> is the MEP identifier.

Copyright© 2022 Ciena® Corporation

To clear delay measurement statistics for all or a specific service local MEP ID

10 Clear delay measurement statistics for all or a specific service local MEP ID:

```
cfm delay clear [service <service>] {local-mepid <NUMBER:
1-8191> | port <PortName> [vlan <Vlan>]}
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the local MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.

To clear loss measurement statistics for all or a specific service local MEP ID

11 Clear loss measurement statistics for all or a specific service local MEP ID:

```
cfm frame-loss clear [service <service>] {local-mepid
<NUMBER: 1-8191> | port <PortName> [vlan <Vlan>]} [mepid
<remote-mep-id>] [test-id <INTEGER: 0..4294967295>]
{statistics} [history]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the local MEP identifier.
port <PortName>	is the port.
vlan <Vlan>	is the VLAN.
mepid <NUMBER: 1-8191>	is the remote MEP identifier.
test-id <INTEGER: 0..4294967295>	is a unique test session in a local and remote MEP. The default value is 1 . If a test-id of 0 is used, then the DMM PDU is transmitted with 0 in the version field. (Optional)
statistics	displays statistics.
history	displays history.

—end—

Copyright© 2022 Ciena® Corporation

Example

Table 2-32 describes the global statistics CFM supports.

Table 2-32
CFM supported statistics

Statistics	Description
Tx Total Frames	Total CFM frames transmitted including CCM, Loopback, Linktrace, Delay Measurement, and Loss Measurement
Tx Flooded frames	Total non-local CFM frames flooded in the VS
Tx Flood ignored - STP state	Total CFM frames eligible to be flooded, but ignored because of STP state of the sub-interface
Rx Total Frames	Total CFM frames received including CCM, Loopback, Linktrace, Delay Measurement, and Loss Measurement
Rx Drop- STP state not Forwarding	Total CFM frames dropped because of the STP state
Rx Drop - L2 Loop	Total received CFM frames discarded by the L2 Loopback Detection feature
Rx Dropped - Blocked by Opposite MEP	Total frames dropped because they hit a higher level MEP of the opposite type.
Tx Total CSF	Total client signal fail (CSF) PDU transmitted
Tx Total CSF-Los	Total CSF Los PDU transmitted
Tx Total CSF-Dci	Total CSF Dci PDU transmitted
Rx Total Valid CSF	Total valid CSF PDU received
Rx Total Invalid CSF	Total invalid CSF PDU received
Rx Total CSF-Los	Total CSF Los PDU received
Rx Total CSF-Dci	Total CSF Dci PDU received

The following example shows sample output for the cfm show statistics command.

```
> cfm show statistics
```


Copyright© 2022 Ciena® Corporation

CFM GLOBAL STATISTICS	
Tx Total Frames	1252945758
Tx Flooded frames	1252945658
Tx Flood ignored - STP State	0
Rx Total Frames	1252860681
Rx Total Valid Frames	1252847005
Rx Total Frames Not Validated	0
Rx Total Invalid Frames	0
Invalid Message Overflow	0
Invalid Port Status TLV	0
Invalid Interface Status TLV	0
Invalid Sender ID TLV	0
Rx Forward - Unprocessed	0
Rx Drop - Admin Disable	0
Rx Drop - Invalid Etype	0
Rx Drop - Invalid Op-Code	0
Rx Drop - STP state not Forwarding	0
Rx Drop - L2 Loop	0
Rx Drop - Blocked by Opposite MEP	0
CCM:	
Tx Total CCM	2936970
Tx Total CCM Flooded	0
Rx Total Valid CCM	5565643
Rx Total CCM In Sequence	5565506
Rx Total CCM Sequence Errors	18
Rx Total MD Level Xcon CCM	0
Rx Total MAID Xcon CCM	0
Rx Total MEPID Error CCM	119
Rx Total CCM-Interval Error CCM	0
Rx Total Invalid CCM	0
Loopback:	
Tx Total LBM	0
Tx Total LBR	0
Rx Total In-order LBR	0
Rx Total Out-of-order LBR	0
Rx Total Content Mismatch	0
Rx Total Unexpected LBR	0
Rx Total Invalid LBR	0
Rx Total Valid LBM	0
Rx Total Invalid LBM	0
LinkTrace:	
Tx Total LTM	0
Tx Total LTR	0
Rx Total Valid LTM	0
Rx Total Valid LTR	0
Rx Total Unexpected LTR	0
Rx Total Invalid LTR	0
LTR Invalid Relay Action	0
Rx Total Invalid LTM	0
Rx Unresolved LTM	0
Delay Measurement:	
Tx Total DMM	2635427197
Tx Total DMR	100
Rx Total Valid DMM	100
Rx Total Invalid DMM	0
Rx Total Valid DMR	2634253262

Copyright© 2022 Ciena® Corporation

```
|    Rx Total Invalid DMR                  | 0                 |
|    Rx Total Unexpected DMR               | 0                 |
+------------------------------------------+-------------------+
| Loss Measurement:                        |                   |
|    Tx Total LMM                          | 0                 |
|    Tx Total LMR                          | 0                 |
|    Rx Total Valid LMM                    | 0                 |
|    Rx Total Invalid LMM                  | 0                 |
|    Rx Total Valid LMR                    | 0                 |
|    Rx Total Invalid LMR                  | 0                 |
+------------------------------------------+-------------------+
| Synthetic Loss Measurement:              |                   |
|    Tx Total SLM                          | 2909548787        |
|    Tx Total SLR                          | 0                 |
|    Rx Total Valid SLM                    | 0                 |
|    Rx Total Invalid SLM                  | 0                 |
|    Rx Total Valid SLR                    | 2907995285        |
|    Rx Total Invalid SLR                  | 0                 |
+------------------------------------------+-------------------+
| Client Signal Fail:                      |                   |
|    Tx Total CSF                          | 0                 |
|    Tx Total CSF-Los                      | 0                 |
|    Tx Total CSF-Dci                      | 0                 |
|    Rx Total Valid CSF                    | 0                 |
|    Rx Total Invalid CSF                  | 0                 |
|    Rx Total CSF-Los                      | 0                 |
|    Rx Total CSF-Dci                      | 0                 |
+------------------------------------------+-------------------+
```

The following example displays CFM statistics for a specific service.

```
> cfm service show service VLAN#2005 statistics

+------------------------------- CFM SERVICE STATS ----------------------+
| Parameter                                | Value                        |
+------------------------------------------+------------------------------+
| CFM Service Name                         | VLAN#2005                    |
| Service Index                            | 1                            |
| Service Type                             | VLAN                         |
+------------------------------------------+------------------------------+
| General Message Stats                    |                              |
|    Rx Total Valid Frames                 | 1253398979                   |
|    Rx Total Invalid Frames               | 0                            |
|       Invalid Message Overflow           | 0                            |
|       Invalid Port Status TLV            | 0                            |
|       Invalid Interface Status TLV       | 0                            |
|       Invalid Sender ID TLV              | 0                            |
+------------------------------------------+------------------------------+
| CCM Stats                                |                              |
|    Total Tx                              | 2937268                      |
|    Total Rx Valid                        | 5565942                      |
|    Total Rx In Sequence                  | 5565805                      |
|    Total Rx Sequence Errors              | 18                           |
|    Total Rx MD Level Xcon                | 0                            |
|    Total Rx MAID Xcon                    | 0                            |
|    Total Rx MEPID Error                  | 119                          |
|    Total Rx CCM-Interval Error           | 0                            |
|    Total Rx Invalid                      | 0                            |
+------------------------------------------+------------------------------+
```


Copyright© 2022 Ciena® Corporation

```
| Linktrace Stats                          |                                  |
|    Total Tx LTM                          | 0                                |
|    Total Tx LTR                          | 0                                |
|    Total Rx Valid LTR                    | 0                                |
|    Total Rx Unexpected LTR               | 0                                |
|    Total Rx Invalid LTR                  | 0                                |
|          Rx Invalid Relay Action LTR     | 0                                |
|    Total Rx Valid LTM                    | 0                                |
|    Total Rx Invalid LTM                  | 0                                |
+------------------------------------------+----------------------------------+
| Loopback Stats                           |                                  |
|    Total Tx LBM                          | 0                                |
|    Total Tx LBR                          | 0                                |
|    Total Rx In-order LBR                 | 0                                |
|    Total Rx Out-of-order LBR             | 0                                |
|    Total Rx Content Mismatch LBR         | 0                                |
|    Total Rx Unexpected LBR               | 0                                |
|    Total Rx Invalid LBR                  | 0                                |
|    Total Rx Valid LBM                    | 0                                |
|    Total Rx Invalid LBM                  | 0                                |
+------------------------------------------+----------------------------------+
| Delay Stats                              |                                  |
|    Total Tx DMM                          | 2635680614                       |
|    Total Tx DMR                          | 100                              |
|    Total Rx Valid DMM                    | 100                              |
|    Total Rx Invalid DMM                  | 0                                |
|    Total Rx Valid DMR                    | 2634506678                       |
|    Total Rx Invalid DMR                  | 0                                |
|    Total Rx Unexpected DMR               | 0                                |
+------------------------------------------+----------------------------------+
| Loss Stats                               |                                  |
|    Total Tx LMM                          | 0                                |
|    Total Tx LMR                          | 0                                |
|    Total Rx Valid LMM                    | 0                                |
|    Total Rx Invalid LMM                  | 0                                |
|    Total Rx Valid LMR                    | 0                                |
|    Total Rx Invalid LMR                  | 0                                |
+------------------------------------------+----------------------------------+
| Synthetic Loss Stats                     |                                  |
|    Total Tx SLM                          | 2909847045                       |
|    Total Tx SLR                          | 0                                |
|    Total Rx Valid SLM                    | 0                                |
|    Total Rx Invalid SLM                  | 0                                |
|    Total Rx Valid SLR                    | 2908293544                       |
|    Total Rx Invalid SLR                  | 0                                |
+------------------------------------------+----------------------------------+
| CSF Stats                                |                                  |
|    Total Tx CSF                          | 0                                |
|    Total Tx Los CSF                      | 0                                |
|    Total Tx Dci CSF                      | 0                                |
|    Total Rx Valid CSF                    | 0                                |
|    Total Rx Invalid CSF                  | 0                                |
|    Total Rx Los CSF                      | 0                                |
|    Total Rx Dci CSF                      | 0                                |
+------------------------------------------+----------------------------------+
```

The following example clears global CFM statistics.

```
cfm clear statistics
```


Copyright© 2022 Ciena® Corporation

The following example clears CFM statistics for all services.

```
cfm service clear statistics
```

The following example clears CFM statistics for a specific service.

```
cfm service clear service v1100 statistics
```

The following example clears CFM statistics for all MEPs.

```
cfm mep clear statistics
```

The following example clears CFM statistics for a specific MEP.

```
cfm mep clear service v1100 port 5 statistics
```

The following example clears CFM statistics for all remote MEPs.

```
cfm remote-mep clear statistics
```

The following example clears CFM statistics for a specific remote MEP.

```
cfm remote-mep clear service v1100 mep-id 600 statistics
```

The following example clears all delay measurement statistics.

```
cfm delay clear
```

The following example clears all loss measurement statistics.

```
cfm frame-loss clear
```


Copyright© 2022 Ciena® Corporation

Procedure 2-33
Displaying CFM port stack information

CFM port stack information includes the MEPs and MIPs present in each interface, along with the service associated with each MEP.

Step	Action

1 Display CFM port stack information:

```
cfm stack show [vlan <VlanId>] [order-by-interface]
```

where

vlan <VlanId>	is the VLAN.
order-by-interface	orders results by interface.

—end—

Example

The following example shows sample output for the cfm stack show command.

```
> cfm stack show

+-------------------------- CFM Interface Stacks -------------------------+
|Service Inst|Vlan|Port    |Type|L|Mep |Adm|Service    |MAC Address      |
+------------+----+--------+----+-+----+---+-----------+-----------------+
|VLAN#1001    1001 1       |Down|3|1   |en |VLAN#1001  |00:02:A1:24:0E:32|
+------------+----+--------+----+-+----+---+-----------+-----------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-34
Configuring a VLAN CFM service

Configure a VLAN CFM service.

Note: Steps 1 through 2 are for configuring the VLAN and are not specific to CFM.

Step	Action
1	Create the VLAN: `vlan create`
2	Add the ports to the VLAN: `vlan add`

3	Configure MD settings. (Optional)
	`cfm md create`
	`cfm md set`

4	Create the CFM service `cfm service create`
5	Create a down MEP for the network facing port. `cfm mep create`
6	Enable CFM globally. `cfm enable`
7	Enable the CFM service `cfm service enable`

—end—

Example

This configuration example shows how to configure CFM to monitor connectivity between the two CE devices by configuring a VLAN CFM service.

Configure CFM on CE1.

```
vlan create vlan 10
vlan add vlan 10 port 1
cfm service create vlan 10 name CFM_VLAN_10 level 5
cfm md set level 5 name Customer
cfm mep create service CFM_VLAN_10 port 1 type down mepid 1
cfm enable
cfm service enable service CFM_VLAN_10
```

Configure CFM on CE2.

Copyright© 2022 Ciena® Corporation

```
vlan create vlan 10
vlan add vlan 10 port 10
cfm service create vlan 10 name CFM_VLAN_10 level 5
cfm md set level 5 name Customer
cfm mep create service CFM_VLAN_10 port 10 type down mepid 2
cfm enable
cfm service enable service CFM_VLAN_10
```

Same Forwarding Domain Example

You can configure the same level services on the same forwarding domain if you use a unique VLAN/MEPID for each, where the VLAN must be unique per MEP. For example:

```
vlan create vlan 103
vlan add vlan 103 port 1
cfm service create vlan 103 name s103-c30-4 level 4 next-mepid 7401
cfm mep create service s103-c30-4 port 1 vlan 30 type up mepid 7400
cfm service create vlan 103 name s103-c1050-4 level 4 next-mepid 7406
cfm mep create service s103-c1050-4 port 1 vlan 1050 type up mepid 7405
```

MAID Configuration Example

The following commands demonstrate configuring two CFM services at the same MD level with their MD names set to unique service identifiers, but their short MA names set to a common service type designator. This configuration requires each CFM service to belong to a different MD so that its MAID can contain a unique MD name. The *ma-name-string* parameter is used to specify a short MA name string during CFM service creation. The resulting MAIDs are also shown.

```
vlan create vlan 20
vlan add vlan 20 port 1
cfm md create level 4 name VPLS:30203-4
cfm service create vlan 20 name VPLS:30203-4 md VPLS:30203-4 ma-name diag

Maintenance Domain Name Format:  4  (Character string)
Maintenance Domain Name Length:  12
Maintenance Domain Name:  VPLS:30203-4
Short MA Name Format:  2  (Character string)
Short MA Name Length:   4
Short MA Name   diag

> cfm md create level 4 name VPLS:30303-4
> cfm service create vlan 30 name VPLS:30303-4 md VPLS:30303-4 ma-name diag

Maintenance Domain Name Format:  4  (Character string)
Maintenance Domain Name Length:  12
Maintenance Domain Name:  VPLS:30303-4
Short MA Name Format:  2  (Character string)
Short MA Name Length:   4
Short MA Name   diag
```


Copyright© 2022 Ciena® Corporation

Procedure 2-35
Configuring CFM services for a virtual switch service

Configure CFM service for a virtual switch service.

Step	Action

1 Create the CFM service:

```
cfm service create vs <vs> [accelerate][default-mep-type
<up|down>][level <NUMBER: 0-7>]ma-name-format <icc-based
| integer | string | vid | vpnid> ma-name-integer <NUMBER:
0-65535> ma-name-string <String[45]> ma-name-vid <VLAN
ID> ma-name-vpn-oui <Organization Unique Identifier> ma-
name-vpn-index <NUMBER> md <CFM MD Name> [name
<String[43]>] [next-mepid <NUMBER:1 - 8191>]
```

where

vs <vs>	is the virtual switch service.
accelerate	identifies the service as a hardware-assisted service.
default-mep-type <up | down>	is the default type for MEPs.
level <NUMBER: 0-7>	is the maintenance domain level . The default value for level is 3.
ma-name-format <icc-based | integer | string | vid | vpnid>	is the short MA name format.
ma-name-integer <NUMBER: 0-65535>	is a 2-octet integer for short MA name.
ma-name-string <String[45]>	is a short MA name character string.
ma-name-vid <VLAN ID>	is a short MA Name Primary VID.
ma-name-vpn-oui <Organization Unique Identifier>	is a short MA Name VPN OUI.
ma-name-vpn-index <NUMBER>	is a short MA Name VPN Index.

Copyright© 2022 Ciena® Corporation

where

md <CFM MD Name>	is the maintenance domain.
name <String[31]>	is the service name. If unspecified, the new CFM service has the same name as its VLAN or VS.
next-mepid <NUMBER:1 - 8191>	is the next mep ID.The default value for next-mepid is 1. Note that since next-mepid is used to generate default ME-PIDs, it is important to set it to a unique value on each device in the service instance.

2 Enable CFM globally:

```
cfm enable
```

3 Enable the CFM service.

```
cfm service <service> enable
```

where

service <service>	is the CFM service name.

—end—

Example

The following example configures CFM for a virtual switch VS-1

```
cfm service create vs VS-1 name CFM_VS_1
cfm enable
cfm service enable service CFM_VS_1
```


Copyright© 2022 Ciena® Corporation

Procedure 2-36
Configuring CFM over MPLS

Configure CFM over MPLS.

Note the following limitations:

- CFM over MPLS is not intended to directly monitor underlying LSPs or trigger MPLS tunnel failover.
- Virtual circuit MEPs of type down are not supported.
- MIPs are not supported on either attachment circuit or virtual circuit interfaces.
- Specifying the vlan parameter is optional when creating a MEP of type up on a tagged attachment circuit member port.
  - The commands cfm mep create service <s> port <p> vlan <v> and cfm mep create service <s> port <p> are equivalent.
  - If the vlan parameter is specified, it must match the member vlan.
  - It is not possible or necessary to create a Q-in-Q style port-based AC MEP when a MEP has already been created using port/vlan.
- CFM over MPLS services cannot be accelerated, that is, made hardware-based, due to lack of support for MEPs of type up.

  Note 1: MEP tag-mode can be used to push an additional tag on originated frames.

  Note 2: Steps 1 through 15 are for configuring MPLS and are not specific to CFM.

Step	Action

1 Create a loopback interface:

```
interface create loopback <loopback> {ip <IP address>}
```

where

loopback <loopback>	loopback interface name
ip <IP address>	interface IP address

Copyright© 2022 Ciena® Corporation

2 Create an interface with ip forwarding on:

```
interface create ip-interface <ip-interface> ip {ip <IP
addressWithMask>} vlan <VLAN> ip-forwarding on
```

where

ip-interface <ip-interface>	is the interface name.
ip {ip <IP addressWith Mask>}	is the IP address in CIDR notation.
vlan <VLAN>	is the interface VLAN.
ip-forwarding	is the setting for interface IP forwarding

3 Add a port to the VLAN:

```
vlan add vlan <VLAN> port <PortList>
```

where

vlan <VLAN>	is the VLAN list to add ports.
port <PortList>	is the list of ports to add to VLAN.

4 Create an ethernet virtual switch with mode vpls:

```
virtual-switch ethernet create vs <String[31]> mode vpls
```

where

vs <String[31]>	is the virtual switch name.
mode	is the capability of virtual-switch.

5 Attach the loopback interface to the OSPF instance:

```
ospf interface attach ip-interface <ip-interface> {area
<IP address>} {ospf-instance <OSPF Instance>}
```

where

ip-interface <ip-interface>	is the loopback interface name.
{area <IP address>}	is the OSPF area.
{ospf-instance <OSPF Instance>}	is the OSPF instance name.

Copyright© 2022 Ciena® Corporation

6 Attach the ip interface to the OSPF instance:

```
ospf interface attach ip-interface <ip-interface> {area
<IP address>} {ospf-instance <OSPF Instance>}
```

where

ip-interface <ip-interface>	is the ip interface name.
{area <IP address>}	is the OSPF area.
{ospf-instance <OSPF Instance>}	is the OSPF instance name.

7 Enable RSVP on the loopback interface:

```
rsvp-te enable ip-interface <ip-interface>
```

where

ip-interface <ip-interface>	is the loopback interface name.

8 Enable RSVP on the ip interface:

```
rsvp-te enable ip-interface <ip-interface>
```

where

ip-interface <ip-interface>	is the ip interface name.

9 Create an RSVP path:

```
rsvp-te path create rsvp-path <rsvp-path>
```

where

rsvp-path <rsvp-path>	is the RSVP path to create.

10 Set the RSVP path:

```
rsvp-te path set rsvp-path <rsvp-path> {index <NUMBER: 1-
16>} {ip <IP address>}
```

where

rsvp-path <rsvp-path>	add path
index <NUMBER: 1-16>	is the position of node in the rsvp path list.
ip <IP address>	is the IP address.

Copyright© 2022 Ciena® Corporation

11 Create an encapsulation tunnel:

```
mpls tunnel create rsvp-ingress <rsvp-ingress> [path
<MPLS Rsvp Path>] {dest-ip <IP address>}
```

where

rsvp-ingress <rsvp-ingress>	is the RSVP tunnel name.
[path <MPLS Rsvp Path>]	is the RSVP path name.
{dest-ip <IP address>}	is the tunnel destination IP address.

12 Enable the LDP protocol:

```
ldp enable
```

13 Create LDP signaled virtual circuit:

```
mpls l2-vpn create dynamic-vc <dynamic-vc> {pw-id
<NUMBER: 1-2147483647>} {peer <IP address>} {tunnel <MPLS
ingress primary tunnel>} pw-mode <mesh | spoke>] [pw-type
<eth-raw | eth-tagged>]
```

where

dynamic-vc <dynamic-vc>	is the dynamic virtual-circuit name.
{pw-id <NUMBER: 1-2147483647>}	is the VPN ID.
{peer <IP address>}	is the destination IP address.
{tunnel <MPLS ingress primary tunnel>}	is the transport tunnel.
pw-mode <mesh | spoke>]	is the pseudowire mode.
[pw-type <eth-raw | eth-tagged>]	is the pseudowire type.

Copyright© 2022 Ciena® Corporation

14 Add subscriber members to virtual switch:

```
virtual-switch ethernet add vs <vs> {port <PortList>}
{vlan <VLAN list>} {ip-interface <interface-name>}
{encap-cos-policy <fixed | port-inherit | vs-inherit>}
{encap-fixed-dot1dpri <NUMBER: 0-7>} [statistics <on |
off>] [translate-tag <NUMBER: 0-4094>]
```

where

vs <vs>	is the virtual switch name.
port <PortList>	is the subscriber port list.
vlan <VLAN>	is the subscriber VLAN id.
ip-interface <interface-name>	is the name of the IP interface.
encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.

15 Attach members to an MPLS capable virtual switch:

```
virtual-switch ethernet attach mpls-vc <mpls-vc> vs <vs>
```

where

mpls-vc <mpls-vc>	is the list of mpls-vcs.
vs <vs>	is the virtual switch name.

Copyright© 2022 Ciena® Corporation

Create CFM service and up MEPs

16 Create a CFM service:

```
cfm service create vs <vs> name <String[45]>
```

where

vs <vs>	is the virtual switch.
name <String[45]>	is the CFM service name.

17 Enable the CFM service:

```
cfm service enable service <service>
```

where

service <service>	is the service name.

18 Create MEP:

```
cfm mep create service <service> port <port> vlan <VLAN>
type up mepid <NUMBER: 1-8191>
```

where

service <service>	is the service name.
port <port>	is the service port.
vlan <VLAN>	is the vlan.
mepid <NUMBER: 1-8191>	is the MEP identifier.

19 Create additional MEP:

```
cfm mep create service <service> port <port> type up mepid
<NUMBER: 1-8191>
```

where

service <service>	is the service name.
port <port>	is the service port.
mepid <NUMBER: 1-8191>	is the MEP identifier.

—end—

Example

The following example configures an MPLS VS with AC and VC attachments.

```
interface create loopback LBK ip 10.10.10.2
interface create ip-interface ip1 ip 11.1.1.2/24 vlan 20 ip-forwarding on
vlan add vlan 20 port 6
virtual-switch ethernet create vs vpls1 mode vpls
ospf interface attach ip-interface LBK area 0.0.0.0 ospf-instance ospf-inst
ospf interface attach ip-interface ip1 area 0.0.0.0 ospf-instance ospf-inst
```


Copyright© 2022 Ciena® Corporation

```
rsvp-te enable ip-interface LBK
rsvp-te enable ip-interface ip1
rsvp-te path create rsvp-path path
rsvp-te path set rsvp-path path1 index 1 ip 11.1.1.1
mpls tunnel create rsvp-ingress tun1 path path1 dest-ip 10.10.10.1
ldp enable
mpls l2-vpn create dynamic-vc vc1 pw-id 100 peer 10.10.10.1 tunnel tun1 pw-
mode spoke pw-type eth-tagged
virtual-switch ethernet add vs vpls1 port 1 vlan 999
virtual-switch ethernet attach mpls-vc vc1 vs vpls1
cfm service create vs vpls1 name mpls
cfm service enable service mpls
cfm mep create service mpls port 1 vlan 999 type up mepid 9
cfm mep create service mpls port 4 type up mepid 8
```


Copyright© 2022 Ciena® Corporation

Procedure 2-37
Displaying SLM frame loss test results

Display SLM frame loss test results.

Step	Action

1 Display synthetic frame loss test results:

```
cfm synthetic-loss show <mep-object> [mepid <remote-
mepid>] [test-id <SLM-test-id>] [history]
```

where

mep-object	is one of: • service local-mepid • service port • service port vlan
mepid <remote-mepid>	is the remote MEP ID.
test-id <SLM-test-id>	is the test ID.
history	is history.

Copyright© 2022 Ciena® Corporation

Procedure 2-38
Configuring a MEF 35 compliant delay session

Configure a MEF 35 compliant delay session.

Step	Action

1 Create a MEF 35 compliant delay session.

```
cfm mef delay create {service <service>}{local-mepid
<NUMBER: 1-8191>}{remote-mepid <NUMBER: 1-8191>| mac
<remote-mac-address>}[session-type <on-demand|
proactive>][test-id <NUMBER: 1-4294967295>][message-
interval
<3.33ms|10ms|100ms|1sec|10sec|1min|10min>][measurement-
interval <MINUTES: 1..1440>][priority <NUMBER: 0-7>]
[repetition-time <MINUTES: 0..43200>] [start-now] [start-
at-time <time: hh:mm:ss or hh:mm>] [start-at-date <date:
yyyy-mm-dd or mm-dd>] [start-after <duration: {N
[yMwdhms]}] [stop-none] [stop-at-time <time: hh:mm:ss>]
[stop-at-date <date: yyyy-mm-dd>] [stop-after <duration:
{N[yMwdhms]}][accelerate] [align-measurement-
interval[align-measurement- offset <MINUTES:
0..60>][stored-interval-count <NUMBER: 2..96>] [frame-
size <NUMBER: 140..2000>] [delay-bins <profile-name>]
[delay-range-bins <profile-name>][ifdv-bins <profile-
name>][forward-ifdv-bins <profile-name>][backward-ifdv-
bins <profile-name>][cos-mode]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the mepid of the local-mep.
remote-mepid <NUMBER: 1-8191> | mac <remote-mac-address>	is the mepid of the remote-mep or the MAC address of the remote-mep.
session-type <on-demand | proactive	is the delay session type. The default is proactive.
test-id <NUMBER: 1-4294967295>	is the test ID to identify the session between a local and remote MEP pair. If this value is not specified, it will be equal to the session ID.

Copyright© 2022 Ciena® Corporation

where

message-interval <3.3ms|10ms|100ms|1sec|10sec|1min|10min>	is the DMM message priority. The default is 7.
measurement-interval <MINUTES: 1..1440>]	is the amount of time in minutes that the test iteration should run. The default is 15 min (proactive), 5min (on-demand).
priority <NUMBER: 0-7>]	is the DMM message priority. The default is 7.
repetition-time <MINUTES: 0..43200>	is the time in minutes between the start of the first measurement interval and the start of the next measurement interval.
start-now	starts the session immediately.
start-at-time <time: hh:mm:ss 0r hh:mm>	is fixed mode, meaning that the session is started at the input time.
start-at-date <date: yyyy-mm-dd or mm-dd>	is fixed mode, meaning that it starts the session at the input date.
start-after <duration: {N [yMwdhms]}	is relative mode, meaning the session starts at the input time from now.
stop-none	the session runs forever.
stop-at-time <time: hh:mm:ss>	is fixed mode, meaning that the session stops at the input time.
stop-at-date <date: yyyy-mm-dd>	is fixed mode, meaning the session stops at the input date.
stop-after <duration: {N[yMwdhms]}>	is relative mode, meaning the session stops at the input time from start time.
accelerate	selects the system to offload the MEF session to enhance the scale of Y.1731 sessions. Whenever accelerated sessions are created, corresponding accelerated responders should be created at the far end. ***Note:*** On the 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved to use the accelerate option.
align-measurement-interval	aligns the session with a zero offset to real time. The default is false, meaning the test session will not be aligned.

Copyright© 2022 Ciena® Corporation

where

align-measurement-offset <MINUTES: 0..60>	is the offset in minutes from the time of day value. The default is false, meaning the test session will not be aligned.
stored-interval-count <NUMBER: 2..96>	is the number of completed measurement intervals to be stored in the history statistics table. The default is 32.
frame-size <NUMBER: 140..2000>	is the base CFM frame size. If the 0 value is specified, it denotes the default frame size for that test session. The frame size does not account for any tags.
delay-bins <profile-name>	is the delay-bins profile name.
delay-range-bins <profile-name>	is the delay-range profile name.
ifdv-bins <profile-name>	is the jitter profile name.
forward-ifdv-bins <profile-name>	is the jitter profile name for forward direction.
backward-ifdv-bins <profile-name>	is the jitter profile name for backward direction.
cos-mode	is the substitute DMR p-bits for test-id when the TestID TLV is missing.

—end—

Examples

The following example creates a delay measurement service with a proactive session:

```
> cfm mef delay create service serv1 session-type proactive local-mepid 2
remote-mepid 1 start-now stop-none
```

The following example creates a delay measurement service with an on-demand session with fixed start and stop times:

```
> cfm mef delay create service serv2 session-type local-mepid 3 remote-mepid
2 session-type on-demand start-at-time 10:50:45 start-at-date 2017-03-14
stop-at-time 15:20:50 stop-at-date 2017-04-15
```

The following example creates a delay measurement service with an on-demand session with relative start and stop times.

```
> cfm mef delay create service serv3 session-type local-mepid 3 remote-mepid
2 session-type on-demand start-after 09:45:30 stop-after 18:35:45
```


Copyright© 2022 Ciena® Corporation

Procedure 2-39
Configuring a MEF 35 compliant synthetic loss measurement session

Configure a MEF 35 compliant synthetic loss measurement session.

Step	Action

1 Create a MEF 35 compliant synthetic loss measurement session:

```
cfm mef synthetic-loss create {service <service>}{local-
mepid <NUMBER: 1-8191>}{remote-mepid <NUMBER:1-8191> |
mac <remote-mac-address>}[session-type <on-demand |
proactive>][test-id <NUMBER: 1-4294967295>][message-
interval <3.33ms|10ms|100ms|1sec|10sec|1min|10min>]
[priority <NUMBER: 0-7>][measurement-interval <MINUTES:
1..43200>] [repetition-time <MINUTES: 0..43200>][start-
now] [start-at-time <time: hh:mm:ss or hh:mm>] [start-at-
date <date: yyyy-mm-dd or mm-dd>] [start-after <duration:
{N [yMwdhms]}] [stop-after <duration: {N[yMwdhms]}]
[stop-none] [stop-at-time <time: hh:mm:ss>] [stop-at-date
<date: yyyy-mm-dd>] [accelerate][align-measurement-
interval[align-measurement-offset <MINUTES: 0..1440>]
[stored-interval-count <NUMBER: 2..96>][frame-size
<NUMBER:64..2000>][avail-measurement-interval <MINUTES:
1..43200>][avail-consecutive-pdu-count <NUMBER:
10..1000000>][avail-flr-threshold <MILLIPERCENT:
0..100000>] [avail-consecutive-intervals <NUMBER:
1..1000>] [avail-consecutive-high-flr <NUMBER: 1..1000>]
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the mepid of the local-mep.
remote-mepid <NUMBER: 1-8191> | mac <remote-mac-address>	is the mepid of the remote-mep or the MAC address of the remote-mep.
session-type <on-demand | proactive	is the delay session type. The default is proactive.
test-id <NUMBER: 1-4294967295>	is the test ID to identify the session between a local and remote MEP pair. If this value is not specified, it will be equal to the session ID.

Copyright© 2022 Ciena® Corporation

where

message-interval <3.33ms | 10ms | 100ms | 1sec | 10sec | 1min | 10min>	is the DMM transmission interval time. The default is 100 milliseconds.
priority <NUMBER: 0-7>	is the DM message priority. The default is 7.
measurement-interval <MINUTES: 1..525600>	is the amount of time, in minutes, that the test iteration should run. The default is 15min (proactive, 5min(on-demand).
repetition-time <MINUTES: 0..43200>]	is the time, in minutes, between the start of the first measurement interval and the start of the next measurement interval.
start-now	starts the session immediately.
start-at-time <time: hh:mm:ss or hh:mm>	is fixed mode, meaning that the session is started at the input time.
start-at-date <date: yyyy-mm-dd or mm-dd>	is fixed mode, meaning that it starts the session at the input date.
start-after <duration: {N [yMwdhms]}	is relative mode, meaning the session starts at the input time from now.
[stop-after <duration: {N[yMwdhms]}>]	is relative mode, meaning the session stops at the input time from start time.
stop-none	the session runs forever.
stop-at-time <time: hh:mm:ss>	is fixed mode, meaning that the session stops at the input time.
stop-at-date <date: yyyy-mm-dd>	is fixed mode, meaning the session stops at the input date.
accelerate	selects the system to offload the MEF session to enhance the scale of Y.1731 sessions. ***Note:*** ON the 3924, 3926 and 3928 platforms, the enhanced CFM port needs to be reserved to use the accelerate option.
align-measurement-interval	aligns the session with a zero offset to real time. Whenever accelerated sessions are created, corresponding accelerated responders should be created at the far end.

Copyright© 2022 Ciena® Corporation

where

align-measurement-offset <MINUTES: 0..1440>	is the offset in minutes from the time of day value.
stored-interval-count <NUMBER: 2..96>	is the number of completed measurement intervals to be stored in the history statistics table. The default is 32.
frame-size <NUMBER: 64..2000>	is the base CFM frame size. If the 0 value is specified, it denotes the default frame size for that test session. The frame size does not account for any tags.
avail-measurement-interval <MINUTES: 1..43200>	specifies the availability measurement interval. The default is 15.
avail-consecutive-pdu-count <NUMBER: 10..1000000>	is the number of SLM PDUs transmitted during each delta_t period. The default is 10.
avail-flr-threshold <MILLIPERCENT: 0..100000>	is the threshold, in milli-percent, used in evaluating the availability/unavailability status of each delta_t. The default of 50000.
avail-consecutive-intervals <NUMBER: 1..1000>	is the number of consecutive availability indicators used to determine a change in the availability status. The default is 10.
avail-consecutive-high-flr <NUMBER: 1..1000>	is the number of consecutive availability indicators used for assessing CHLI. The default is 5.

—end—

Examples

The following example creates a synthetic loss service with a proactive session:

```
> cfm mef synthetic-loss create service serv1 session-type proactive local-
mepid 2 remote-mepid 1 start-now stop-none
```

The following example creates a synthetic loss service with an on-demand session with fixed start and stop times:

```
> cfm mef synthetic-loss create service serv2 session-type local-mepid 3
remote-mepid 2 session-type on-demand start-at-time 10:50:45 start-at-date
2017-03-14 stop-at-time 15:20:50 stop-at-date 2017-04-15
```


Copyright© 2022 Ciena® Corporation

The following example creates a synthetic loss service with an on-demand session with relative start and stop times.

```
> cfm mef synthetic-loss create service serv3 session-type local-mepid 3
remote-mepid 2 session-type on-demand start-after 09:45:30 stop-after
18:35:45
```


Copyright© 2022 Ciena® Corporation

Procedure 2-40
Deleting a MEF 35 compliant delay session

Delete a MEF 35 compliant delay session.

Step	Action
1	Delete the MEF 35 compliant delay measurement session: `cfm mef delay delete service <service> {local-mepid <NUMBER: 1-8191>} {session-id <NUMBER: 1-4294967295>}` where service <service> is the CFM service name. local-mepid <NUMBER: 1-8191> is the mepid of the local-mep. session-id <NUMBER: 1-4294967295> is the session-id number

—end—

Example

The following example deletes a delay measurement session:

```
> cfm mef delay service serv1 local-mepid 2 session-id 55000
```


Copyright© 2022 Ciena® Corporation

Procedure 2-41
Deleting a MEF 35 compliant synthetic loss measurement session

Delete a MEF 35 compliant synthetic loss measurement session.

Step	Action
1	Delete the MEF 35 compliant synthetic loss measurement session: `cfm mef synthetic-loss delete service <service> {local-mepid <NUMBER: 1-8191>} {session-id <NUMBER: 1-4294967295>}` where service <service> is the CFM service name. local-mepid <NUMBER: 1-8191> is the mepid of the local-mep. session-id <NUMBER: 1-4294967295> is the session-id number

—end—

Example

The following example deletes a synthetic loss measurement session:

```
> cfm mef synthetic-loss service serv1 local-mepid 2 session-id 55000
```


Copyright© 2022 Ciena® Corporation

Procedure 2-42
Disabling a MEF 35 compliant delay measurement session

Disable a MEF 35 compliant delay measurement session.

Note: Enable operation is not currently supported for synthetic loss measurement and delay measurement sessions.

Step	Action
1	Disable the MEF 35 compliant delay measurement session: `cfm mef delay disable service <service> {local-mepid <NUMBER: 1-8191>} {session-id <NUMBER: 1-4294967295>}` where service <service> is the CFM service name. local-mepid <NUMBER: 1-8191> is the mepid of the local-mep. session-id <NUMBER: 1-4294967295> is the session-id number.

—end—

Example

The following example disables a delay measurement session:

```
> cfm mef delay disable service serv1 local-mepid 2 session-id 55000
```


Copyright© 2022 Ciena® Corporation

Procedure 2-43
Disabling a MEF 35 compliant synthetic loss measurement session

Disable a MEF 35 compliant synthetic loss measurement session.

Note: Enable operation is not currently supported for synthetic loss measurement and delay measurement sessions.

Step	Action
1	Disable the MEF 35 compliant synthetic loss measurement session: `cfm mef synthetic-loss disable service <service> {local-mepid <NUMBER: 1-8191>} {session-id ,NUMBER: 1-4294967295>}` where service <service> is the CFM service name. local-mepid <NUMBER: 1-8191> is the mepid of the local-mep. session-id <NUMBER: 1-4294967295> is the session-id number

—end—

Example

The following example disables a synthetic loss measurement session:

```
> cfm mef synthetic-loss disable service serv1 local-mepid 2 session-id 55000
```


Copyright© 2022 Ciena® Corporation

Procedure 2-44
Configuring a MEF 35 compliant frame delay range

A frame delay range is a delay measurement key performance indicator (KPI).

Step	Action
1	Configure a frame delay range binning profile: `cfm profile bins create delay-range <Name (no !%, ?*) String[1..45]>` where delay-range <Name (no !%,?*) String[1..45] — is the delay range profile. **—end—**

Copyright© 2022 Ciena® Corporation

Procedure 2-45
Configuring a MEF 35 frame delay range bins lower threshold

Configure a MEF 35 frame delay range bins lower threshold.

Configure a MEF 35 frame delay range lower threshold

1 Configure a MEF 35 frame delay range bins lower threshold:

```
cfm profile bins set delay-range <profile-name> bin-index
<NUMBER: 1..10> threshold <NUMBER: 0..2147483674>
```

where

delay-range <profile-name>	is the delay profile name.
bin-index <NUMBER: 1..10>	is the bin-index number.
threshold <NUMBER: 0..2147483674>	is the lower threshold.

Return a MEF 35 frame delay range lower threshold to default values

2 Return a MEF 35 frame delay range lower threshold to default values:

```
cfm profile bins unset delay-range <profile-name> bin-
index <NUMBER>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-46
Deleting a MEF 35 frame delay range binning profile

Delete a MEF 35 frame delay range binning profile.

1 Delete a MEF 35 frame delay range binning profile:

```
cfm profile bins delete delay-range <profile-name>
```

where

delay-range <profile-name>	is the delay-range profile name.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 2-47
Displaying MEF 35 delay measurement information

Display the following MEF 35 delay measurement information:

- current measurement interval of all sessions
- delay measurement current statistics for a specific session
- all bins of the current measurement-interval for delay measurement sessions
- all bins of the current measurement-interval for delay measurement sessions
- history statistics of a specified delay measurement session

Step	Action

To display the current measurement interval of all sessions

1 Display the current measurement interval of all the sessions:

```
cfm mef delay show
```

To display delay measurement current statistics for a specific session

2 Display the delay measurement current statistics for a specific session:

```
cfm mef delay show service <service> {local-mepid
<NUMBER: 1-8191>} {session-id ,NUMBER: 1-4294967295>}
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the mepid of the local-mep.
session-id <NUMBER: 1-4294967295>	is the session-id number

To display all bins of the current measurement-interval for delay measurement sessions

3 Display all bins of the current measurement-interval for delay measurement sessions:

```
cfm mef delay show bins
```

To display all bins of the current measurement-interval for delay measurement sessions

4 Display bins of a current measurement-interval of a specific delay measurement session:

```
cfm mef delay show service <service> local-mepid <mepid>
session-id <index> bins
```


Copyright© 2022 Ciena® Corporation

To display history statistics of a specific delay measurement session

5 Display display history statistics of a specific delay measurement session:

```
cfm mef delay show service <service> local-mepid <mepid>
session=id <index> history
```

—end—

Examples

The following example shows output for the cfm mef delay show command.

```
> cfm mef delay show

+-------------- MEP DELAY SESSION MEASUREMENT INTERVAL INFO --------------+
| Service                | cfm201                                         |
| Local Mepid            | 107                                            |
| Remote Mepid           | 98                                             |
| Test-Id                | 1                                              |
| Session-Id             | 1                                              |
| Active                 | Yes                                            |
+------------------------+------------------------------------------------+
+---------------------------- Measured Stats -----------------------------+
| Stats           | Two-Way(us)     | Forward(us)     | Backward(us)       |
+-----------------+-----------------+-----------------+--------------------+
| Frame Delay     | 7               | N/A             | N/A                |
| IFDV            | 0               | 1               | 1                  |
+-----------------+-----------------+-----------------+--------------------+
+------------------------ Measurement Interval --------------------------+
| Interval-Index         | 67                                            |
| Start Time(date/time)  | 01/02/2000 14:56:05                           |
| Elapsed Time (ms)      | 308048                                        |
| Pdu Sent               | 3071                                          |
| Pdu Received           | 3071                                          |
| Suspect                | No                                            |
+------------------------+------------------------------------------------+
+------------------------------ Statistics -------------------------------+
| Stats    | Frame Delay(us)  | IFDV(us)           | Frame Delay Range(us)  |
+----------+------------------+--------------------+------------------------+
| Two-way  |                  |                    |                        |
|     Min: | 5                | 0                  | 0                      |
|     Avg: | 6                | 0                  | 1                      |
|     Max: | 8                | 3                  | 3                      |
| Forward  |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 0                  | N/A                    |
|     Max: | N/A              | 2                  | N/A                    |
| Backward |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 0                  | N/A                    |
|     Max: | N/A              | 2                  | N/A                    |
+----------+------------------+--------------------+------------------------+
```

The following example shows output for a specific session (to be identified using service, lmepid and session ID).

```
> cfm mef delay show service cfm201 local-mepid 107 session-id 1
```


Copyright© 2022 Ciena® Corporation

```
+-------------- MEP DELAY SESSION MEASUREMENT INTERVAL INFO --------------+
| Service                | cfm201                                        |
| Local Mepid            | 107                                           |
| Remote Mepid           | 98                                            |
| Test-Id                | 1                                             |
| Session-Id             | 1                                             |
| Active                 | Yes                                           |
+------------------------+-----------------------------------------------+
+-------------------------- SESSION PARAMETERS ---------------------------+
| Admin State            | Enabled                                       |
| Session Type           | Proactive                                     |
| Start Type             | Immediate                                     |
| Stop Type              | None                                          |
| Start Time(date/time)  | 01/01/2000 22:26:02                           |
| Stop Time(date/time)   | N/A                                           |
| Meas Interval(min)     | 15                                            |
| Repetition Time(sec)   | 0                                             |
| Remote Mac             | 9C:7A:03:05:1D:F4                             |
| Source Mac             | 2C:39:C1:2A:B7:04                             |
| Message Period         | 100ms                                         |
| Priority               | 7                                             |
| Frame Size             | 64                                            |
| History Size           | 32                                            |
| Align-Meas Intervals   | No                                            |
| Align-Meas Offset(min) | 0                                             |
| CosMode                | No                                            |
| Delay Profile          | Default-Delay-Profile-Name                    |
| Delay Range Profile    | Default-Delay-Range-Profile-Name              |
| Two-way IFDV Profile   | Default-Jitter-Profile-Name                   |
| Forward IFDV Profile   | Default-Jitter-Profile-Name                   |
| Backward IFDV Profile  | Default-Jitter-Profile-Name                   |
+------------------------+-----------------------------------------------+
+---------------------------- Measured Stats -----------------------------+
| Stats           | Two-Way(us)     | Forward(us)     | Backward(us)       |
+-----------------+-----------------+-----------------+--------------------+
| Frame Delay     | 7               | N/A             | N/A                |
| IFDV            | 1               | 1               | 2                  |
+-----------------+-----------------+-----------------+--------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 67                                           |
| Start Time(date/time)  | 01/02/2000 14:56:05                          |
| Elapsed Time (ms)      | 831701                                       |
| Pdu Sent               | 8290                                         |
| Pdu Received           | 8291                                         |
| Suspect                | No                                           |
+------------------------+-----------------------------------------------+
+------------------------------ Statistics -------------------------------+
| Stats    | Frame Delay(us)  | IFDV(us)           | Frame Delay Range(us) |
+----------+------------------+--------------------+-----------------------+
| Two-way  |                  |                    |                       |
|     Min: | 5                | 0                  | 0                     |
|     Avg: | 6                | 0                  | 1                     |
|     Max: | 8                | 3                  | 3                     |
| Forward  |                  |                    |                       |
|     Min: | N/A              | 0                  | N/A                   |
|     Avg: | N/A              | 1                  | N/A                   |
|     Max: | N/A              | 3                  | N/A                   |
| Backward |                  |                    |                       |
|     Min: | N/A              | 0                  | N/A                   |
|     Avg: | N/A              | 1                  | N/A                   |
```


Copyright© 2022 Ciena® Corporation

```
|      Max: | N/A                | 2                   | N/A                       |
+-----------+--------------------+---------------------+---------------------------+
+---------------------------------- Bin Statistics -----------------------------------+
|     |       Two Way Frame Delay Result        |   Two Way Frame Delay Range Result      |
| Bin | Threshold(us)       | Count              | Threshold(us)       | Count             |
+-----+---------------------+--------------------+---------------------+-------------------+
| 0   | 0                   | 8291               | 0                   | 8291              |
| 1   | 5000                | 0                  | 5000                | 0                 |
| 2   | 10000               | 0                  | 10000               | 0                 |
| 3   | 15000               | 0                  |                     |                   |
+-----+---------------------+--------------------+---------------------+-------------------+
|     |   Two Way IFDV Result     |    Forward IFDV Result    |   Backward IFDV Result    |
| Bin |Threshold(us)| Count       |Threshold(us)| Count       |Threshold(us)| Count       |
+-----+-------------+-------------+-------------+-------------+-------------+-------------+
| 0   | 0           | 8290        | 0           | 8290        | 0           | 8290        |
| 1   | 5000        | 0           | 5000        | 0           | 5000        | 0           |
| 2   | 10000       | 0           | 10000       | 0           | 10000       | 0           |
+-----+-------------+-------------+-------------+-------------+-------------+-------------+
```

The following example shows the output from the cfm mef delay show bins command. You can also display bins of the current measurement interval of a specific delay measurement session. The output is the same for both commands shown.

```
> cfm mef delay show bins

> cfm mef delay show service cfm 201 local-mepid 107 session-id 1 bins

+------------------- MEP DELAY MEASUREMENT RESULT BINS --------------------+
| Service                | cfm201                                          |
| Local Mepid            | 107                                             |
| Remote Mepid           | 98                                              |
| Test-Id                | 1                                               |
| Session-Id             | 1                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 68                                              |
| Start Time(date/time)  | 01/02/2000 15:11:05                             |
| Elapsed Time (ms)      | 122932                                          |
| Pdu Sent               | 1225                                            |
| Pdu Received           | 1226                                            |
| Suspect                | No                                              |
+------------------------+-------------------------------------------------+
+---------------------------------- Bin Statistics -----------------------------------+
|     |       Two Way Frame Delay Result        |   Two Way Frame Delay Range Result      |
| Bin | Threshold(us)       | Count              | Threshold(us)       | Count             |
+-----+---------------------+--------------------+---------------------+-------------------+
| 0   | 0                   | 1226               | 0                   | 1226              |
| 1   | 5000                | 0                  | 5000                | 0                 |
| 2   | 10000               | 0                  | 10000               | 0                 |
| 3   | 15000               | 0                  |                     |                   |
+-----+---------------------+--------------------+---------------------+-------------------+
|     |   Two Way IFDV Result     |    Forward IFDV Result    |   Backward IFDV Result    |
| Bin |Threshold(us)| Count       |Threshold(us)| Count       |Threshold(us)| Count       |
+-----+-------------+-------------+-------------+-------------+-------------+-------------+
| 0   | 0           | 1225        | 0           | 1225        | 0           | 1225        |
| 1   | 5000        | 0           | 5000        | 0           | 5000        | 0           |
| 2   | 10000       | 0           | 10000       | 0           | 10000       | 0           |
+-----+-------------+-------------+-------------+-------------+-------------+-------------+
```

The following example shows the output when displaying history statistics of a specific delay measurement session:

```
> cfm mef delay show service cfm201 local-mepid 107 session-id 1 history
```


Copyright© 2022 Ciena® Corporation

```
+----------------- MEP DELAY SESSION MEASUREMENT HISTORY -----------------+
| Service                | cfm201                                        |
| Local Mepid            | 107                                           |
| Remote Mepid           | 98                                            |
| Test-Id                | 1                                             |
| Session-Id             | 1                                             |
| Active                 | Yes                                           |
+------------------------+-----------------------------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 36                                            |
| End Time(date/time)    | 01/02/2000 07:26:05                           |
| Elapsed Time (ms)      | 899998                                        |
| Pdu Sent               | 8972                                          |
| Pdu Received           | 8972                                          |
| Suspect                | No                                            |
+------------------------+-----------------------------------------------+
+----------------------------- Statistics -------------------------------+
| Stats    | Frame Delay(us)  | IFDV(us)           | Frame Delay Range(us)  |
+----------+------------------+--------------------+------------------------+
| Two-way  |                  |                    |                        |
|     Min: | 5                | 0                  | 0                      |
|     Avg: | 6                | 0                  | 1                      |
|     Max: | 8                | 3                  | 3                      |
| Forward  |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 0                  | N/A                    |
|     Max: | N/A              | 2                  | N/A                    |
| Backward |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 0                  | N/A                    |
|     Max: | N/A              | 3                  | N/A                    |
+----------+------------------+--------------------+------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 37                                            |
| End Time(date/time)    | 01/02/2000 07:41:05                           |
| Elapsed Time (ms)      | 900007                                        |
| Pdu Sent               | 8972                                          |
| Pdu Received           | 8972                                          |
| Suspect                | No                                            |
+------------------------+-----------------------------------------------+
+----------------------------- Statistics -------------------------------+
| Stats    | Frame Delay(us)  | IFDV(us)           | Frame Delay Range(us)  |
+----------+------------------+--------------------+------------------------+
| Two-way  |                  |                    |                        |
|     Min: | 5                | 0                  | 0                      |
|     Avg: | 6                | 0                  | 1                      |
|     Max: | 8                | 3                  | 3                      |
| Forward  |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 1                  | N/A                    |
|     Max: | N/A              | 3                  | N/A                    |
| Backward |                  |                    |                        |
|     Min: | N/A              | 0                  | N/A                    |
|     Avg: | N/A              | 1                  | N/A                    |
|     Max: | N/A              | 2                  | N/A                    |
+----------+------------------+--------------------+------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 38                                            |
| End Time(date/time)    | 01/02/2000 07:56:05                           |
```


Copyright© 2022 Ciena® Corporation

Elapsed Time (ms)	899994
Pdu Sent	8972
Pdu Received	8972
Suspect	No

Statistics

Stats	Frame Delay(us)	IFDV(us)	Frame Delay Range(us)
Two-way			
Min:	5	0	0
Avg:	6	0	1
Max:	8	3	3
Forward			
Min:	N/A	0	N/A
Avg:	N/A	1	N/A
Max:	N/A	3	N/A
Backward			
Min:	N/A	0	N/A
Avg:	N/A	1	N/A
Max:	N/A	3	N/A

Copyright© 2022 Ciena® Corporation

Procedure 2-48
Displaying MEF 35 synthetic loss session information

Display the following synthetic loss session information:

- current measurement interval of all synthetic loss sessions
- current measurement interval statistics of a specific synthetic loss session
- history statistics of a specific synthetic-loss measurement
- availability statistics of a specific synthetic-loss measurement session
- history availability statistics of a specific synthetic loss measurement session

Step	Action

To display the current measurement interval of all synthetic loss sessions

1 Display the current measurement interval of all the sessions:

```
cfm mef synthetic-loss show
```

To display the current measurement interval statistics of a specific synthetic loss session

2 Display the current measurement interval of a specific synthetic loss session:

```
cfm mef synthetic-loss show service <service> local-mepid
<mepid> session-id <index>
```

where

service <service>	is the CFM service name.
local-mepid <NUMBER: 1-8191>	is the mepid of the local-mep.
session-id <NUMBER: 1-4294967295>	is the session-id number

To display history statistics of a specific synthetic-loss measurement session

3 Display history statistics of a specific synthetic-loss measurement session:

```
cfm mef synthetic-loss show service <service> local-mepid
<mepid> session-id <index> history
```

To display the availability statistics of a specific synthetic-loss measurement session

4 Display availability statistics of a specific synthetic-loss measurement session:

```
cfm mef synthetic-loss show availability-stats service
<service> local-mepid <mepid>
```


Copyright© 2022 Ciena® Corporation

To display history availability statistics of a specific synthetic loss measurement session

5 Display history availability statistics of a specific synthetic loss measurement session:

```
cfm mef synthetic-loss show availability-stats service
<service> local-mepid <mepid> history all
```

—end—

Examples

The following example shows output from the cfm mef synthetic-loss show command:

```
> cfm mef synthetic-loss show

+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                | serv                                            |
| Local Mepid            | 77                                              |
| Remote Mepid           | 67                                              |
| Test-Id                | 1                                               |
| Session-Id             | 1                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+--------------------------- Measured Stats ----------------------------+
|                |     FLR      |          Availability Parameters         |
|                |   (milli %)  | Status       | Last Transition Time      |
+----------------+--------------+--------------+---------------------------+
| Forward        | 0            | Available    | 04/21/2017 05:36:18       |
| Backward       | 0            | Available    | 0                         |
+----------------+--------------+--------------+---------------------------+
+------------------------ Measurement Interval --------------------------+
| Interval-Index         | 38                                             |
| Start Time(date/time)  | 04/21/2017 09:41:24                            |
| Elapsed Time (ms)      | 83261                                          |
| Pdu Sent               | 16599                                          |
| Pdu Received           | 16598                                          |
| Suspect                | No                                             |
+------------------------+-------------------------------------------------+
+---------------------------- Statistics -------------------------------+
| Statistic                  | Forward              | Backward           |
| Transmit                   | 16599                | 16598              |
| Received                   | 16598                | 16598              |
| Frame Loss                 | 0                    | 0                  |
| FLR Min(milli %)           | 0                    | 0                  |
| FLR Avg(milli %)           | 0                    | 0                  |
| FLR Max(milli %)           | 0                    | 0                  |
+----------------------------+----------------------+--------------------+
+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                | serv                                            |
| Local Mepid            | 77                                              |
| Remote Mepid           | 67                                              |
| Test-Id                | 2                                               |
| Session-Id             | 2                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+--------------------------- Measured Stats ----------------------------+
|                |     FLR      |          Availability Parameters         |
|                |   (milli %)  | Status       | Last Transition Time      |
```


Copyright© 2022 Ciena® Corporation

```
+---------------+--------------+--------------+---------------------------+
| Forward       | 0            | Available    | 04/21/2017 05:36:33       |
| Backward      | 0            | Available    | 0                         |
+---------------+--------------+--------------+---------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index          | 38                                            |
| Start Time(date/time)   | 04/21/2017 09:35:31                           |
| Elapsed Time (ms)       | 436237                                        |
| Pdu Sent                | 43486                                         |
| Pdu Received            | 43486                                         |
| Suspect                 | No                                            |
+-------------------------+-----------------------------------------------+
+----------------------------- Statistics -------------------------------+
| Statistic                 | Forward               | Backward              |
| Transmit                  | 43486                 | 43486                 |
| Received                  | 43486                 | 43486                 |
| Frame Loss                | 0                     | 0                     |
| FLR Min(milli %)          | 0                     | 0                     |
| FLR Avg(milli %)          | 0                     | 0                     |
| FLR Max(milli %)          | 0                     | 0                     |
+---------------------------+-----------------------+-----------------------+
+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                 | serv                                          |
| Local Mepid             | 77                                            |
| Remote Mepid            | 67                                            |
| Test-Id                 | 3                                             |
| Session-Id              | 3                                             |
| Active                  | Yes                                           |
+-------------------------+-----------------------------------------------+
+---------------------------- Measured Stats ----------------------------+
|               |     FLR      |           Availability Parameters         |
|               |   (milli %)  | Status       | Last Transition Time       |
+---------------+--------------+--------------+---------------------------+
| Forward       | 0            | Available    | 0                         |
| Backward      | 0            | Available    | 0                         |
+---------------+--------------+--------------+---------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index          | 38                                            |
| Start Time(date/time)   | 04/21/2017 09:36:18                           |
| Elapsed Time (ms)       | 388557                                        |
| Pdu Sent                | 6                                             |
| Pdu Received            | 7                                             |
| Suspect                 | No                                            |
+-------------------------+-----------------------------------------------+
+----------------------------- Statistics -------------------------------+
| Statistic                 | Forward               | Backward              |
| Transmit                  | 6                     | 7                     |
| Received                  | 7                     | 7                     |
| Frame Loss                | 0                     | 0                     |
| FLR Min(milli %)          | 0                     | 0                     |
| FLR Avg(milli %)          | 0                     | 0                     |
| FLR Max(milli %)          | 0                     | 0                     |
+---------------------------+-----------------------+-----------------------+
+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                 | serv                                          |
| Local Mepid             | 77                                            |
| Remote Mepid            | 67                                            |
| Test-Id                 | 4                                             |
| Session-Id              | 4                                             |
| Active                  | Yes                                           |
```


Copyright© 2022 Ciena® Corporation

```
+-----------------------+-------------------------------------------------+
+---------------------------- Measured Stats ----------------------------+
|                |     FLR      |          Availability Parameters          |
|                |   (milli %)  | Status        | Last Transition Time      |
+---------------+--------------+--------------+---------------------------+
| Forward        | 0            | Available    | 0                         |
| Backward       | 0            | Available    | 0                         |
+---------------+--------------+--------------+---------------------------+
+------------------------- Measurement Interval -------------------------+
| Interval-Index          | 38                                            |
| Start Time(date/time)   | 04/21/2017 09:35:49                           |
| Elapsed Time (ms)       | 417731                                        |
| Pdu Sent                | 1                                             |
| Pdu Received            | 2                                             |
| Suspect                 | No                                            |
+-----------------------+-------------------------------------------------+
+----------------------------- Statistics ------------------------------+
| Statistic                  | Forward                | Backward            |
| Transmit                   | 1                      | 2                   |
| Received                   | 2                      | 2                   |
| Frame Loss                 | 0                      | 0                   |
| FLR Min(milli %)           | 0                      | 0                   |
| FLR Avg(milli %)           | 0                      | 0                   |
| FLR Max(milli %)           | 0                      | 0                   |
+---------------------------+----------------------+----------------------+
```

The following example shows the output when displaying history statistics for a specific synthetic-loss measurement session.

```
> cfm mef synthetic-loss show service cfm201 local-mepid 107 session-id 4
history

+------------ MEP SYNTHETIC LOSS SESSION MEASUREMENT HISTORY -------------+
| Service                 | cfm201                                        |
| Local Mepid             | 107                                           |
| Remote Mepid            | 98                                            |
| Test-Id                 | 4                                             |
| Session-Id              | 4                                             |
| Active                  | Yes                                           |
+-----------------------+-------------------------------------------------+
+------------------------- Measurement Interval -------------------------+
| Interval-Index          | 1                                             |
| End Time(date/time)     | 01/02/2000 05:47:26                           |
| Elapsed Time (ms)       | 7223068                                       |
| Pdu Sent                | 7201                                          |
| Pdu Received            | 7200                                          |
| Suspect                 | No                                            |
+-----------------------+-------------------------------------------------+
+----------------------------- Statistics ------------------------------+
| Statistic                  | Forward                | Backward            |
| Transmit                   | 7201                   | 7200                |
| Received                   | 7200                   | 7200                |
| Frame Loss                 | 0                      | 0                   |
| FLR Min(milli %)           | 0                      | 0                   |
| FLR Avg(milli %)           | 0                      | 0                   |
| FLR Max(milli %)           | 0                      | 0                   |
+---------------------------+----------------------+----------------------+
+------------------------- Measurement Interval -------------------------+
| Interval-Index          | 2                                             |
```


Copyright© 2022 Ciena® Corporation

```
| End Time(date/time)    | 01/02/2000 07:47:25                                  |
| Elapsed Time (ms)      | 7199957                                              |
| Pdu Sent               | 7178                                                 |
| Pdu Received           | 7178                                                 |
| Suspect                | No                                                   |
+------------------------+------------------------------------------------------+
+------------------------------ Statistics --------------------------------+
| Statistic                | Forward               | Backward              |
| Transmit                 | 7178                  | 7178                  |
| Received                 | 7178                  | 7178                  |
| Frame Loss               | 0                     | 0                     |
| FLR Min(milli %)         | 0                     | 0                     |
| FLR Avg(milli %)         | 0                     | 0                     |
| FLR Max(milli %)         | 0                     | 0                     |
+--------------------------+-----------------------+-----------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 3                                                  |
| End Time(date/time)    | 01/02/2000 09:47:26                                |
| Elapsed Time (ms)      | 7200044                                            |
| Pdu Sent               | 7178                                               |
| Pdu Received           | 7178                                               |
| Suspect                | No                                                 |
+------------------------+----------------------------------------------------+
+------------------------------ Statistics --------------------------------+
| Statistic                | Forward               | Backward              |
| Transmit                 | 7178                  | 7178                  |
| Received                 | 7178                  | 7178                  |
| Frame Loss               | 0                     | 0                     |
| FLR Min(milli %)         | 0                     | 0                     |
| FLR Avg(milli %)         | 0                     | 0                     |
| FLR Max(milli %)         | 0                     | 0                     |
+--------------------------+-----------------------+-----------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 4                                                  |
| End Time(date/time)    | 01/02/2000 11:47:25                                |
| Elapsed Time (ms)      | 7199956                                            |
| Pdu Sent               | 7178                                               |
| Pdu Received           | 7178                                               |
| Suspect                | No                                                 |
+------------------------+----------------------------------------------------+
+------------------------------ Statistics --------------------------------+
| Statistic                | Forward               | Backward              |
| Transmit                 | 7178                  | 7178                  |
| Received                 | 7178                  | 7178                  |
| Frame Loss               | 0                     | 0                     |
| FLR Min(milli %)         | 0                     | 0                     |
| FLR Avg(milli %)         | 0                     | 0                     |
| FLR Max(milli %)         | 0                     | 0                     |
+--------------------------+-----------------------+-----------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 5                                                  |
| End Time(date/time)    | 01/02/2000 13:47:26                                |
| Elapsed Time (ms)      | 7200052                                            |
| Pdu Sent               | 7178                                               |
| Pdu Received           | 7178                                               |
| Suspect                | No                                                 |
+------------------------+----------------------------------------------------+
+------------------------------ Statistics --------------------------------+
| Statistic                | Forward               | Backward              |
| Transmit                 | 7178                  | 7178                  |
```


Copyright© 2022 Ciena® Corporation

```
| Received                  | 7178                  | 7178                  |
| Frame Loss                | 0                     | 0                     |
| FLR Min(milli %)          | 0                     | 0                     |
| FLR Avg(milli %)          | 0                     | 0                     |
| FLR Max(milli %)          | 0                     | 0                     |
+---------------------------+-----------------------+-----------------------+
```

The following example shows the output when displaying the availability statistics of a specific synthetic loss measurement session.

```
cfm mef synthetic-loss show service cfm201 local-mepid 107
+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                | cfm201                                          |
| Local Mepid            | 107                                             |
| Remote Mepid           | 98                                              |
| Test-Id                | 2                                               |
| Session-Id             | 2                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+---------------------------- Measured Stats -----------------------------+
|                |     FLR      |          Availability Parameters          |
|                |   (milli %)  | Status       | Last Transition Time       |
+----------------+--------------+--------------+----------------------------+
| Forward        | 0            | Available    | 0                          |
| Backward       | 0            | Available    | 0                          |
+----------------+--------------+--------------+----------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 48                                             |
| Start Time(date/time)  | 01/02/2000 15:22:14                            |
| Elapsed Time (ms)      | 489770                                         |
| Pdu Sent               | 488                                            |
| Pdu Received           | 489                                            |
| Suspect                | No                                             |
+------------------------+-------------------------------------------------+
+------------------------------ Statistics -------------------------------+
| Statistic                 | Forward               | Backward              |
| Transmit                  | 488                   | 489                   |
| Received                  | 489                   | 489                   |
| Frame Loss                | 0                     | 0                     |
| FLR Min(milli %)          | 0                     | 0                     |
| FLR Avg(milli %)          | 0                     | 0                     |
| FLR Max(milli %)          | 0                     | 0                     |
+---------------------------+-----------------------+-----------------------+
+--------- MEP SYNTHETIC LOSS SESSION MEASUREMENT INTERVAL INFO ----------+
| Service                | cfm201                                          |
| Local Mepid            | 107                                             |
| Remote Mepid           | 98                                              |
| Test-Id                | 4                                               |
| Session-Id             | 4                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+---------------------------- Measured Stats -----------------------------+
|                |     FLR      |          Availability Parameters          |
|                |   (milli %)  | Status       | Last Transition Time       |
+----------------+--------------+--------------+----------------------------+
| Forward        | 0            | Available    | 0                          |
| Backward       | 0            | Available    | 0                          |
+----------------+--------------+--------------+----------------------------+
+------------------------- Measurement Interval --------------------------+
| Interval-Index         | 6                                              |
```


Copyright© 2022 Ciena® Corporation

```
| Start Time(date/time)  | 01/02/2000 13:47:26                                  |
| Elapsed Time (ms)      | 6178581                                              |
| Pdu Sent               | 6159                                                 |
| Pdu Received           | 6160                                                 |
| Suspect                | No                                                   |
+------------------------+------------------------------------------------------+
+------------------------------ Statistics --------------------------------+
| Statistic                | Forward               | Backward              |
| Transmit                 | 6159                  | 6160                  |
| Received                 | 6160                  | 6160                  |
| Frame Loss               | 0                     | 0                     |
| FLR Min(milli %)         | 0                     | 0                     |
| FLR Avg(milli %)         | 0                     | 0                     |
| FLR Max(milli %)         | 0                     | 0                     |
+--------------------------+-----------------------+-----------------------+
```

The following example shows output when displaying history availability statistics of a specific synthetic loss measurement session.

```
> cfm mef synthetic-loss availability show service cfm201 local-mepid 107
session-id 4
+--------------- MEP AVAILABILITY MEASUREMENT INFORMATION ----------------+
| Service                | cfm201                                          |
| Local Mepid            | 107                                             |
| Remote Mepid           | 98                                              |
| Test-Id                | 4                                               |
| Session-Id             | 4                                               |
| Active                 | Yes                                             |
+------------------------+-------------------------------------------------+
+------------------- Availability Measurement Interval --------------------+
| Interval-Index         | 48                                              |
| Start Time(date/time)  | 01/02/2000 15:32:03                             |
| Measurement Interval   | 15                                              |
| Elapsed Time (ms)      | 69286                                           |
| Consecutive Meas Pdus  | 10                                              |
| FLR Threshold(milli%)  | 50000                                           |
| Consecutive Interval   | 10                                              |
| Consecutive High FLR   | 5                                               |
| Suspect                | No                                              |
+------------------------+-------------------------------------------------+
+------------------------ Availability Statistics -------------------------+
| Availability KPI           | Forward               | Backward              |
+----------------------------+-----------------------+-----------------------+
| High Loss Count (HLI)      | 0                     | 0                     |
| Consecutive HLI Count      | 0                     | 0                     |
| Available Indicator        | 0                     | 0                     |
| Unavailable Indicator      | 0                     | 0                     |
| FLR Min(milli %)           | 0                     | 0                     |
| FLR Avg(milli %)           | 0                     | 0                     |
| FLR Max(milli %)           | 0                     | 0                     |
+----------------------------+-----------------------+-----------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-49
Displaying MEF 35 SOAM sessions on a MEP sorted by session index

Display MEF 35 SOAM sessions on a MEP sorted by session index.

Step	Action
1	Display SOAM sessions on a MEP sorted by session index. `cfm mef session show service <service> {local-mepid <NUMBER: 1-8191>} {test-type <delay | synthetic-loss>}`

—end—

Example

The following example shows the output when listing SOAM sessions on a MEP sorted by the session index.

```
> cfm mef session show service cfm201 local-mepid 107 test-type delay

+-------------------------- MEP Y1731 SESSION LIST INFO ---------------------------+
|                    | Local | Remote |            |            | Test     | Oper     |
|Service             | Mepid | Mepid  | Session-Id | Test-Id    | Type     | State    |
+--------------------+-------+--------+------------+------------+----------+----------+
|cfm201              | 107   | 98     | 1          | 1          | MEF DM   | Active   |
+--------------------+-------+--------+------------+------------+----------+----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-50
Displaying MEF 35 frame relay range profiles

Display MEF 35 frame relay range profiles

Step	Action

To display all MEF 35 frame relay range profiles

1 Display all MEF 35 frame relay range profiles:

```
cfm profile bins show
```

To display specific MEF 35 frame relay range profiles

2 Display specific MEF 35 frame relay range profiles:

```
cfm profile bins show delay-range Default-Delay-Range-
Profile-Name
```

—end—

Example

The following example shows the output for the cfm profile bins show command.

```
> cfm profile bins show

+-------------- DELAY MEASURMENTBINS DELAY PROFILE ---------------+
| Name | Default-Delay-Profile-Name                                |
+------+-------------------------+------+-------------------------+
| Bins | Threshold (us)          | Bins | Threshold (us)          |
+------+-------------------------+------+-------------------------+
| 1    | 5000                    | 2    | 10000                   |
+------+-------------------------+------+-------------------------+
| 3    | 15000                   |      |                         |
+------+-------------------------+------+-------------------------+

+-------------- DELAY MEASURMENTBINS JITTER PROFILE --------------+
| Name | Default-Jitter-Profile-Name                               |
+------+-------------------------+------+-------------------------+
| Bins | Threshold (us)          | Bins | Threshold (us)          |
+------+-------------------------+------+-------------------------+
| 1    | 5000                    | 2    | 10000                   |
+------+-------------------------+------+-------------------------+

+----------- DELAY MEASURMENTBINS DELAY RANGE PROFILE ------------+
| Name | Default-Delay-Range-Profile-Name                          |
+------+-------------------------+------+-------------------------+
| Bins | Threshold (us)          | Bins | Threshold (us)          |
+------+-------------------------+------+-------------------------+
| 1    | 5000                    | 2    | 10000                   |
+------+-------------------------+------+-------------------------+
```

The following example shows the output from the cfm profile bins show delay-range Default-Delay-Range-Profile-Name command:

Copyright© 2022 Ciena® Corporation

```
> cfm profile bins show delay-range Default-Delay-Range-Profile-Name

+----------- DELAY MEASURMENTBINS DELAY RANGE PROFILE ------------+
| Name | Default-Delay-Range-Profile-Name                          |
+------+-------------------------+------+-------------------------+
| Bins | Threshold (us)          | Bins | Threshold (us)          |
+------+-------------------------+------+-------------------------+
| 1    | 5000                    | 2    | 10000                   |
+------+-------------------------+------+-------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 2-51
Creating a MEF 35 compliant threshold profile

You can create the following MEF 35 TCA profiles:

- loss
- delay

Step	Action

To create a TCA loss profile

1 Create a TCA loss profile:

```
cfm profile threshold create loss <Name (no ,)
String[1..45]>
```

where

loss <Name (no ,) String[1..45]> is the name of the loss profile.

To create a delay profile

2 Create a TCA delay profile:

```
cfm profile threshold create delay <Name (no ,)
String[1..45]>
```

where

delay <Name (no ,) String[1..45]> is the name of the delay profile.

—end—

Example

The following example creates a loss profile:

```
> cfm profile threshold create loss lossprofile1
```


Copyright© 2022 Ciena® Corporation

Procedure 2-52
Deleting a MEF 35 compliant threshold profile

You can delete the following MEF 35 compliant TCA profiles:

- loss
- delay

Step	Action

To delete a MEF 35 compliant loss profile

1 Delete a MEF 35 compliant loss profile:

```
cfm profile threshold delete loss <Name (no ,)
String[1..45]>
```

To delete a MEF 35 compliant delay profile

2 Delete a MEF 35 compliant delay profile:

```
cfm profile threshold delete delay <Name (no ,)
String[1..45]>
```

—end—

Example

The following example deletes a MEF 35 compliant loss profile:

```
> cfm profile threshold delete loss lossprofile1
```


Copyright© 2022 Ciena® Corporation

Procedure 2-53
Configuring parameters to a MEF 35 compliant threshold profile

You can configure the following parameters to a MEF 35 compliant threshold profile:

- loss
- delay

Step	Action

To configure a loss profile parameters to a MEF 35 compliant threshold profile

1 Configure loss profile parameters to a MEF 35 compliant threshold profile:

```
cfm profile threshold set loss <profile-name> [forward-maximum-flr <value> forward-average-flr <value> backward-maximum-flr <value> backward-average-flr <value> avail-forward-high-loss <value> avail-forward-consecutive-high-loss <value> avail-backward-high-loss <value> avail-backward-consecutive-high-loss <value> avail-forward-unavailable-count <value> avail-backward-unavailable-count <value> avail-forward-available-ratio <value> avail-backward-available-ratio <value>]
```

where

loss <profile-name>	is the loss profile name.
forward-maximum-flr <value>	is the forward maximum flr value. Default is 100000.
forward-average-flr <value>	is the forward average flr value. Default is 100000.
backward-maximum-flr <value>	is the backward maximum flr value. Default is 100000.
backward-average-flr <value>	is the backward average flr value. Default is 100000.
avail-forward-high-loss <value>	is the availability forward high-loss value. Default is 4294967295.
avail-forward-consecutive-high-loss <value>	is the availability forward consecutive high-loss value. Default is 4294967295.

Copyright© 2022 Ciena® Corporation

avail-backward-high-loss <value>	is the availability backward high-loss value. Default is 4294967295.
avail-backward-consecutive-high-loss <value>	is the availability backward consecutive high-loss value. Default is 4294967295.
avail-forward-unavailable-count <value>	is the availability forward available count value. Default is 4294967295.
avail-backward-unavailable-count <value>	is the availability backward unavailable count value. Default is 4294967295.
avail-forward-available-ratio <value>	is the availability forward available ratio value. Default is 0.
avail-backward-available-ratio <value>	is the availability backward available ratio value. Default is 0.

To configure delay profile parameters to a MEF 35 compliant threshold profile

2 Configure delay profile parameters to a MEF 35 compliant threshold profile:

```
cfm profile threshold set delay <profile-name> [forward-maximum-ifdv <value> forward-average-ifdv <value> backward-maximum-ifdv <value> backward-average-ifdv <value> two-way-maximum-fd <value> two-way-average-fd<value> two-way-maximum-ifdv <value> two-way-average-ifdv <value> two-way-maximum-fdr<value> two-way-average-fdr <value>]
```

where

delay <profile-name>	is the profile name of the delay profile.
two-way-average-fd <value>	is the two way average fd value in microseconds. Default is 4294967295.
two-way-maximum-ifdv <value>	is the two way maximum ifdv value in microseconds. Default is 4294967295.
forward-maximum-ifdv <value>	is the forward maximum ifdv value in microseconds. Default is 4294967295.
forward-average-ifdv <value>	is the forward average ifdv value in microseconds. Default is 4294967295.
backward-maximum-ifdv <value>	is the backward maximum ifdv value in microseconds. Default is 4294967295.

Copyright© 2022 Ciena® Corporation

backward-average-ifdv <value>	is the backward average ifdv value in microseconds. Default is 4294967295.
two-way-maximum-fd <value>	is the two way maximum fd value in microseconds. Default is 4294967295.
two-way-average-ifdv <value>	is the two way average iffdv value in microseconds. Default is 4294967295.
two-way-maximum-fdr <value>	is the two way maximum frdr value in microseconds. Default is 4294967295.
two-way-average-fdr <value>	is the two way average frd value in microseconds. Default is 4294967295.

To return loss profile parameters of a MEF 35 compliant threshold profile to default values

3 Return loss profile parameters of a MEF 35 compliant threshold profile to default values:

```
cfm profile threshold unset loss <profile-name> [forward-maximum-flr forward-average-flr backward-maximum-flr backward-average-flr avail-forward-high-loss avail-forward-consecutive-high-loss avail-backward-high-loss avail-backward-consecutive-high-loss avail-forward-unavailable-count avail-backward-unavailable-count avail-forward-available-ratio avail-backward-available-ratio]
```

To return delay profile parameters of a MEF 35 compliant threshold profile to default values

4 Return delay profile parameters to a MEF 35 compliant threshold profile to default values:

```
cfm profile threshold unset delay <profile-name> [forward-maximum-ifdv forward-average-ifdv backward-maximum-ifdv backward-average-ifdv two-way-maximum-fd two-way-average-fd two-way-maximum-ifdv two-way-average-ifdvtwo-way-maximum-fdr two-way-average-fdr]
```

—end—

Example

The following example configures delay profile parameters in a threshold profile.

```
> cfm profile threshold set delay dm1 forward-maximum-ifdv 4300
```

The following example configures loss profile parameters in a threshold profile.

```
> cfm profile threshold set loss loss1 forward-maximum-ifdv 4300
```


Copyright© 2022 Ciena® Corporation

Procedure 2-54
Attaching a threshold profile to MEF 35 compliant sessions

Attach a threshold profile to the following MEF 35 compliant sessions:

- loss
- delay

Step	Action

To attach a threshold profile to a MEF 35 compliant loss session

1 Create an MEF 35 compliant loss profile

```
cfm profile threshold create loss <Name (no ,)
String[1..45]
```

where

loss <Name (no ,) String[1..45] is the name of the loss profile.

2 Configure the loss profile parameters to a MEF 35 compliant threshold profile:

```
cfm profile threshold set loss <Name (no ,) String[1..45]>
forward-maximum-flr <value>
```

3 Attach a threshold profile to a MEF 35 compliant loss session:

```
cfm mef synthetic-loss create service <service> local-
mepid <lmep id> remote-mepid <rmep id> threshold profile
<profile name>
```

where

service <service> is the CFM service name.

local-mepid <lmep id> is the local mep ID.

remote-mepid <rmep id> is the remote mep ID.

threshold <profile name> is the threshold profile name.

To attach a threshold profile to a MEF 35 compliant delay session

4 Create an MEF 35 compliant delay profile

```
cfm profile threshold create delay <Name (no ,)
String[1..45]
```

where

delay <Name (no ,) String[1..45] is the name of the delay profile.

Copyright© 2022 Ciena® Corporation

5 Configure the delay profile parameters to a MEF 35 compliant threshold profile:

```
cfm profile threshold set delay <Name (no ,)
String[1..45]> forward-maximum-flr <value>
```

6 Attach a threshold profile to a MEF 35 compliant delay session:

```
cfm mef delay create service <service> local-mepid <lmep
id> remote-mepid <remep id> threshold profile <profile
name>
```

—end—

Example

The following example attaches a profile to a MEF 35 complaint loss session:

```
> cfm profile threshold create delay dm1
> cfm profile threshold set delay dm1 forward-maximum-ifdv 500
> cfm mef delay create service servicename local-mepid 1 remote-mepid 2
threshold-profile dm1
```


Copyright© 2022 Ciena® Corporation

Procedure 2-55
Displaying MEF 35 compliant threshold profiles

You can display MEF 35 compliant threshold profiles:

- all threshold profiles
- specific threshold profiles

Step	Action

To display all MEF 35 compliant threshold profiles

1 Display all threshold profiles:

```
cfm profile threshold show
```

To display a specific MEF 35 compliant threshold profile

2 Delete a TCA delay profile:

```
cfm profile threshold show delay delayprofile2
```

—end—

Example

The following example shows the output for the cfm profile threshold show command:

```
> cfm profile threshold show

+----------------- LOSS THRESHOLD PROFILE -----------------+
| Name | lossprofile1                                      |
+------+-------------+------------------+------------------+
| PARAMETER          | FORWARD          | BACKWARD         |
+--------------------+------------------+------------------+
| Maximum FLR(milli%)| 100000           | 100000           |
| Average FLR(milli%)| 100000           | 100000           |
| Avail Ratio(milli%)| 0                | 0                |
| High Loss          | 4294967295       | 4294967295       |
| Cons High Loss     | 4294967295       | 4294967295       |
| Unavailable Count  | 4294967295       | 4294967295       |
+--------------------+------------------+------------------+

+---------------- DELAY THRESHOLD PROFILE -----------------+
| Name | delayprofile1                                     |
+------+---------+-------------+-------------+-------------+
| PARAMETER      | FORWARD(us) | BACKWARD(us)| TWO WAY(us) |
+----------------+-------------+-------------+-------------+
| Maximum IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Average IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Maximum FD     | N/A         | N/A         | 4294967295  |
| Average FD     | N/A         | N/A         | 4294967295  |
| Maximum FDR    | N/A         | N/A         | 4294967295  |
| Average FDR    | N/A         | N/A         | 4294967295  |
+----------------+-------------+-------------+-------------+
```


Copyright© 2022 Ciena® Corporation

```
+------+-------------------------------------------------+
| Name | delayprofile2                                   |
+------+---------+-------------+-------------+-------------+
| PARAMETER      | FORWARD(us) | BACKWARD(us)| TWO WAY(us) |
+----------------+-------------+-------------+-------------+
| Maximum IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Average IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Maximum FD     | N/A         | N/A         | 4294967295  |
| Average FD     | N/A         | N/A         | 4294967295  |
| Maximum FDR    | N/A         | N/A         | 4294967295  |
| Average FDR    | N/A         | N/A         | 4294967295  |
+----------------+-------------+-------------+-------------+
```

The following example shows the output for the cfm profile threshold show command for a specific threshold:

```
>cfm profile threshold show delay delayprofile2

+---------------- DELAY THRESHOLD PROFILE -----------------+
| Name | delayprofile2                                   |
+------+---------+-------------+-------------+-------------+
| PARAMETER      | FORWARD(us) | BACKWARD(us)| TWO WAY(us) |
+----------------+-------------+-------------+-------------+
| Maximum IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Average IFDV   | 4294967295  | 4294967295  | 4294967295  |
| Maximum FD     | N/A         | N/A         | 4294967295  |
| Average FD     | N/A         | N/A         | 4294967295  |
| Maximum FDR    | N/A         | N/A         | 4294967295  |
| Average FDR    | N/A         | N/A         | 4294967295  |
+----------------+-------------+-------------+-------------+
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Signal degrade detection

Signal degrade is partial loss of signal between two or more communicating devices in Carrier Ethernet due to such things as environmental conditions, poor devices or fiber cuts. Signal degrade conditions can be detected by

- Bit error rates over threshold, for example, greater than 10^{-8}
- Frame loss rates over threshold
- Frame latency/jitter rates over threshold

Signal degrade detection is supported on 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 devices. Signal degrade detection is supported on aggregation ports. It is not supported on TDM and aggregation member ports.

Signal degrade can be used as a trigger to perform protection switching on static co-routed bi-directional tunnels. See *39XX/51XX MPLS Configuration* for the configuration steps.

> ***Note:*** Signal degrade detection is useful for aggregation ports with only one member. For multi-member aggregation ports, signal degrade detection occurs on one of the aggregation members only.

Signal degrade conditions are reported on a per-port-basis using SNMP traps. The system raises a signal degrade alarm on a port when a signal degrade condition is detected. The alarm is cleared when the signal degrade condition is cleared.

Bit error rate to frame error rate relationship

Frame error rate (FER) is the ratio of undelivered data frames divided by the total number of transmitted frames. A frame is declared erred or lost if at least one bit is erroneous.

Copyright© 2022 Ciena® Corporation

Assuming bit errors are independent of each other, then the expected value of the FER, (which for a data packet length of L bits) can be expressed as FER ~ 1 - (1-BER)^{L}. An example of this is shown in Table 3-1.

Table 3-1
BER to FER relationship

Bit error rate	Frame size (bytes)	Frame error rate
10^{-8}	64	5.12×10^{-6}
	512	4.10×10^{-5}
	1522	1.22×10^{-4}
	9216	7.11×10^{-4}

A bit error rate (BER) is the probability that any single bit is decoded incorrectly (regardless of any other bit). The probability that any such single bit is decoded correctly is 1-BER. The probability of correctly decoding all (L) bits in the frame is (1-BER)^{L}.

Signal degrade detection

Y.1731 Synthetic Loss Measurement (SLM) tests are used for signal degrade detection on SAOS 6.x devices. These tests exchange synthetic frames on the link to be monitored for signal degrade over a configured duration and compare frame loss with the configurable threshold to determine if signal degrade exists on the link.

As Y.1731 SLM sessions run between Maintenance End Points (MEPs) belonging to a common CFM service (maintenance association), down MEP based Connectivity Fault Management (CFM) service must be configured at two ends of the link to be monitored for signal degrade. Signal degrade detection is not supported using MEF mode Y.1731 synthetic-loss sessions.

SLM tests measure near-end and far-end frame loss using synthetic frames.

- Near-end frame loss is frame loss associated with ingress synthetic frames.
- Far-end frame loss is frame-loss associated with egress synthetic frames.

Copyright© 2022 Ciena® Corporation

Signal degrade detection compares frame loss with signal-degrade thresholds and triggers signal degrade events if the frame loss exceeds the threshold. Device supports two modes of signal degrade detection based on how frame loss shall be compared with “signal-degrade-thresholds” as described in Table 3-2.

Table 3-2

Signal-degrade trigger mode	Frame loss comparison algorithm
Near-end (default)	In this mode, near-end frame loss is compared with “signal-degrade-thresholds”. As the signal degrade condition is “Receive” direction degradation, this is an ideal way of performing signal degrade detection. However, this requires SLM test sessions to be initiated from both ends of the link.
Near-far-ends	In this mode, both near-end and far-end frame losses are compared with “signal-degrade-thresholds”. If either frame loss exceed the threshold, a signal degrade event is reported. As both forward and backward direction failures are detected by a common node only, this mode has limitations that it does not indicate the direction of degradation correctly.

Synthetic-loss test frames

If there are more than one SLM session running on the monitored link with different frame sizes, signal degrade is reported if any of these sessions observes frame-loss more than the signal degrade set threshold. When signal degrade is reported on the port, recovery is done only if all such sessions detect frame-loss below the signal degrade clear threshold value.

> ***Note:*** Frame-size specified in the “cfm synthetic-loss send” command does not include VLAN tag length.

Synthetic-loss test session duration

As Y.1731 synthetic frames are used for signal degrade detection, the SLM interval should not be greater than 100ms. The test duration should be configured such that at least 5000 synthetic test frames are exchanged within a given test-iteration for a reliable determination of signal degrade condition. All SLM sessions should be proactive without any idle period. This means that they start immediately and run forever with a zero repeat delay.

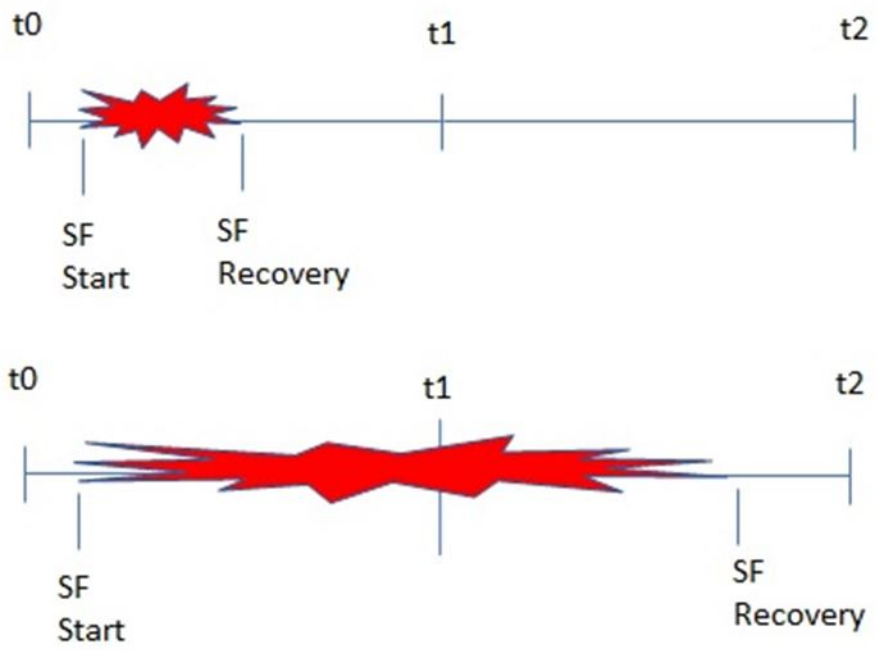
Copyright© 2022 Ciena® Corporation

If there are more than one SLM sessions running on the monitored link with different frame sizes or priorities for signal degrade detection, use identical test-duration for all such sessions.

To ensure that frame-loss observed within a measurement test-duration is not caused by signal fail, signal degrade detection is performed at the end of the measurement duration only if the link remains up throughout the duration.

Figure 3-1 shows an example of the relationship between signal fail and signal degrade. In the first example, signal fail was detected in measurement interval t0-t1, meaning that frame loss in this duration could be because of signal fail. The software treats this measurement duration as suspicious and does not perform frame-loss comparison with signal degrade-set threshold at the end of the duration. The next measurement window t1-t2 performs signal degrade detection as usual.

Figure 3-1
Signal fail and degrade example



In the second example, a single fail condition persists along two measurement windows (t0-t1 and t1-t2). Both measurement test-durations are treated as suspicious and are not eligible for signal degrade detection.

Copyright© 2022 Ciena® Corporation

If signal degrade is reported on a port and the port goes down (due to fiber cut or admin disable), signal degrade is cleared. When the port comes up again, signal degrade detection is then performed again from the next non-suspicious measurement test-duration.

Signal degrade detection thresholds

Y.1731 synthetic loss sessions are configured with distinct thresholds for signal degrade set and clear detection. If frame-loss exceeds “signal degrade set-threshold”, a signal degrade set event is reported for the port. If a signal degrade condition is reported on a given port, a signal degrade clear event is reported only if the frame-loss drops below the “signal degrade clear-threshold”. Signal degrade thresholds are configurable and its unit is “the number of frames lost within a test iteration duration.

Signal degrade detection based on delay/jitter

The service degrade protection switch is triggered based on delay, latency or jitter. Proactive Y.1731 delay measurement tests exchange DMM frames on a link to be monitored for signal degrade over a configured measurement window (duration) and compare delay, jitter with configurable thresholds to determine the signal degrade condition on the link.

The sequence of operations is as follows:

- Multiple iterations delay measurement tests are run and then the average is calculated. This value is then compared with the threshold value.
- When a threshold value is met or exceeded, the port marks a signal degrade state.
- AIS reads the state of the port in signal degrade state and then based on the configured actions link transition take place. This usually means AIS is paired with another protocol.
- Recovery is done only if the detect frame-loss is below the SD-clear threshold.

Signal degrade can be applied to MPLS-TP tunnels, essentially in conjunction with AIS.

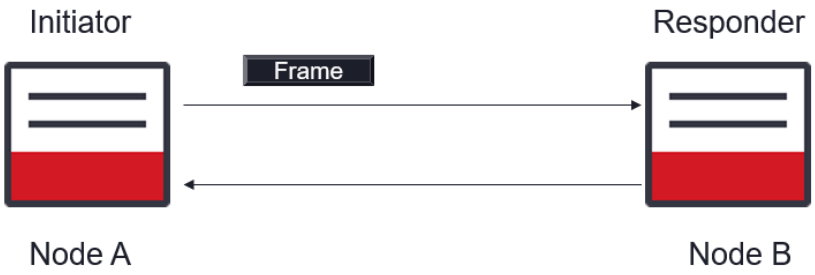
Y.1731 delay measurement tests measure two-way delay and jitter (backwards) using delay measurement (DM) frames as follows:

- Two-way delay refers to the overall time taken for a frame to travel from the initiator to the responder and return to the initiator.
- Backward jitter refers to delay associated with ingress delay frames.

The following figure describes how signal degrade works.

Copyright© 2022 Ciena® Corporation

Figure 3-2
Signal degrade detection

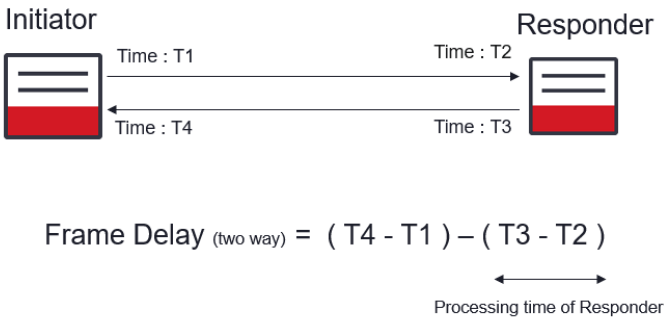


Signal degrade thresholds are configurable in microseconds.

In two-way delay mode, the frame is compared with “signal-degrade-thresholds. As both forward and backward direction failures are detected by common node (initiator) only, this mode is limited in that it does not provide complete information on the direction of the degradation. However, this is not useful if the node at the other end of the link does not support this feature or it does not have free resources to initiate ETH-DM test sessions.

The following figure shows two-way frame delay.

Figure 3-3
Two-way frame delay



Backward jitter is compared with “signal-degrade-thresholds”. As the signal degrade condition is “Rx” direction, this is an ideal way of performing SD detection. This would, however, require DM test sessions to be initiated from both ends of the link. The following figure describes inter frame delay variation in far to near direction:

Copyright© 2022 Ciena® Corporation

Figure 3-4
Backward jitter

Example from Node X's perspective acting as Initiator Frame Delay (backward jitter) = V.a – V.b

Where V.a = (T1.a-T2.a) , First run of the DM test

V.b = (T1.b-T2.b) , Second run of the DM test

Considerations for applying delay measurement

Take into account the following considerations when applying delay measurement:

- As delay measurement is based on a statistical sample, and it should be applied keeping in consideration the traffic pattern of actual network traffic. For example, assuming that traffic follows an IMIX (Internet Mix) distribution, then 3 ETH-DM sessions would need to be set up, each with different frame sizes (64, 598, 1400 bytes).
- DM should not be lower than 100ms (responder might not have hardware support for DM). The test duration should be configured such that at least 5000 delay test frames are exchanged within a given test-iteration for a reliable determination of signal degrade condition. All such DM sessions should be proactive, meaning the start immediately and run forever) without any idle period.
- If there is more than one DM session running on the monitored link with different frame sizes or priorities for signal degrade detection, it is recommended to use identical test duration for all such sessions. While using SLM and DM combined triggers, you can use the same duration in all SLM and DM test sessions.

SLM and DM session inter-working

SLM and DM sessions inter-work as follows:

- Signal degrade detection based on synthetic-loss and delay measurement sessions may be achieved simultaneously.
- SD-set event generated if one or more sessions on SD-monitoring enabled MEP crosses corresponding SD-set-threshold.
- SD-clear event generated when performance values of all SLM and DM sessions go under SD-clear threshold.

Copyright© 2022 Ciena® Corporation

Frame error rate to signal degrade threshold relationship

If the synthetic-loss frame size on the wire is N bytes and the length in bits (L) equals N x 8, the frame error rate equals $1 - (1\text{-BER})^{L}$.

If the Y.1731 test iteration duration is Y seconds and slm-interval duration is 100ms, the total number of synthetic frames sent equals Y x 10. Therefore, sd-set-threshold for the given test-duration is (FER x Y x 10). As signal distortion is random in nature, this threshold is an estimation. Configure the signal degrade threshold lower than the value computed by the formula. If possible, monitor synthetic loss history results for a few iterations and consider these results while determining the signal degrade threshold.

Table 3-3 captures the approximate signal detection set threshold for different frame sizes with a synthetic loss measurement interval of 100ms and test-duration of 15 minutes.

Table 3-3
FER to signal degrade threshold relationship

Bit error rate	Frame size (bytes)	Frame error rate	Approximate signal degrade set threshold
10^{-6}	68	5.44×10^{-4}	5
	512	4.10×10^{-5}	37
	1522	1.22×10^{-4}	109
	9216	7.11×10^{-4}	640

Signal degrade clear threshold must not be higher than “SD set threshold”. It lets the user set distinct clear threshold to avoid signal degrade toggling. It is recommended that “SD clear threshold” is configured significantly lower than “SD set threshold”.

Copyright© 2022 Ciena® Corporation

Procedure 3-1
Configuring signal degrade detection on a port

Signal degrade detection is not supported using MEF mode Y.1731 synthetic-loss sessions. By default, signal degrade detection is disabled.

Note: It is not necessary to perform step 1 and step 2 if the port is already part of the VLAN having the IP interface configured on it. In this case, you must configure CFM service/SLM session on the VLAN having the IP interface configured on it.

Step	Action

1 Create the VLAN which will be used to configure CFM service and initiate Y.1731 synthetic-loss measurement test(s) on:

```
vlan create vlan <vlan-id>
```

where

vlan <vlan-id> is the VLAN name.

2 Add the port to the VLAN you created:

```
vlan add vlan <vlan-id> port <port>
```

where

vlan <vlan-id> is the VLAN created in step 1.

port <port> is the port number.

3 Enable CFM globally:

```
cfm enable
```

4 Create CFM service on VLAN at the desired MD level:

```
cfm service create vlan <vlan-id> name <cfm-service>
level <level>
```

where

name <cfm-service> is the CFM service level

level <level> is the Maintenance Domain level.

5 Enable CFM service:

```
cfm service enable service <service>
```


Copyright© 2022 Ciena® Corporation

6 Create the down MEP on CFM service:

```
cfm mep create service <service> port <port> type down
mepid <mep-id>
```

where

mepid <mep-id> is the remote MEP identifier.

7 Set the signal degrade detection trigger mode and signal degrade monitoring on the down MEP:

```
cfm mep set service <service> local-mepid <lmep-id sd-
monitoring <on|off> sd-trigger-mode <near-end|near-far-
end>
```

where

sd-trigger mode <near-end|near-far-end>	sets the signal degrade detection mode on the MEP. • For near-end, the near-end loss is compared against the signal degrade threshold for determining the signal degrade condition. • For near-far-end, both near-end and far-end losses are compared against the signal degrade threshold to determine the signal degrade condition. • Default is near-end.

8 Initiate a proactive (non-terminating) SLM/SLR session with sd-set-threshold and sd-clear threshold configured:

```
cfm synthetic-loss send service <service> local-mepid
<lmep-id> mepid <remote mepid> duration <duration in
secs> iterate 0 slm-interval <interval> frame-size
<NUMBER: 64..1400> priority <NUMBER: 0..7> sd-set-
threshold <NUMBER: 0..65535> sd-clear-threshold <NUMBER:
0..65535>
```


Copyright© 2022 Ciena® Corporation

where

local-mepid <lmep-id>	is the local MEP identifier.
mepid <remote mepid>	is the remote MEP identifier.
duration <duration in secs>	is the duration of the test in seconds.
slm-interval <interval>	is the interval between the SLM frames.
frame-size <NUMBER: 64..1400>	specifies the frame size. Each SLM session can be configured with a distinct frame-size. The frame-size does not include VLAN tags size. If the frames are singly tagged and N bytes in length, frame-size should be (N-4).
priority <NUMBER: 0..7>	specifies the priority of the synthetic frames.
sd-set-threshold <NUMBER: 0..65535>	specifies the threshold value for setting signal degrade detection. The default is -1.
sd-clear-threshold <NUMBER: 0..65535>	specifies the threshold value for clearing signal degrade detection. The default is -1.

Note: If the signal degrade trigger mode is near-end, synthetic-loss tests are initiated from both ends of the link. If the signal degrade trigger mode is near-far-end, synthetic loss tests are initiated from one end only.

9 If required, create synthetic-loss responder at the far end of the link corresponding to the test session. This means that the far-end responder test-id must match the test-id chosen by the initiator.

```
cfm synthetic-loss-responder create service <service>
local-mepid <lmep-id mepid <remote mepid> test-id <id>
```

where

test-id <id>	is the test-id for the test session.

10 Enable signal degrade detection on the port:

```
port set port <port-id> signal-degrade-detection y1731-
performance-monitoring
```

where

signal-degrade-detection y1731-performance-monitoring>	enables the signal degrade detection on the port using Y1731 both SLM and DM sessions.

Copyright© 2022 Ciena® Corporation

11 Initiate proactive (non-terminating) DMM/DMR session with sd-set-threshold and sd-clear threshold configured.

Note: Sd-monitoring must be enabled on the MEP.

```
cfm-delay send service <service> local mepid <lmep-id
mepid> mepid <mepid> mepid <mepid> count <2..65535> dmm-
interval <interval> iterate <NUMBER 0..60> sd-delay-set-
threshold <threshold> sd-delay-clear-threshold
<threshold> sd-jitter-set-threshold <threshold> sd-
jitter-clear-threshold <threshold>
```

where

service <service>	specifies the CFM service level.
local mepid <lmep-id mep>	specifies the local MEP identifier.
mepid <mepid>	specifies the mepid.
count <NUMBER 2..65535>	specifies the number of DMMs to transmit in an iteration. The default is 100.
dmm-interval <interval>	specifies the interval between DMM frames.
iterate <NUMBER 0..60>	specifies he number of times the DMM test has to iterate. The default is 1. Continuous test is 0.
sd-delay-set-threshold <threshold>	specifies the threshold value, in microseconds, for setting two-way delay based signal delay detection.
sd-delay-clear-threshold <threshold>	specifies the threshold value, in microseconds, for clearing two-way delay based signal delay detection.
sd-jitter-set-threshold <threshold>	specifies the threshold value, in microseconds, for setting backward-jitter signal delay detection.
sd-jitter-clear-threshold <threshold>	specifies the threshold value, in microseconds, for clearing backward-jitter signal delay detection.

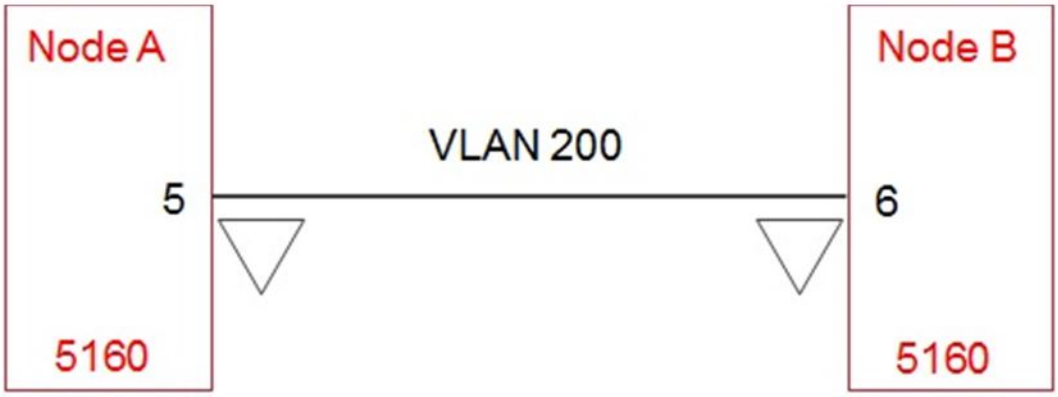
—end—

Examples

Figure 3-5 shows a sample configuration for signal degrade detection on two 5160s.

Copyright© 2022 Ciena® Corporation

Figure 3-5
Signal degrade detection on 5160s



The following commands create CFM service on node A:

```
vlan create vlan 200
vlan add vlan 200 port 5
cfm enable
cfm service create vlan 200 name sdDetection
cfm service enable service sdDetection
cfm mep create service sdDetection port 5 type down mepid 2
```

The following commands turn on signal degrade detection on node A:

```
cfm mep set service sdDetection local-mepid 2 sd-trigger-mode near-end
cfm mep set service sdDetection local-mepid 2 sd-monitoring on
cfm synthetic-loss send service sdDetection local-mepid 2 mepid 3 test-id 1
iterate 0 duration 900 frame-size 128 priority 3 slm-interval 100ms sd-set-
threshold 6500 sd-clear-threshold <7000>
port set port 5 signal-degrade-detection y1731-synthetic-loss

cfm synthetic-loss-responder create service sdDetection local-mepid 2 mepid 3
test-id 2
```

The following commands create CFM service on node B:

```
vlan create vlan 200
vlan add vlan 200 port 6
cfm enable
cfm service create vlan 200 name sdDetection
cfm service enable service sdDetection
cfm mep create service sdDetection port 5 type down mepid 3
```

The following commands turn on signal degrade detection on node B:

```
cfm mep set service sdDetection local-mepid 2 sd-trigger-mode near-end
cfm mep set service sdDetection local-mepid 2 sd-monitoring on
cfm synthetic-loss send service sdDetection local-mepid 3 mepid 2test-id 2
iterate 0 duration 900 frame-size 128 priority 3 slm-interval 100ms sd-set-
threshold 7000 sd-clear-threshold <10000>
port set port 6 signal-degrade-detection y1731-synthetic-loss
```

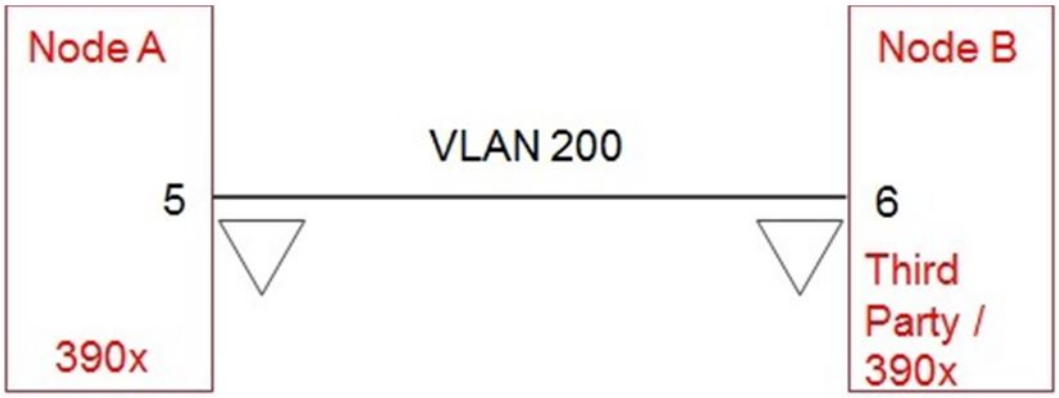

Copyright© 2022 Ciena® Corporation

```
cfm synthetic-loss-responder create service sdDetection local-mepid 3 mepid 2
test-id 1
```

If one end of the link does not support signal degrade detection or does not have the resources available to initiate a synthetic-loss session, the other end of the link should be performing signal degrade detection in near-far-end trigger mode.

Figure 3-6 shows a sample configuration for signal degrade detection on two 390x devices.

Figure 3-6
Signal degrade detection on 390x



The following commands create CFM service on node A:

```
vlan create vlan 200
vlan add vlan 200 port 5
cfm enable
cfm service create vlan 200 name sdDetection
cfm service enable service sdDetection
cfm mep create service sdDetection port 5 type down mepid 2
```

The following commands turn on signal degrade detection on node A:

```
cfm mep set service sdDetection local-mepid 2 sd-trigger-mode near-end
cfm mep set service sdDetection local-mepid 2 sd-monitoring on
cfm synthetic-loss send service sdDetection local-mepid 2 mepid 3 test-id 1
iterate 0 duration 900 frame-size 128 priority 3 slm-interval 100ms sd-set-
threshold 9000 sd-clear-threshold 20000
port set port 5 signal-degrade-detection y1731-synthetic-loss
```

The following commands create CFM service on node B:

```
vlan create vlan 200
vlan add vlan 200 port 6
cfm enable
```


Copyright© 2022 Ciena® Corporation

```
cfm service create vlan 200 name sdDetection
cfm service enable service sdDetection
cfm mep create service sdDetection port 5 type down mepid 3
```

The following commands creates a responder, if needed, on node B:

```
cfm synthetic-loss-responder create service sdDetection local-mepid 3 mepid 2
test-id 1
```

The following commands configures signal degrade detection based upon delay and jitter thresholds:

```
port set port 10 signal-degrade-detection y1731-performance-monitoring

cfm delay send service serv100 local-mepid 10 mepid 20 count 10 dmm-interval
1sec iterate 0 sd-delay-set threshold 11 sd-delay-clear-threshold 10 sd-
jittery-set-threshold 3 sd-jitter-clear-threshold1
```


Copyright© 2022 Ciena® Corporation

Procedure 3-2
Displaying signal degrade detection information

Display signal degrade detection information on a port. The degrade state has these possible values:

- “None” (default)
- “Degraded”

The degrade detection mode has these possible values:

- Off
- y1731-synthetic-loss
- y1731-performance-monitoring

Admin and Oper values of “Degrade detection mode” is the same in all cases other than port show of “LAG member port”. The LAG member port may have any Admin value, but Oper value is inherited from the parent LAG.

Step	Action
1	Display signal degrade detection information on a port. `port show port <port>` where port <port> is the port that you wish to display signal degrade detection information on.

—end—

Example

The following example shows output for signal degrade detection on port 3.

```
> port show port 3

+------------------------------- PORT 3 INFO ---------------------------------+
| Field                    | Admin                    | Oper                     |
+--------------------------+--------------------------+--------------------------+
| Type                     | 100/G                    | Lag (100/G)              |
| Description              |                                                      |
| Spanning Tree State      | Disabled                                             |
| MAC Address              | 2c:39:c1:cc:cd:64                                    |
| Phy Loopback             | Off                                                  |
| Link Flap Detection      | Off                                                  |
| Link Flap Count          | 5                                                    |
| Link Flap Detect Time    | 10                                                   |
| Link Flap Hold Time      | 300                                                  |
| Flow Loop Detect State   | Off                                                  |
| Flow Loop Detection      | Off                      | Off                      |
| L2CFT Status             | Disabled                 | Disabled                 |
| L2CFT Profile            |                          |                          |
| Link State               | Enabled                  | Disabled                 |
```


Copyright© 2022 Ciena® Corporation

VLLI State		Enabled
Rx Low Power Detection		
State Group Link State		
Degrade Detection Mode	off	off
Degrade State		None
Mode	default	unknown
Speed	1 Gbps	0 Gbps
Duplex	full	
Flow Control	off	
Auto Negotiation	Enabled	
Flow Control Advertised	off	
Speed Advertised		
Duplex Advertised		
PVID	1	1
Untag Ingress Data Vid	0	0
Fixed Resolved CoS	0	0
Fixed Resolved Color	green	green
Ingress VLAN Filter	Enabled	Enabled
Ingress VS Filter	Off	Off
Egress VS Filter	Off	Off
Acceptable Frame Type	all	all
Egress Untag VLAN	1	1
Max Frame Size	1526	1526
Inter-Packet Gap Size	12	12
Egress Frame Cos Policy	ignore	ignore
Untagged Data VS		
Untagged Ctrl VS		
VS L2 Transform Mode	i-push,e-pop	
Resolved CoS Policy	dot1d-tag1-cos	dot1d-tag1-cos
Service Port Type	Subscriber	Subscriber
Eth VC EtherType	8100	8100
Eth VC EtherType Policy	all	all
Mirror-port	Off	Off
Mirroring Encapsulation	none	
Mirror Encap VID	1	
Mirror Encap TPID	8100	
Ingress-mirror		
Egress-mirror		
Ingress to Egress QMap	Default-RCOS	Default-RCOS
XCVR caps mismatch	[NONE]	
Ingress FCOS->RCOS Map	DefaultFcosRcos	DefaultFcosRcos
Ingress RCOS Remark L2	False	False
Egress RCOS->FCOS Map	DefaultRcosFcos	DefaultRcosFcos
Benchmark State	Disabled	Disabled
Ingress ACL		
Aggregation Membership		agg1
VLAN Membership	1	1,777

Note 1: The degrade state has two possible values: “None” (default) and “Degraded”.

Note 2: Degrade detection mode has three possible values: Off, y1731-synthetic-loss and y1731-performance-monitoring.

Note 3: Admin and Oper values of “Degrade detection mode” are the same in all cases other than port show of “LAG member port”. The LAG member port may have any Admin value, but Oper value is always inherited from the parent LAG.

Copyright© 2022 Ciena® Corporation

Procedure 3-3
Displaying MEPs with signal-degrade monitoring filter

Display MEPs with signal-degrade monitoring filter.

Step	Action
1	Display MEPs with signal-degrade monitoring filter: `cfm mep show sd-monitoring`

—end—

Examples

The following example shows output for the cfm mep show sd-monitoring on command.

```
> cfm mep show sd-monitoring

+------------------------------------------------ CFM MEPs ------------------------------------------+
|                |        |    |     |    |                 |Admin|CCM  |CCM|Accelerated|SD Trigger   |
|Service         |Port    |Vid |Mepid|Type|   Mac Address   |State|State|Pri|           |Mode         |
+----------------+--------+----+-----+----+-----------------+-----+-----+---+-----------+-------------+
|ma11            |3       |200 |3    |down|2C:39:C1:FE:9C:74|en   |on   |2  |No         |near-end     |
|ma13            |2       |400 |8    |down|2C:39:C1:FE:9C:73|en   |on   |7  |No         |near-far-end |
+----------------+--------+----+-----+----+-----------------+-----+-----+---+-----------+-------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-4
Displaying signal degrade set and clear thresholds on a synthetic-loss session

Display the signal degrade set and clear thresholds.

Step	Action

1 Display signal degrade set and clear thresholds on a synthetic-loss session:

```
cfm synthetic-loss show service <service> local-mepid
<NUMBER: 1..8191> mepid <NUMBER: 1..8191> test-id
<NUMBER: 1..4294967295>
```

where

service <service>	is the name of the service.
local-mepid <NUMBER: 1..8191>	is the local MEPID.
mepid <NUMBER: 1..8191>	is the remote MEPID.
test-id <NUMBER: 1..4294967295>	is the test ID.

—end—

Example

The following example shows signal degrade set and clear threshold information on a synthetic-loss session:

```
> cfm synthetic-loss show service ma11 local-mepid 3 mepid 4 test-id 1

+---------------------- CFM SYNTHETIC LOSS SESSION INFO ----------------+
| Parameter                       | Value                                |
+---------------------------------+--------------------------------------+
| Service Name                    | ma11                                 |
| Service Index                   | 1                                    |
| Local Mepid                     | 3                                    |
| Remote Mepid                    | 4                                    |
| Test ID                         | 1                                    |
| Priority                        | 7                                    |
| Source MAC Address              | 2C:39:C1:FE:9C:74                    |
| Target MAC Address              | 00:03:18:CD:58:D6                    |
| SLM Interval                    | 100ms                                |
| Count                           | 1201                                 |
| Duration (sec)                  | 120                                  |
| Iteration Count                 | 1                                    |
| Repeat Delay (minutes)          | 0                                    |
```


Copyright© 2022 Ciena® Corporation

```
| Repeat Flag                    | 0                                    |
| Rx Timeout                     | 5000                                 |
| Device TYpe                    | 0                                    |
| Configured Frame Size          | 64                                   |
| Fln Threshold                  | 10                                   |
| Flf Threshold                  | 10                                   |
| SD Set Threshold               | 44                                   |
| SD Clear Threshold             | 11                                   |
| Accelerated                    | No                                   |
| Config Accelerated             | No                                   |
+---------------------------- Last Test Result -------------------------+
| Iteration                      | 1                                    |
| Start                          | 01/01/2000 00:18:55                  |
| End                            | 01/01/2000 00:19:58                  |
| Duration (ms)                  | 63200                                |
| SLM Tx                         | 630                                  |
| SLR Rx                         | 630                                  |
| Frame Delivery Ratio           | 100.00%                              |
| Far Loss                       | 0                                    |
|    Ratio                       | 0.0000%                              |
|    Minimum                     | 0                                    |
|    Average                     | 0                                    |
|    Maximum                     | 0                                    |
| Near Loss                      | 0                                    |
|    Ratio                       | 0.0000%                              |
|    Minimum                     | 0                                    |
|    Average                     | 0                                    |
|    Maximum                     | 0                                    |
| Frame Size                     | 64                                   |
| Status                         | Start                                |
+----------------------------- Session Operation -----------------------+
| Total Request Tx               | 630                                  |
| Total Response Rx              | 630                                  |
| Total Far Loss                 | 0                                    |
| Total Near Loss                | 0                                    |
| TxFCl                          | 630                                  |
| TxFCfLast                      | 630                                  |
| TxFCfFirst                     | 1                                    |
| TxFCbLast                      | 1506946                              |
| TxFCbFirst                     | 1506317                              |
| RxFCl                          | 630                                  |
| RxFClStart                     | 1                                    |
| Fln Threshold Exceeded         | No                                   |
| Flf Threshold Exceeded         | No                                   |
| Session Duration (ms)          | 125000                               |
| Iteration Duration (ms)        | 125000                               |
| Active                         | Yes                                  |
| Persistent                     | No                                   |
| Tx Timer Set                   | Yes                                  |
| Wait Timer Set                 | No                                   |
| Tx Mode                        | Normal                               |
| Test History Wrapped           | No                                   |
+-------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-5
Displaying operational information for signal degrade enabled synthetic loss sessions

Display the operational information for signal degrade enabled synthetic loss sessions.

Step	Action

1 Display the operational information for signal degrade enabled synthetic loss sessions.

```
cfm signal-degrade synthetic-loss show service <service>
local-mepid <NUMBER: 1..8191> mepid <NUMBER: 1..8191>
test-id <NUMBER: 1..4294967295>
```

where

service <service>	is the name of the service (mandatory).
local-mepid <NUMBER: 1..8191>	is the local MEPID (mandatory).
mepid <NUMBER 1..8191>	is the remote mepid (optional)
test-id <NUMBER: 1..4294967295>	is the test ID (optional).

—end—

Example

The following example shows operational information for signal degrade enabled synthetic loss sessions:

```
> cfm signal-degrade synthetic-loss show service ma11 local-mepid 3 mepid 4
test-id 1

+----------------SIGNAL DEGRADE SYNTHETIC LOSS INFORMATION----------------+
|         |Local|Remote|        |           |Near End|Far End |Signal    |     |
|Service  |Mepid|Mepid |TestId  |Iteration  |Loss    |Loss    |Degraded  |Acc  |
+---------+-----+------+--------+-----------+--------+--------+----------+-----+
|ma11     |3    |4     |1       |0          |18      |18      | Yes      | No  |
+---------+-----+------+--------+-----------+--------+--------+----------+-----+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-6
Displaying historical information for signal degrade enabled synthetic loss sessions

Display historical information for signal degrade enabled synthetic loss sessions.

Step	Action
1	Display historical information for signal degrade enabled synthetic loss sessions. `cfm signal-degrade synthetic-loss show service <service> local-mepid <NUMBER: 1..8191> mepid <remote mepid> test-id <NUMBER: 1..4294967295> history` where service <service> is the name of the service (mandatory). local-mepid <NUMBER: 1..8191> is the local MEPID (mandatory). mepid <remote mepid> is the remote MEPID (optional) test-id <NUMBER: 1..4294967295> is the test ID (optional). history displays historical information (optional)

—end—

Example

The following example shows historical information for signal degrade enabled synthetic loss sessions:

```
> cfm signal-degrade synthetic-loss show service ma11 local-mepid 3 mepid 4
test-id 1 history
```


Copyright© 2022 Ciena® Corporation

```
+-------------------------SIGNAL DEGRADE SYNTHETIC LOSS MEASUREMENT HISTORY -------------------------+
|                           |                          |         |          |        |Signal  |Suspect |
|    Session Parameters     |           Time           |Iteration| Near Loss|Far Loss|Degraded|Interval|
+---------------------------+--------------------------+---------+----------+--------+--------+--------+
|RMEP ID: 4                 |Start: 01/01/2000 10:20:35|1        |0         |0       |No      |No      |
|TestId: 1                  |End:   01/01/2000 10:20:50|         |          |        |        |        |
|Priority: 7                |Duration (ms): 15086      |         |          |        |        |        |
|Interval: 100ms            |                          |         |          |        |        |        |
|Frame Size: 64             |                          |         |          |        |        |        |
+---------------------------+--------------------------+---------+----------+--------+--------+--------+
|RMEP ID: 4                 |Start: 01/01/2000 10:20:50|2        |0         |0       |No      |No      |
|TestId: 1                  |End:   01/01/2000 10:21:05|         |          |        |        |        |
|Priority: 7                |Duration (ms): 15087      |         |          |        |        |        |
|Interval: 100ms            |                          |         |          |        |        |        |
|Frame Size: 64             |                          |         |          |        |        |        |
+---------------------------+--------------------------+---------+----------+--------+--------+--------+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-7
Displaying signal degrade set and clear thresholds on a delay measurement session

Display the signal degrade set and clear thresholds for delay measurement sessions.

Step	Action

1 Display signal degrade set and clear thresholds:

```
cfm delay show service <service> local-mepid <NUMBER:
1..8191> mepid <NUMBER: 1..8191> test-id <NUMBER:
1..4294967295>
```

where

service <service>	is the name of the service.
local-mepid <NUMBER: 1..8191>	is the local MEPID.
mepid <NUMBER: 1..8191>	is the remote MEPID.
test-id <NUMBER: 1..4294967295>	is the test ID.

—end—

Example

The following example shows signal degrade set and clear threshold information for a delay measurement session:

```
> cfm delay show service dmm_sd1 local-mepid 100 mepid 101 test-id 1

+--------------------------- CFM DELAY SESSION INFO --------------+
| Parameter                           | Value                     |
+-------------------------------------+---------------------------+
| Service Name                        | dmm_sd_1                  |
| Service Index                       | 1                         |
| Local Mepid                         | 100                       |
| Remote Mepid                        | 101                       |
| Test ID                             | 1                         |
| Priority                            | 7                         |
| Drop Eligibility                    | 0                         |
| Source MAC Address                  | 2C:39:C1:03:12:23         |
| Target MAC Address                  | 74:87:BB:09:34:E3         |
| DMM Interval                        | 100ms                     |
| Count                               | 100                       |
| Duration (sec)                      | 9                         |
```


Copyright© 2022 Ciena® Corporation

```
| Iteration Count                      | 1                                |
| Repeat Delay (minutes)               | 0                                |
| Repeat Flag                          | 0                                |
| Rx Timeout                           | 5000                             |
| Device TYpe                          | 0                                |
| Configured Frame Size                | 64                               |
| Delay Threshold                      | -1                               |
| Jitter Threshold                     | -1                               |
| Max Delay Threshold                  | -1                               |
| Max Jitter Threshold                 | -1                               |
| Accelerated                          | No                               |
| Config Accelerated                   | No                               |
| Timestamp                            | Hardware                         |
| CoS Mode                             | No                               |
| SD Delay Clear Threshold             | 5                                |
| SD Delay Set Threshold               | 10                               |
| SD Jitter Clear Threshold            | 3                                |
| SD Jitter Set Threshold              | 5                                |
+---------------------------- Last Test Result -------------------+
| Iteration                            | 1                                |
| Start                                | 09/11/2019 05:19:58              |
| End                                  | 09/11/2019 05:20:13              |
| Duration (ms)                        | 14816                            |
| DMM Tx                               | 100                              |
| DMR Rx                               | 100                              |
| Avg Delay                            | 10                               |
| Min Delay                            | 9                                |
| Max Delay                            | 16                               |
| Avg Jitter                           | 1                                |
| Min Jitter                           | 0                                |
| Max Jitter                           | 6                                |
| Total Jitter                         | 115                              |
| Forward Avg Jitter                   | 0                                |
| Forward Min Jitter                   | 0                                |
| Forward Max Jitter                   | 4                                |
| Forward Total Jitter                 | 72                               |
| Backward Avg Jitter                  | 0                                |
| Backward Min Jitter                  | 0                                |
| Backward Max Jitter                  | 5                                |
| Backward Total Jitter                | 75                               |
| Frame Size                           | 68                               |
| Status                               | Start                            |
+---------------------------- Session Operation ------------------+
| Total DMM Tx                         | 100                              |
| Total DMR Rx                         | 100                              |
| Delay Threshold Exceeded             | No                               |
| Jitter Threshold Exceeded            | No                               |
| Max Delay Threshold Exceeded         | No                               |
| Max Jitter Threshold Exceeded        | No                               |
| Session Duration (ms)                | 14900                            |
| Iteration Duration (ms)              | 14900                            |
| Active                               | Yes                              |
| Persistent                           | No                               |
| Tx Timer Set                         | No                               |
| Wait Timer Set                       | Yes                              |
| Tx Mode                              | Normal                           |
| Test History Wrapped                 | No                               |
+-------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

DELAY MEASUREMENT RESULT BINS

Delay Result			Jitter Result		
Bin	Threshold (us)	Count	Bin	Threshold (us)	Count
0	0	100	0	0	99
1	5000	0	1	5000	0
2	10000	0	2	10000	0
3	15000	0			
				Forward	
			0	0	99
			1	5000	0
			2	10000	0
				Backward	
			0	0	99
			1	5000	0
			2	10000	0

Copyright© 2022 Ciena® Corporation

Procedure 3-8
Displaying operational information for signal degrade enabled delay measurement session

Display the operational information for signal degrade enabled delay measurement sessions.

Step	Action

1 Display the operational information for signal degrade enabled delay measurement session.

```
cfm signal-degrade delay show service <service> local-
mepid <NUMBER: 1..8191> mepid <NUMBER: 1..8191> test-id
<NUMBER: 1..4294967295>
```

where

service <service>	is the name of the service (mandatory).
local-mepid <NUMBER: 1..8191>	is the local MEPID (mandatory).
mepid <NUMBER 1..8191>	is the remote mepid (optional)
test-id <NUMBER: 1..4294967295>	is the test ID (optional).

—end—

Example

The following example shows operational information for signal degrade enabled delay measurement sessions:

```
> cfm signal-degrade delay show service ma11 serv100 local-mepid 10 mepid 20
test-id 1
```

```
+------------------------ SIGNAL DEGRADE DELAY MEASUREMENT INFORMATION -------------------------+
|                |Local|Remote|          |          |               |               |Signal   |   |
|service         |Mepid|Mepid |  TestId  |Iteration | Two-way Delay |Backward Jitter|Degraded|Acc|
+----------------+-----+------+----------+----------+---------------+---------------+--------+---+
|serv100         |10   |20    |1         |207       |            190|              6|No      |No |
+----------------+-----+------+----------+----------+---------------+---------------+--------+---+
```


Copyright© 2022 Ciena® Corporation

Procedure 3-9
Displaying historical information for signal degrade enabled for delay measurement sessions

Display signal degrade information for delay measurement sessions. You can retrieve information of the delay measurement sessions which are running on a given service-localMEP pair with a valid value of “sd-delay” and “sd-jitter” thresholds as follows:

- Service name
- Local MEPID
- Remote MEPID
- TestId
- Iteration
- Avg two-way delay
- Avg backward jitter
- Signal degrade state (yes/no)
- Suspect interval (yes/no)
- History

Step	Action
1	Display signal degrade information for delay measurement sessions: `cfm signal-degrade delay show service <String[1..45]> local-mepid <NUMBER 1..8191> [mepid <NUMBER: 1..8191>] [test-id <NUMBER” 1//4294967295>] [history]`

Example

The following example shows historical information for signal degrade enabled delay measurement sessions.

```
> cfm signal-degrade delay show service serv100 local-mepid 10 test-id 1
history
```


Copyright© 2022 Ciena® Corporation

DEGRADE DELAY MEASUREMENT INFORMATION

Session Parameters	Time	Iteration	Two-way Delay	Backward Jitter	Signal Degraded	Suspect Interval
RMEP ID: 20 TestId: 1 Priority: 7 Interval: 1sec Frame Size: 68	Start: 06/04/2019 12:53:47 End: 06/04/2019 12:54:21 Duration (ms): 34003	1	222	68	Yes	No
Session Parameters	Time	Iteration	Two-way Delay	Backward Jitter	Signal Degraded	Suspect Interval
RMEP ID: 20 TestId: 1 Priority: 7 Interval: 1sec Frame Size: 68	Start: 06/04/2019 12:54:21 End: 06/04/2019 12:54:56 Duration (ms): 34064	2	187	10	No	No

Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Ethernet Operations, Administration and Maintenance (EOAM) configuration

This chapter provides an overview of the IEEE 802.3ah Ethernet Operations, Administration and Maintenance (EOAM) and how to configure it.

> ***Note:*** In order to configure EOAM, you need to install the Advanced OAM (AOAM) license key. To obtain the Advanced-OAM license key, contact Ciena Sales.

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

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

The port will go into remote loopback mode when:

- EOAM is enabled globally.
- EOAM is enabled on the port.
- Loopback mode is initiated by the remote bridge.

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

Copyright© 2022 Ciena® Corporation

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

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

OAMPDUs are Slow Protocol frames. OAMPDUs must be standard length frames (64-1518 octets) and must be untagged. A maximum of 10 OAMPDUs may be sent per one second or per 100 msec, depending on the PDU timer. The 100 msec setting is non-standard, therefore the PDU timer should be kept at 1 second when interoperability is required with devices that do not support similar behavior.

Support of standard tools

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

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

FPGA hardware assist

Some ports have an FPGA that enables hardware assist for EOAM, and it affects the remote loopback operation.

When a port with no FPGA assist goes into remote loopback mode:

- No frames egress the port other than OAM BPDU frames which are identified by MAC DA=01:80:C3:00:00:02 and etype=88-09 and subtype=3.
- EOAM frames continue to egress the port at the same rate.
- All frames which ingress the port are dropped other than EOAM frames.

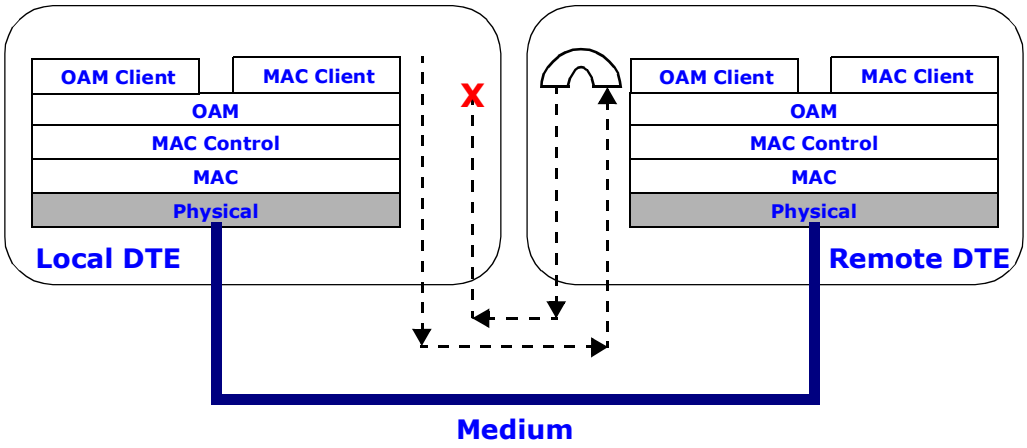
Copyright© 2022 Ciena® Corporation

- EOAM Loopback packets received on the port are sent out immediately on the same port and with no changes to the packet content. Loopback packets are identified by the MAC DA 01:80:C2:00:00:09.
- There is a limit to the number of loopback packets the system supports. At a minimum, the switch processes one loopback packet per port per second for all ports in remote loopback mode.
- Port statistics continue to function normally.

When a port with FPGA hardware assist goes into remote loopback mode:

- The port loops back all frames which ingress the port, except for EOAM frames which are identified by MAC DA=01:80:C3:00:00:02 and etype=88-09 and subtype=3.
- The port loops back all frames at line rate.
- No packets egress the port other than EOAM packets plus all packets which ingress the port and are looped back out.
- Port statistics do not function normally. Only EOAM packets are counted.

Figure 4-1
Operation of EOAM Remote Loopback



Link events

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

Copyright© 2022 Ciena® Corporation

Critical events

Critical events are generated for the following events:

- Dying Gasp: generated when
  - a reboot command is issued administratively
  - power is lost
  - there is a fatal software error

For the power is lost scenario, chassis dying gasp must be enabled for the EOAM Dying Gasp to be sent.

- Critical Link Event: generated when
  - unit temperature crosses above the configured threshold
  - unit temperature crosses below the configured threshold

Non-critical events

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

- Errored Frame Event: generated when the number of frame errors exceeds a threshold within a given window defined by a period of time, for example, 10 frames in 1 second had errors.
- Errored Frame Period Event: generated when the number of frame errors exceeds a threshold within a given window defined by a number of frames, for example, 10 frames out of 1000 had errors.
- Errored Frame Seconds Summary Event: generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a 1 second interval wherein at least one frame error is detected. Jabber, oversize, undersize, fragment and CRC errors are all monitored.

This chapter provides the following procedures for EOAM:

- "Enabling OAM on a port" on page 4-5
- "Enabling loopback" on page 4-9
- "Displaying EOAM information" on page 4-11

Copyright© 2022 Ciena® Corporation

Procedure 4-1
Enabling OAM on a port

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

Step	Action

1 Enable global EOAM on both devices:

```
eoam enable [port <port>]
```

where

port <port>	is the list of ports.

2 Display the current state of the selected port on the first device:

```
eoam show port <port> {link-events} {errd-events-
statistics} {event-log}
```

where

port <port>	is the port.
link-events	displays OAM link event configuration.
errd-events-statistics	displays link events statistics.
event-log	displays OAM event log for the specified port.

3 Set the selected port on the neighboring device to passive mode:

```
eoam set port <port> {critical-event <on|off>} {dying-
gasp <on|off>} {errd-frame-ev-notify <on|off>} {errd-
frame-window <#10..600>} {errd-frame-threshold
<#0..4294967293>} {errd-frame-period-ev-notify <on|off>}
{errd-frame-period-window <#1488..892857120>} {errd-
frame-period-threshold <#0..4294967293>} {errd-frame-
secs-summary <on|off>} {errd-frame-secs-threshold
<#0..65535>} {errd-frame-secs-window <#100..9000>}
{errd-frame-secs-threshold <#0..65535>} {errd-frame-
secs-window <#100..9000>} {errd-frame-secs-threshold
<#0..65535>} {link-lost-timer <#500..5000>} {mode
passive} {pdu-timer <#100..1000>}
```

where

port <port>	is the list of ports.
{critical-event <on | off>}	sets critical event.
dying-gasp <on | off>	sets dying gasp.

Copyright© 2022 Ciena® Corporation

where

errd-frame-ev-notify <on | off>	sets errored frame event notification.
errd-frame-window <DECISECONDS>	is the errored frame window. The default value is 10.
errd-frame-threshold <NUMBER: 0-4294967293>	is the errored frame threshold. The default value is 1.
errd-frame-period-ev-notify <on | off>	sets errored frame period event notification.
errd-frame-period-window <NUMBER: 1488-892857120>	is the errored frame period window.
errd-frame-period-threshold <NUMBER: 0-4294967293>	is the errored frame period threshold. The default value is 1.
errd-frame-secs-summary <on | off>	sets errored frame seconds summary event notification.
{errd-frame-secs-threshold <NUMBER: 0-65535>	is the errored frame seconds summary threshold.
errd-frame-secs-window <DECISECONDS>	is the errored frame seconds summary window.
errd-frame-secs-threshold <NUMBER: 0-65535>	is the errored frame seconds summary threshold.
errd-frame-secs-window <NUMBER: 100-9000>	is the errored frame seconds summary window. The default value is 60.
errd-frame-secs-threshold <NUMBER: 0-65535>	is the errored frame seconds summary threshold. The default value is 1.
link-lost-timer <MILLISECONDS: 500-5000>	is the link lost timer in milliseconds.
mode passive	sets OAM mode to passive.

Copyright© 2022 Ciena® Corporation

4 Enable OAM on the port:

```
eoam enable [[port <port>]
```

where

port <port>	is the port.

5 (Optional) Verify the configuration of the port.

```
eoam show <port> {link-events} {errd-events-statistics}
{event-log}
```

where

port <port>	is the port.
link-events	displays OAM link event configuration.
errd-events-statistics	displays link events statistics.
event-log	displays OAM event log for the specified port.

—end—

Example

The following example shows that port 7 is active.

```
> eoam show port 7
+--Global Oam Status --+
|        Disable       |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin|  Oper State  |Mode|OAM Func Support|  Info  |  Info  | Unkn |   Pdu Timer   |Link-lost Timer|
|    |State|              |    |UniD|Lb |Ev |Var|  PduTx |  PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+--------------+----+----+---+---+---+--------+--------+------+---------------+---------------+
|7   |Dis  |Disable       |Act |0   |0  |0  |0  |277     |0       |0     |1000           |5000           |
+----+-----+--------------+----+----+---+---+---+--------+--------+------+---------------+---------------+

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

> eoam enable
> eoam enable port 7
> eoam show port 7
+--Global Oam Status --+
|        Enable        |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin|  Oper State  |Mode|OAM Func Support|   Info   |  Info  | Unkn |   Pdu Timer   |Link-lost Timer|
|    |State|              |    |UniD|Lb |Ev |Var|  PduTx   |  PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+--------------+----+----+---+---+---+----------+--------+------+---------------+---------------+
|7   |En   |SendAny       |Act |0   |1  |1  |0  |288       |8       |0     |1000           |5000           |
+----+-----+--------------+----+----+---+---+---+----------+--------+------+---------------+---------------+

+----------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State  |Mode|OAM Func Support|Max OamPdu |      Peer Mac Address          | Faults |
|             |    |UniD|Lb |Ev |Var|   size    |                                |CE|DG|LF|
+-------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
|Active       |Pas |0   |1  |1  |0  |1518       |00:02:a1:30:a8:1d               |  |  |  |
+-------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
```


Copyright© 2022 Ciena® Corporation

The following example sets port 7 to passive mode.

```
> eoam show port 7
+--Global Oam Status --+
|       Disable        |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |   Pdu Timer   |Link-lost Timer|
|    |State|            |    |UniD|Lb |Ev |Var|  PduTx |  PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+------------+----+----+---+---+---+--------+--------+------+---------------+---------------+
|7   |Dis  |Disable     |Act |0   |0  |0  |0  |277     |0       |0     |1000           |5000           |
+----+-----+------------+----+----+---+---+---+--------+--------+------+---------------+---------------+

+---------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State |Mode|OAM Func Support|Max OamPdu |      Peer Mac Address          | Faults |
|            |    |UniD|Lb |Ev |Var|   size    |                                |CE|DG|LF|
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
|In-Active   |Unk |0   |0  |0  |0  |0          |00:00:00:00:00:00               |  |  |  |
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
> eoam enable
> eoam set port 7 mode passive
> eoam enable port 7
> eoam show port 7
+--Global Oam Status --+
|        Enable        |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin| Oper State |Mode|OAM Func Support|  Info  |  Info  | Unkn |   Pdu Timer   |Link-lost Timer|
|    |State|            |    |UniD|Lb |Ev |Var|  PduTx |  PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+------------+----+----+---+---+---+--------+--------+------+---------------+---------------+
|7   |En   |SendAny     |Pas |0   |1  |1  |0  |1233    |1259    |0     |1000           |5000           |
+----+-----+------------+----+----+---+---+---+--------+--------+------+---------------+---------------+

+---------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State |Mode|OAM Func Support|Max OamPdu |      Peer Mac Address          | Faults |
|            |    |UniD|Lb |Ev |Var|   size    |                                |CE|DG|LF|
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
|Active      |Act |0   |1  |1  |0  |1518       |00:02:a1:30:a8:1d               |  |  |  |
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
```


Copyright© 2022 Ciena® Corporation

Procedure 4-2
Enabling loopback

Enable loopback.

Step	Action

1 Display the current state of the selected port on the first device:

```
eoam show port <port> {link-events} {errd-events-statistics} {event-log}
```

where

port <port>	is the port.
link-events	displays OAM link event configuration.
errd-events-statistics	displays link events statistics.
event-log	displays OAM event log for the specified port.

2 Start loopback on the selected port:

```
eoam loopback start port <port>
```

where

port <port>	is the port.

3 (Optional) Verify the configuration of the port.

```
eoam show port <port> {link-events} {errd-events-statistics} {event-log}
```

where

port <port>	is the port.
link-events	displays OAM link event configuration.
errd-events-statistics	displays link events statistics.
event-log	displays OAM event log for the specified port.

4 View loopback statistics.

```
eoam loopback show
```

5 When you have completed troubleshooting, stop the OAM loopback:

```
eoam loopback stop port port <port>
```

where

port <port>	is the port.

—end—

Copyright© 2022 Ciena® Corporation

Example

The following example displays the state of port 7, and then enables the loopback on this port. This example assumes that the peer device/port has been enabled to participate in OAM loopback.

```
> eoam show port 7
+--Global Oam Status --+
|         Enable       |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin| Oper State |Mode|OAM Func Support| Info  | Info  | Unkn |    Pdu Timer   |Link-lost Timer|
|    |State|            |    |UniD|Lb |Ev |Var| PduTx | PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+------------+----+----+---+---+---+-------+-------+------+---------------+---------------+
|7   |En   |SendAny     |Act |0   |1  |1  |0  |2171   |2492   |0     |1000           |5000           |
+----+-----+------------+----+----+---+---+---+-------+-------+------+---------------+---------------+


+---------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State |Mode|OAM Func Support|Max OamPdu |      Peer Mac Address          | Faults |
|            |    |UniD|Lb |Ev |Var|   size    |                                |CE|DG|LF|
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
|Active      |Act |0   |1  |1  |0  |1518       |00:02:a1:30:a8:1d               |  |  |  |
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
> eoam loopback start port 7
> eoam show port 7
+--Global Oam Status --+
|         Enable       |
+----------------------+
+------------------------------------ Oam  Port  Statistics ------------------------------------+
|Port|Admin| Oper State |Mode|OAM Func Support| Info  | Info  | Unkn |    Pdu Timer   |Link-lost Timer|
|    |State|            |    |UniD|Lb |Ev |Var| PduTx | PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+------------+----+----+---+---+---+-------+-------+------+---------------+---------------+
|7   |En   |SendAny     |Act |0   |1  |1  |0  |2285   |2644   |0     |1000           |5000           |
+----+-----+------------+----+----+---+---+---+-------+-------+------+---------------+---------------+

+---------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State |Mode|OAM Func Support|Max OamPdu |      Peer Mac Address          | Faults |
|            |    |UniD|Lb |Ev |Var|   size    |                                |CE|DG|LF|
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
|Active      |Act |0   |1  |1  |0  |1518       |00:02:a1:30:a8:1d               |  |  |  |
+------------+----+----+---+---+---+-----------+--------------------------------+--+--+--+
CN 3928> eoam loopback show port 7
+------------------------------------ Oam Loopback Port Statistics ------------------------------------+
| Port |   Lb    |Lb Ignore|PeerLb |  LbPduTx   |    LbPduRx     |   LbPduRxError   | Lb Ctrl | Lb Ctrl |
|      | Status  |  State  |Support|            |                |                  |   Tx    |   Rx    |
+------+---------+---------+-------+------------+----------------+------------------+---------+---------+
|7     | Lb-Tx   |Process  | Yes   | 51         | 50             | 0                | 3       | 0       |
+------+---------+---------+-------+------------+----------------+------------------+---------+---------+
> eoam loopback stop port 7
```


Copyright© 2022 Ciena® Corporation

Procedure 4-3
Displaying EOAM information

Display EOAM information to verify EOAM configuration.

You can display:

- OAM statistics
- OAM link events
- OAM link events by port

When you display link events by port, the Oam Peer Port Info table includes the following information:

- CE, which is the number of Critical Events reported by the peer
- DG, which is the number of Dying Gasps reported by the peer
- LF, which is the number of Link Faults reported by the peer

Step	Action

To display OAM statistics

1 Display OAM statistics:

```
eoam show
```

To display OAM link events

2 Display OAM link events:

```
eoam show {link-events} {errd-events-statistics}
```

where

link-events	displays OAM link event configuration.
errd-events-statistics	displays link events statistics.

To display OAM link events by port

3 Display OAM link events by port:

```
eoam show port <port> {link-events} {errd-events-statistics} {event-log}
```

where

port <port>	port to show
link-events	show OAM link event configuration
errd-events-statistics	show link events statistics
event-log	show OAM event log for the specified port

Copyright© 2022 Ciena® Corporation

—end—

Example

The following example shows sample output for the eoam show port command.

```
> eoam show port 7
+--Global Oam Status --+
|         Enable       |
+----------------------+
+------------------------------------ Oam  Port  Statistics -------------------------------------+
|Port|Admin|  Oper State  |Mode|OAM Func Support| Info  | Info  | Unkn |   Pdu Timer   |Link-lost Timer|
|    |State|              |    |UniD|Lb |Ev |Var| PduTx | PduRx |CodeRx|(milli-seconds)|(milli-seconds)|
+----+-----+--------------+----+----+---+---+---+-------+-------+------+---------------+---------------+
|7   |En   |SendAny       |Act |0   |1  |1  |0  |2171   |2492   |0     |1000           |5000           |
+----+-----+--------------+----+----+---+---+---+-------+-------+------+---------------+---------------+


+---------------------  Oam  Peer Port  Info ----------------------------------------+
| Oper State  |Mode|OAM Func Support|Max OamPdu |     Peer Mac Address          | Faults |
|             |    |UniD|Lb |Ev |Var|   size    |                               |CE|DG|LF|
+-------------+----+----+---+---+---+-----------+-------------------------------+--+--+--+
|Active       |Act |0   |1  |1  |0  |1518       |00:02:a1:30:a8:1d              |  |  |  |
+-------------+----+----+---+---+---+-----------+-------------------------------+--+--+--+
```


Copyright© 2022 Ciena® Corporation

Two-Way Active Measurement Protocol

Two-Way Active Measurement Protocol (TWAMP) provides a way for network administrators to quickly measure latency and jitter between two devices with real-time processing. A TWAMP session must run between two different nodes. As each TWAMP session is initiated, a check is performed to ensure that this session is not aimed at an IP address or MAC address that belongs to the initiating node. This includes the IP addresses configured for the local interface, remote interface and any other configured IP interfaces. TWAMP can be run over IPv4 and IPv6 addresses.

> ***Note 1:*** TWAMP IPv4 configurations remain intact over a software upgrade or downgrade. TWAMP IPv6 configurations are removed during a downgrade.
>
> ***Note 2:*** It is the responsibility of the user to ensure that IP configuration data on the device is not changed while ANY feature (including TWAMP) is actively using that IP configuration data. For example, the user should not remove the IP address of any interface (remote or generic IP interface) that could be in use by an active TWAMP test session.

As defined in RFC4656, One-Way Active Measurement Protocol (OWAMP) measures uni-directional IP performance between two devices. Based upon OWAMP, TWAMP provides bi-directional measurements of IP performance between two devices through an exchange of test messages. The system software supports the following TWAMP modes:

- TWAMP Light Responder
- TWAMP Complete Server
- TWAMP Client

In order to ensure accurate time-stamping of response frames, it is recommended that you configure the NTP client to set the system date and time with a minimum of three configured NTP servers.

> ***Note 1:*** For additional information regarding NTP, refer to *39XX/51XX Switches and Platforms Administration and Security*.

Copyright© 2022 Ciena® Corporation

Note 2: Running TWAMP tests concurrently with benchmark (RFC 2544) tests can result in inaccurate TWAMP measurements, and might prevent the TWAMP tests from running at all. Disable benchmark testing before running TWAMP tests.

To maintain system performance, this implementation of TWAMP does not authenticate with the method described in the standard. Instead, you can implement access control to ensure the validity of TWAMP sessions. For information about access control, refer to *39XX/51XX Switches and Platforms Administration and Security*.

Note: TWAMP is not supported when the remote interface management access is provided over an MPLS VS.

Protocols

In compliance with the Internet Engineering Task Force (IETF) draft document, draft-ietf-ippm-twamp-06.txt, TWAMP Light Responder and Complete TWAMP use the TWAMP-Test protocol to exchange TWAMP test packets between the devices. Complete TWAMP uses a second protocol, TWAMP-Control to initiate, start, and stop a TWAMP test session.

Operational roles

In a TWAMP-Test session, devices operate in the following roles:

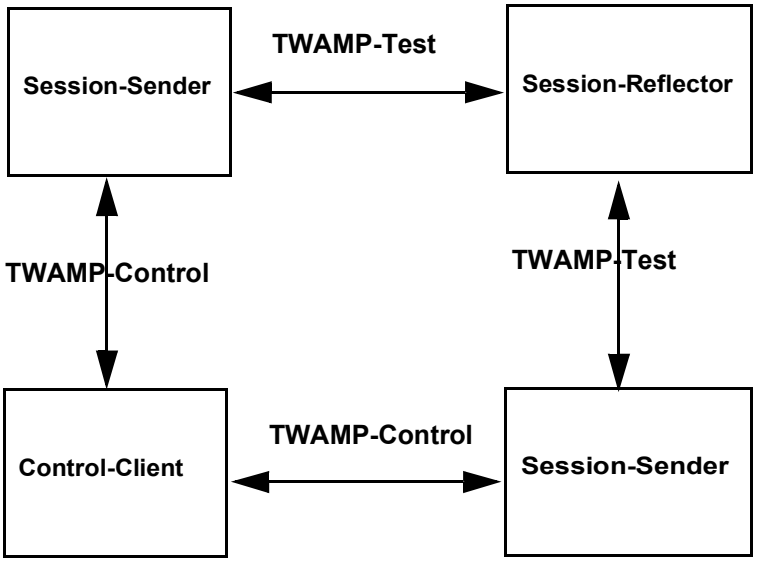
- Session-Sender - Endpoint device that sends TWAMP measurement packets.
- Session-Reflector - Endpoint device that receives TWAMP measurement packets with the ability to create and send TWAMP measurement packets in response.
- Server - Endpoint device that manages one or more TWAMP-Test sessions, including the state of the session endpoint devices.
- Control-Client - Endpoint device that initiates requests, triggers the start and stop of a test session.

Relationship Between Protocols and Operational Roles

Figure 5-1 illustrates the relationship between the TWAMP protocols and the operational roles and shows a potential implementation where four separate devices operate in each role.

Copyright© 2022 Ciena® Corporation

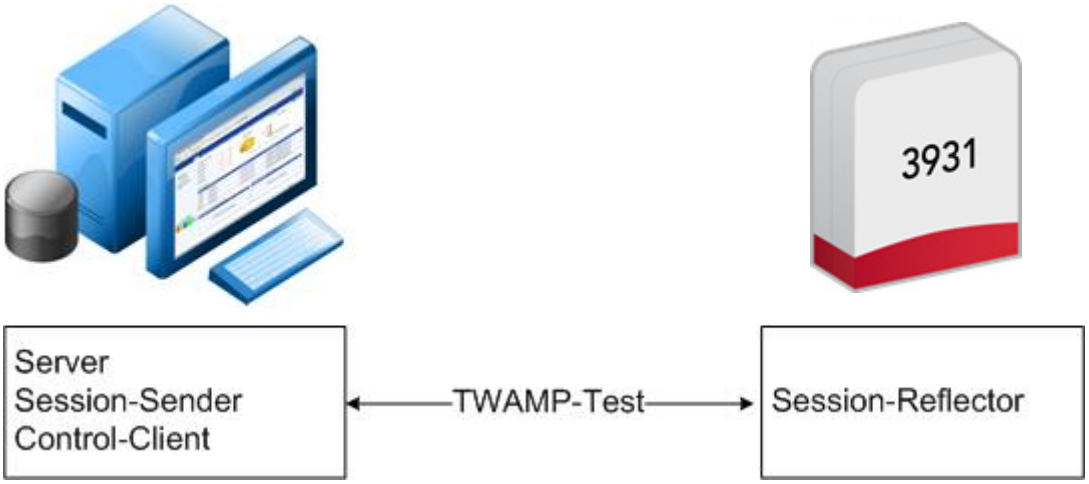
Figure 5-1
TWAMP relationships



TWAMP Light Responder

With TWAMP Light Responder mode, devices operate as Session-Reflectors only, and a performance management system operates in the Session-Sender, Control-Client, and Server roles. Figure 5-2 shows the relationship between the TWAMP-Test protocol and operational roles in TWAMP Light Responder.

Figure 5-2
TWAMP Light Responder relationships



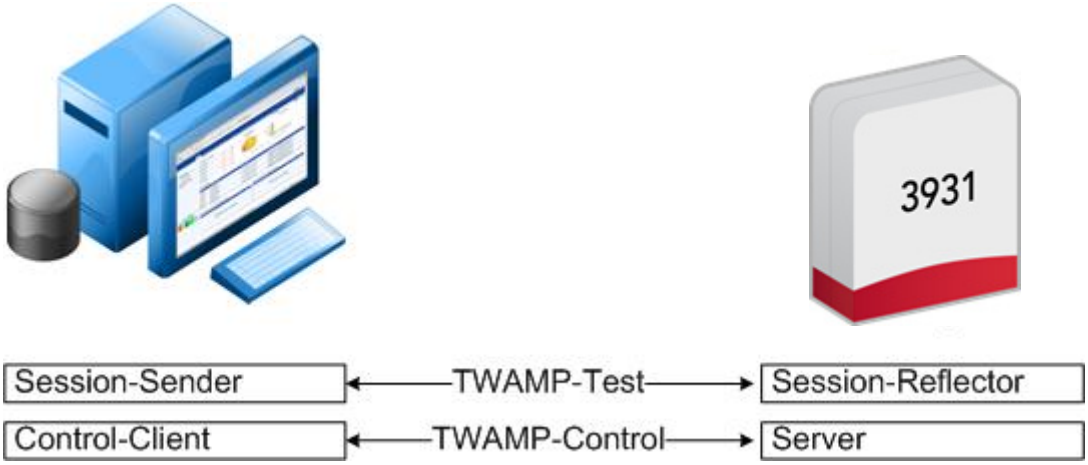
Copyright© 2022 Ciena® Corporation

While the TWAMP-Test session runs, the Session-Sender sends TWAMP-Test packets to the device. When incoming frames contain a UDP packet and the UDP destination port matches the device's configured active TWAMP port, the Session-Reflector processes the packets and returns response packets to the Session-Sender. After the exchange of test packets is complete, the Control-Client ends the session.

TWAMP Complete Server

With TWAMP Complete Server mode, devices operate as Session-Reflectors and Servers and a performance management system operates in the Session-Sender and Control-Client roles. Figure 5-3 illustrates the relationship between the TWAMP protocols and the operational roles in TWAMP Complete Server.

Figure 5-3
TWAMP Complete Server relationships



During a TWAMP session, the Server component recognizes an incoming TCP-based test session request, and configures itself for this test session. Responses are returned only to the control device that established the session. Any other incoming UDP test messages are dropped. Formal requests to establish a test session while one exists will be refused.

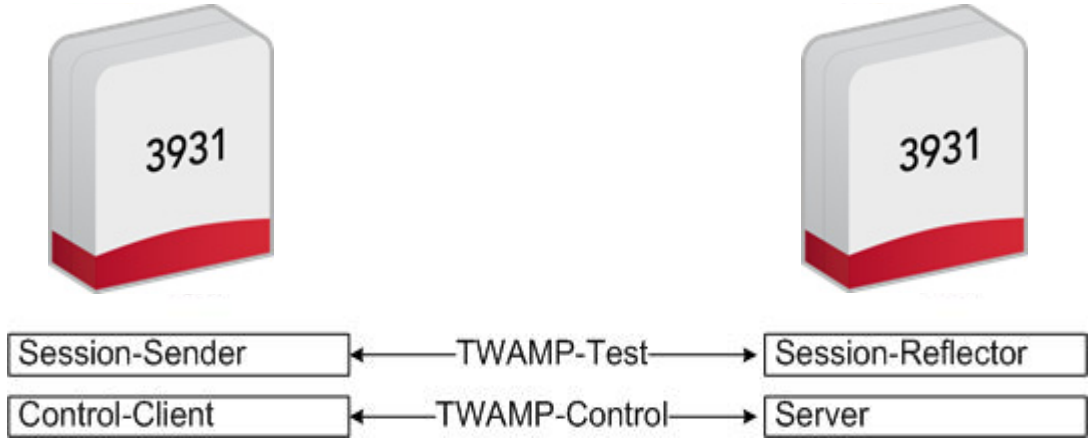
TWAMP Client

With TWAMP Client mode, devices operate as a Control-Client and a Session-Sender enabling the device to establish test sessions and generate test initiation messages. Devices may be used as test originators and manage multiple test sessions with multiple remote devices.

Copyright© 2022 Ciena® Corporation

Figure 5-4 illustrates the relationship between the TWAMP protocols and the operational roles where one device is operating in TWAMP Client mode and the other in TWAMP Complete mode.

Figure 5-4
TWAMP Client relationships



TWAMP-Test Packets

TWAMP supports variable sizes of TWAMP-Test packets, and can process a minimum of 1200 packets per minute. The Session-Sender packet follows the format shown in Figure 5-5.

Figure 5-5
TWAMP-Test packet format from Session-Sender

0 0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
Sequence Number																															
Timestamp																															
Error Estimate																															
Packet Padding																															

Copyright© 2022 Ciena® Corporation

The response packet format is shown in Figure 5-6.

Figure 5-6
TWAMP-Test Response Packet from Session-Reflector

0 0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
Sequence Number																															
Timestamp																															
Error Estimate																Must Be Zero															
Receive Timestamp																															
Sender Sequence Number																															
Sender Timestamp																															
Sender Error Estimate																Must Be Zero															
Sender TTL																															
Packet Padding																															

TWAMP server session deny

TWAMP server session deny allows you to configure a multi-NNI NTE to deny certain TWAMP sessions being negotiated and run over a specified port. Session-deny entries can be specified in both IPv4 and IPv6 format on the TWAMP server.

NNI ports are configured as though the node was part of a G.8032 ring, where any protection switch would cause the traffic from the down NNI port to be automatically switched to the protecting NNI port. You create a list of TWAMP server session deny elements by specifying the IP address of the interface associated with the NNI port and the ingress port number of the protecting port.

Control packets used to negotiate a test session are automatically sent to the CPU for processing by the TWAMP server. These control packets are checked against the server session deny entries for a match. In the case of a match, that is, while a protection switch is active, the packet is dropped and no test session is established.

Copyright© 2022 Ciena® Corporation

When hardware assist is not enabled, TWAMP test PDUs are also sent to the CPU and subjected to the same session deny check as control PDUs. Therefore, if the protection switch happens after the session has been negotiated, the test PDU is dropped when the appropriate session deny entry is programmed.

When hardware assist is enabled on the server and a protection switch happens after the session has been negotiated and started, test PDUs are not sent to the CPU; they are handled by the FPGA. In this case, upon receiving a protection switch notification, the TWAMP server disables any active test sessions that match the NNI port that went down.

When hardware assist is enabled on the server, the session deny functionality is tied to the ring protection mechanism by means of the protection switch event. Therefore, it is important that the RPL be properly set on the virtual ring in order for active test sessions to be canceled when the main port of the ring is blocked because of a forced switch or the port going down.

Aggregated port IDs cannot be used as a port in a TWAMP session deny entry; only physical ports are allowed. It is also not possible to add a physical port that is a member of an aggregated port as the port in a session deny entry. Similarly, a port that is used in a session deny entry cannot be added to an aggregate port.

This chapter provides the following procedures to configure TWAMP:

- “Configuring global TWAMP attributes” on page 5-9
- “Enabling TWAMP” on page 5-11
- “Displaying TWAMP information” on page 5-12
- “Enabling TWAMP Light Responder” on page 5-14
- “Enabling TWAMP complete server” on page 5-15
- “Enabling TWAMP client” on page 5-16
- “Creating a TWAMP client session” on page 5-17
- “Displaying TWAMP client sessions” on page 5-20
- “Updating a TWAMP client session” on page 5-22
- “Deleting a TWAMP client session” on page 5-23
- “Establishing and stopping a test session” on page 5-24
- “Displaying and clearing TWAMP client statistics” on page 5-28
- “Displaying active TWAMP server sessions on the target device” on page 5-29
- “Clearing a TWAMP server session on the target device” on page 5-30

Copyright© 2022 Ciena® Corporation

- “Displaying TWAMP configuration in the configuration file” on page 5-31

Copyright© 2022 Ciena® Corporation

Procedure 5-1
Configuring global TWAMP attributes

The global TWAMP client DSCP and server DSCP entries set the respective DSCP values in TCP messages used for control session communications. It is not possible to configure the DSCP setting for the TCP packets on a per-session basis.

Table 5-1 describes support for hardware-assisted TWAMP by platform.

Table 5-1
Support for hardware-assisted TWAMP by platform

Platform	Support for hardware-assisted TWAMP
3903, 3903x, 3904, 3905, 3906, 3924, 3942 and 5142	all ports
3926	all ports except port 4 (which must be in OAM services mode for HW support)
3928	all ports except port 7 (which must be in OAM services mode for HW support)
5160	all ports except port 20 (which must be in OAM services mode for HW support)

Step	Action

To set the global TWAMP attributes

1 Set the global TWAMP attributes:

```
twamp set [client-dscp <NUMBER: 0-63>] [client-hw-assist
<on|off>] [server-dscp <NUMBER: 0-63>] [server-hw-assist
<on|off>] [port <NUMBER: 256-65535>] [timeout <NUMBER:
60-86400>]
```


Copyright© 2022 Ciena® Corporation

where

client-dscp <NUMBER: 0-63>	is the TWAMP Client TCP DiffServ Code Point. The default value is 0.
client-hw-assist <on|off>	indicates whether to use client hardware assist.
server-dscp <NUMBER: 0-63>	is the TWAMP Server TCP DiffServ Code Point. The default value is 0.
server-hw-assist <on|off>	indicates whether to use server hardware assist.
port <NUMBER: 256-65535>	is the TWAMP TCP/UDP port. The default value is 861. When setting the port, select the port setting defined in the performance management system for testing devices.
timeout <NUMBER: 60-86400>	is the TWAMP Server TCP session timeout in seconds. The default value is 90 seconds.

To reset the port and timeout attributes to their default values

2 Reset the port and timeout attributes to their default values:

```
twamp unset {[port],[timeout]}
```

—end—

Examples

The following example sets the active TWAMP port to 5678.

```
> twamp set port 5678
```

The following example resets the port and timeout attributes to their default values.

```
> twamp unset port timeout
```


Copyright© 2022 Ciena® Corporation

Procedure 5-2
Enabling TWAMP

By default, TWAMP is disabled at the global level. When you enable TWAMP at the global level, then it is automatically enabled for all ports.

Step	Action
To enable globally	
1	Enable globally: `twamp enable`
To enable per port	
2	Enable per port: `twamp enable [port <PhyPortNameList>]`
To disable globally	
3	Disable globally: `twamp disable`
To disable per port	
4	Disable per port: `twamp disable [port <PhyPortNameList>]`

—end—

Examples

The following example enables TWAMP on port 15.

```
> twamp enable port 15
```

The following example disables TWAMP on port 15.

```
> twamp disable port 15
```


Copyright© 2022 Ciena® Corporation

Procedure 5-3
Displaying TWAMP information

You can display the global state, per port state, and active TWAMP port. Optionally, you can display the setting for the active TWAMP port only.

You can display:

- TWAMP settings on the device
- all active sessions on the server
- all server session-deny entries

Step	Action

To display TWAMP settings on the device

1 Display TWAMP settings on the device:

```
twamp show
```

To display all active sessions on the server

2 Display all active sessions on the server:

```
twamp server show
```

To display all server session-deny entries

3 Display all server session-deny entries currently configured and statistics on the number of denied packets for each entry:

```
twamp server session-deny show
```

—end—

Example

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

```
> twamp show
+---------  TWAMP State Info  -------+
|       Parameter        |    Value   |
+------------------------+------------+
| Device Admin State     |  Disabled  |
| Client                 |  Disabled  |
| Server                 |  Disabled  |
| Light Reflector        |  Disabled  |
| Client HW Assist       |         On |
| Server HW Assist       |         On |
+------------------------+------------+
+--------- Active TWAMP Port --------+
| TCP/UDP Port     |  861             |
+------------------+------------------+
+----TWAMP Server Session Timeout----+
|    Timeout       |      90 seconds  |
+------------------+------------------+
```


Copyright© 2022 Ciena® Corporation

```
+-------- TWAMP DSCP Settings -------+
| Client TCP DSCP |  0                |
| Server TCP DSCP |  0                |
+-----------------+-----------------+
+-----------------------------------+
|      Per Port TWAMP State Info    |
+--------+-----------+--------------+
|  Port  |   Admin   |  Operational |
+--------+-----------+--------------+
|    1   |  Enabled  |   Disabled   |
|    2   |  Enabled  |   Disabled   |
|    3   |  Enabled  |   Disabled   |
|    4   |  Enabled  |   Disabled   |
|    5   |  Enabled  |   Disabled   |
|    6   |  Enabled  |   Disabled   |
|    7   |  Enabled  |   Disabled   |
|    8   |  Enabled  |   Disabled   |
|    9   |  Enabled  |   Disabled   |
|   10   |  Enabled  |   Disabled   |
|   11   |  Enabled  |   Disabled   |
|   12   |  Enabled  |   Disabled   |
+--------+-----------+--------------+
```

The following example shows sample output for the twamp server session-deny show command.

```
> twamp server session-deny show
+-------------------- TWAMP Session Deny ----------------------+
|                                      | Ingress |              |
| IP Address                           | Port    | Dropped Pkts |
+--------------------------------------+---------+--------------+
| 192.168.50.2                         | 1       | 0            |
| 2001::db8:f018:1:202:5aff:fe01:b449  | 1       | 0            |
+--------------------------------------+---------+--------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 5-4
Enabling TWAMP Light Responder

You can disable or enable the TWAMP Light Responder state globally. By default TWAMP Light Responder is disabled.

Step	Action

To disable globally

1 Disable globally:

```
twamp light disable
```

To enable globally

2 Enable globally:

```
twamp light enable
```

—end—

Example

The following example disables the TWAMP Light Responder state globally.

```
> twamp light disable
```

The following example enables the TWAMP Light Responder state globally.

```
> twamp light enable
```


Copyright© 2022 Ciena® Corporation

Procedure 5-5
Enabling TWAMP complete server

You can disable or enable the TWAMP Complete Server state globally. By default, TWAMP Complete Server is disabled.

> ***Note:*** Up to 30 “used” sessions (client, server, or combination of both) are supported. A client session is counted as a “used” session, as soon as it is configured. For a server session, it counts as “used” when a session request is received on the local node from a remote client.

Step	Action
To disable globally	
1	Disable globally: `twamp server disable`
To enable globally	
2	Enable globally: `twamp server enable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 5-6
Enabling TWAMP client

You can disable or enable the TWAMP Client state globally. By default, TWAMP Client is disabled. Before you can create any sessions, you must enable the TWAMP Client. In order for the session to start with a target, the target must be configured to support TWAMP Complete Server. On devices running this system software, you need to enable TWAMP Complete Server.

> ***Note:*** TWAMP Client cannot be disabled with existing TWAMP sessions, as each session has memory allocated to it for statistics gathering. Before the disable command will be accepted, delete all sessions. To stop a test, run the `twamp client test stop` command.

Step	Action
To enable globally	
1	Enable globally: `twamp client enable`
To disable globally	
2	Disable globally: `twamp client disable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 5-7
Creating a TWAMP client session

Client sessions always originate from the remote-interface IP address, but can be targeted at a server IP address which is either the server device's remote interface address, or any of the server device's ip-interface addresses. The server address for a session may be an IPv4 or an IPv6 address. When an IPv6 address is used, it may be specified in either full or abbreviated notation.

The TWAMP client may have several IP addresses, but it must have a remote-interface IP address in the same subnet as the targeted server address. This will be used as the source IP address for the test session. If the client has no remote-interface IP address in the same subnet, the session will not run successfully. The client can concurrently source some test sessions from the IPv4 remote-interface address and other sessions from a remote-interface IPv6 address.

Two IP interfaces on the same TWAMP server device may share the same link-local IPv6 address. When using an IPv6 link-local address for a session, which server IP interface the session is received on is dependent on which client interface the session is scoped from. Client sessions are always scoped from the remote interface.

A TWAMP server can concurrently receive and respond to some test sessions that use IPv4 addresses and other test sessions that use IPv6 addresses.

When configuring a TWAMP session to an IP interface ensure that the MTU of the interface is set large enough to accommodate the size of test packet selected for this TWAMP session.

When creating a TWAMP Client session, choose a fixed interval test packet stream or a Poisson distribution packet stream. You can specify that the packets are marked with a CoS policy and priority value, 802.1d (0 to 7), IP Precedence (0 to 7) or Differentiated Services Code Point (DSCP) values (0 to 63, to measure “Real Time” and “Best Effort” paths across the network.

The DSCP/IP-Prec settings of the TWAMP Test (UDP) packets cannot be set on the server. The server always sends test packet responses with the same DSCP/IP-Prec as the test request packet being responded to. The TWAMP Client sets the DSCP/IP-Prec values on the TWAMP Test (UDP) packets on an individual test session basis.

For each client session that is configured, there is a cos-policy [ip-prec | dscp] parameter. The other two parameters that can be configured for this session are ip-prev value <0...7> and dscp value <0...63>. The cos-policy setting

Copyright© 2022 Ciena® Corporation

determines which of these other two parameters will be used in the session. If a session is configured to use an IPv6 address on the targeted host, then the IP-Prec settings are irrelevant. If an IPv6 address is configured as the target host address, then the value of the cos-policy parameter is ignored and the dscp value configured under the dscp parameter is always used.

A packet size can be configured for the session. This is the size of the TWAMP test packet only. It does not include Ethernet encapsulation. The range for this parameter is 64 to 1500 bytes. The minimum size of the 64 bytes is only valid for sessions that use IPv4 addressing. For the sessions that use IPv6 addressing, the minimum packet size that can be configured is 84 bytes.

> ***Note:*** Up to 30 "used" sessions (client, server, or combination of both) are supported. A client session is counted as a "used" session, as soon as it is configured. For a server session, it counts as "used" when a session request is received on the local node from a remote client.

Table 5-2 shows the attributes of the supported packet streams.

Table 5-2
Packet Stream Attributes

Packet Stream Type	Inter-packet Frequency	Packet Size	CoS Marking	Cycle Time
Fixed Interval	100ms	Variable - 64-1500 byte test messages.	2 shared among test sessions and denoted by 802.1d (0-7), IP precedence (0-7) or DSCP (0-63) values.	Variable depending upon number of packets. For every 9,000 packets, the cycle is 15 minutes.
Poisson Distribution	Average 3.3s, 300ms to 12s	Fixed - 238 bytes	4 shared among test sessions and denoted by 802.1d (0-7), IP precedence (0-7) or DSCP (0-63) values.	Variable depending upon number of packets. For every 9,000 packets, the cycle is 15 minutes.

Copyright© 2022 Ciena® Corporation

Step	Action
1	Create a TWAMP client session: `twamp client session create name <String [15]> host <IpAddress> [commport <TCP/UDP port to use if different from global>] [cos-policy <dscp|ip-prec>] [dot1dpri <NUMBER:1-7>] [dscp <NUMBER: 0-63>] [ip-prec <NUMBER: 0-7>] [pkt-size <NUMBER: 64-1500>] [repeat <on|off>] [type <fixed|poisson>] [packets <272-1000000>]` **—end—**

Example

The following example creates a TWAMP client test session for IPv4.

```
> twamp client session create name myTest host 192.168.12.34
cos-policy ip-prec ip-prec 7 repeat off type fixed
```

The following example creates a TWAMP client test session for IPv6. It is not necessary to specify cos-policy setting on an IPv6 session. Cos-policy setting is always fixed as dscp for IPv6, and dscp is the default, so it does not have to be actively set.

```
> twamp client session create name myTest2 host
2001:db8:f018:1:202:5aff:fe01:b449 repeat off type fixed
```


Copyright© 2022 Ciena® Corporation

Procedure 5-8
Displaying TWAMP client sessions

Table 5-3 lists attributes displayed in the TWAMP client session list.

Table 5-3
Attributes for the TWAMP client session

Field	Description
Name	Name of the session.
Ip Addr	Host IP address.
State	Test state. For example, Idle or Test.
Port	TCP/UDP communications port setting.
1D	802.1d setting.
CoS	CoS Policy: • I - IP precedence. • D - DSCP
DSCP	DSCP setting.
IPP	IP precedence setting.
Size	Packet size.
RPT	Repeat setting: • Y - On • N - Off
Type	Packet stream type: • Fix - Fixed • Pois - Poisson
Packets	Number of packets.
TX	Y means that TWAMP test packets are transmitted using hardware assist, otherwise this field is blank.
RX	Y means that TWAMP test packets are received using hardware assist, otherwise this field is blank.
Seq#	Sequence number of the last test packet.

Copyright© 2022 Ciena® Corporation

Step	Action
1	Display TWAMP Client sessions: `twamp client show`

—end—

Example

The following example shows sample output for the twamp client show command.

```
+-----------------------------------------------------------------------------------------------------+
|                                   TWAMP Client Sessions                                             |
+---------+----------------------------------+-----+-----+--+---+----+---+----+---+----+-------+--+----+
| Name    |     IP Addr                      |State| Port|1D|CoS|DSCP|IPP|Size|RPT|Type|Packets|HW|Seq#|
+---------+----------------------------------+-----+-----+--+---+----+---+----+---+----+-------+--+----+
| fred    |2001:db8:f018:1:202:5aff:fe01:b449| Idle|  861| 7| I |  0 | 0 | 142| N | Fix|   272 |  | 0  |
+-----------------+-------------------------------------------------------------------------------|----+
| bert    |2001:db8:f018:1:202:5aff:fe01:b449| Idle|  861| 7| I |  0 | 0 | 142| N | Fix|   900 |  | 0  |
+---------+----------------------------------+-----+-----+--+---+----+---+----+---+----+-------+--+----+
```


Copyright© 2022 Ciena® Corporation

Procedure 5-9
Updating a TWAMP client session

Update a TWAMP client session.

Step	Action
1	Update a TWAMP Client session: `twamp client session set name <SessionName> {[host <IpAddress>], [commport <TCP/UDP port to use if different from global>], [cos-policy <dscp|ip-prec>], [dot1dpri <NUMBER:1-7>], [dscp <NUMBER: 0-63>], [ip-prec <NUMBER: 0-7>], [pkt-size <NUMBER: 64-1500>], [repeat <on|off>], [type <fixed|poisson>], [packets <272-1000000>]}` **—end—**

Example

The following example updates a TWAMP client session.

```
> twamp client session set name myTest type poisson
```


Copyright© 2022 Ciena® Corporation

Procedure 5-10
Deleting a TWAMP client session

Delete a TWAMP client session.

Step	Action
1	Delete a TWAMP Client session: `twamp client session delete name <SessionName>`

—end—

Example

The following example deletes a TWAMP client session.

```
> twamp client delete name myTest
```


Copyright© 2022 Ciena® Corporation

Procedure 5-11
Establishing and stopping a test session

While TWAMP Client tests are in session, the device continues to respond to incoming TWAMP test sessions.

Step	Action
1	Establish or stop a TWAMP Client session: `twamp client test name <SessionName> [host <IpAddress>] [stop]`

—end—

Examples

The following example establishes a session.

```
twamp client test name myTest
```

The following example stops a session.

```
twamp client test name myTest stop
```


Copyright© 2022 Ciena® Corporation

Procedure 5-12
Configuring TWAMP server session deny

You can instruct the TWAMP server to deny sessions associated with one NNI link from being carried over the other NNI link by creating a list of TWAMP server session deny elements.

Session-deny entries must be added for any remote interface IP address that are targeted by the Worldwide IP Measurement (WIPM) client towards a TWAMP server. For example, if the TWAMP sessions are targeted at the servers with IPv4 and IPv6 remote interface IP addresses, three session-deny entries are required for each of these three remote interface IP addresses that could be the target of a TWAMP session on the server node.

The list of TWAMP server session deny elements can contain up to four entries.

You can:

- add a TWAMP server session-deny entry
- change the ingress port for a session-deny entry
- remove a session-deny entry
- clear the statistics for all session-deny entries

Step	Action

To add an entry to the server session deny table

1 Add an entry to the server session deny table:

```
twamp server session-deny ip <IP address> port <phys-port>
```

where

ip <IP address>	is the IP address of the interface associated with the NNI port.
port <phys-port>	is the physical port.

To change the ingress port for a session-deny entry

2 Change the ingress port for a specified session-deny entry:

```
twamp server session-deny set ip <IP address> port <phys-port>
```

where

ip <IP address>	is the interface associated with the NNI port.
port <phys-port>	is the physical port.

Copyright© 2022 Ciena® Corporation

To remove a session-deny entry

3 Remove a specified server session-deny entry:

```
twamp server session-deny remove ip <IP address>
```

where

ip <IP address> is the interface associated with the NNI port.

To clear the statistics for all session-deny entries

4 Clear the statistics for all session-deny entries:

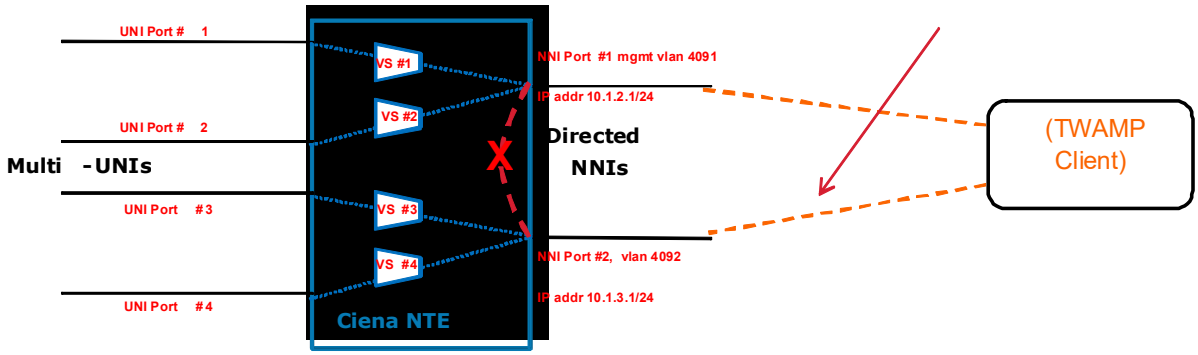
```
twamp server session-deny clear statistics
```

—end—

Example

Figure 5-7 shows a multi-UNI, multi-NNI NTE system. Each NNI uplink is to be monitored using separate TWAMP sessions. A single unique VLAN is assigned to each of the NNI uplink ports. One of the uplinks is associated with the network management VLAN while the other is allocated to another VLAN.

Figure 5-7
Sample multi-UNI, multi NNI NTE setup



An element in the session deny list is added to deny any session request for IP address 10.1.2.1 (address associated with NNI #1) that arrives on port NNI #2.

The following example configures TWAMP server session deny for the configuration shown in Figure 5-7.

Configure VLANs and IP interfaces.

```
vlan create vlan 4091,4092
vlan add vlan 4092 port 9-10
vlan add vlan 4091 port 9-10
```


Copyright© 2022 Ciena® Corporation

```
interface create ip-interface backup-mgmt ip 10.1.3.1/24
vlan 4092
interface remote set ip 10.1.2.1/24 vlan 4091
```

Configure the G.8032 ring.

```
mstp disable port 9,10
rstp disable port 9,10
ring logical-ring create logical-ring-name lr-multiNNI
ring-id 1 east-port 9 west-port 10
ring virtual-ring create virtual-ring-name RemoteIfRing
vr-multiNNI logical-ring lr-multiNNI raps-vid 100
ring virtual-ring create virtual-ring-name IpIfRing
logical-ring lr-multiNNI raps-vid 101
ring virtual-ring set ring RemoteIfRingvr-multiNNI west-
port-rpl owner
ring virtual-ring set ring IpIfRing east-port-rpl owner
ring virtual-ring add ring RemoteIfRing vid 4091
ring virtual-ring add ring IpIfRing vid 4092
```

Configure TWAMP server session deny.

```
twamp enable
twamp server enable
twamp server session-deny ip 10.1.3.1 port 9
twamp server session-deny ip 10.1.2.1 port 10
```


Copyright© 2022 Ciena® Corporation

Procedure 5-13
Displaying and clearing TWAMP client statistics

TWAMP Client test statistics are collected and stored. Statistics are collected and made available at the completion of each test session. For a TWAMP Client session that is set to “repeat”, statistics will be collected and stored at the completion of each iteration. Statistics can be stored for a maximum of 96 iterations of each test session. The statistics storage area works in a First In, First Out fashion. Statistics are stored in RAM and are lost upon reboot.

Step	Action

To display TWAMP Client statistics

1 Display TWAMP Client statistics:

```
twamp client show [statistics [name <SessionName>] [mode
<long|short>] [period <last|8-hour| 24-hour>]]
```

To clear TWAMP Client statistics

2 Clear TWAMP Client statistics:

```
twamp client clear statistics {name <SessionName>|all}
```

—end—

Example

The following example displays statistics for “myTest”:

```
> twamp client show statistics name myTest

+---------------+---------+-----------+----+----+----+----+---------------+
|     Name      | RT 95th | RT 99.9th | Tx | Rx | RL | OL |Completion Time|
+---------------+---------+-----------+----+----+----+----+---------------+
| myTest        |   0.312 |    0.410  | 272| 272|   0|   0| 08/ 5/08 21:29|
+---------------+---------+-----------+----+----+----+----+---------------+
```

The following example clears statistics for “myTest”:

```
> twamp client clear statistics name myTest
```


Copyright© 2022 Ciena® Corporation

Procedure 5-14
Displaying active TWAMP server sessions on the target device

You can display active server sessions on target devices running this system software.

Step	Action
1	Display the test session on the target: `twamp server show`

—end—

Example

The following example shows sample output for the twamp server show command.

```
> twamp server show

+-------------------------------------------------------------------------+
|                     TWAMP Server Ctrl Sessions                          |
+----+--------+---------------------------------------+--------+----------+
| ID |  State |          Host IP                      |  Port  | Test Sessions|
+----+--------+---------------------------------------+--------+----------+
|  1 |   Test | 2001::f018:1:202:5aff:fe01:b449       | 48970  | 1        |
|  2 | Listen | fe80::202:5aff;fe01:d16f              | 87564  | 2        |
| 29 | Listen | 0.0.0.0                               |     0  |          |
| 30 | Listen | 0.0.0.0                               |     0  |          |
+----+--------+---------------------------------------+--------+----------+


+-------------------------------------------------------------------------------+
|                      TWAMP Server Test Sessions                               |
+---+------+----------+-----------------------------------+------+-----------+---+
| ID| State| Src Port |    Host IP                        | Pkts |  SeqNum   |HW |
+---+------+----------+-----------------------------------+------+-----------+---+
| 1 | Test | 46517    | 2001:db8:f018:1:202:5aff:fe01:b449|  272 |        22 |   |
| 2 | Test | 87565    | fe80::202:5aff:fe01:d16f          |  900 |        75 |   |
|29 | Idle |       0  |                   0.0.0.0         |    0 |         0 |   |
|30 | Idle |       0  |                   0.0.0.0         |    0 |         0 |   |
...
+---+------+----------+-----------------------------------+------+-----------+---+
```


Copyright© 2022 Ciena® Corporation

Procedure 5-15
Clearing a TWAMP server session on the target device

You can force a TWAMP server session down from the target devices running this system software.

Step	Action
1	Clear a session: `twamp server clear session <NUMBER: 1-30>`

—end—

Example

The following example clears session 1.

```
> twamp server clear session 1
```


Copyright© 2022 Ciena® Corporation

Procedure 5-16
Displaying TWAMP configuration in the configuration file

TWAMP configuration is saved to the configuration file in the TWAMP CONFIG: section.

Step	Action
1	Display TWAMP configuration in the configuration file: `configuration show`

—end—

Example

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

```
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! TWAMP CONFIG:
!
twamp set port 5678
twamp enable
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

System performance testing with RFC2544 and Y.1564 benchmark services

This chapter explains how to configure and run benchmark services for monitoring system performance based on RFC2544 and Y.1564 testing methodology.

Benchmark services allow generic benchmarking and performance analysis for Ethernet network devices and end-to-end testing of networks. Benchmark services provide consistent measurement and reporting of Y.1564 and RFC2544 test results.

Topics are:

- "Benchmarking test types" on page 6-1
- "Operational roles" on page 6-7
- "Benchmark statistics" on page 6-14
- "Test results" on page 6-17
- "Benchmark NETCONF" on page 6-17

Benchmarking test types

Benchmarking test types are:

- "Throughput test" on page 6-2
- "Frame loss test" on page 6-2
- "Latency test" on page 6-3
- "Packet delay variation test" on page 6-3
- "Outage test" on page 6-4
- "RFC2544 test" on page 6-4
- "Y.1564 test" on page 6-4

Copyright© 2022 Ciena® Corporation

Additionally, this section discusses

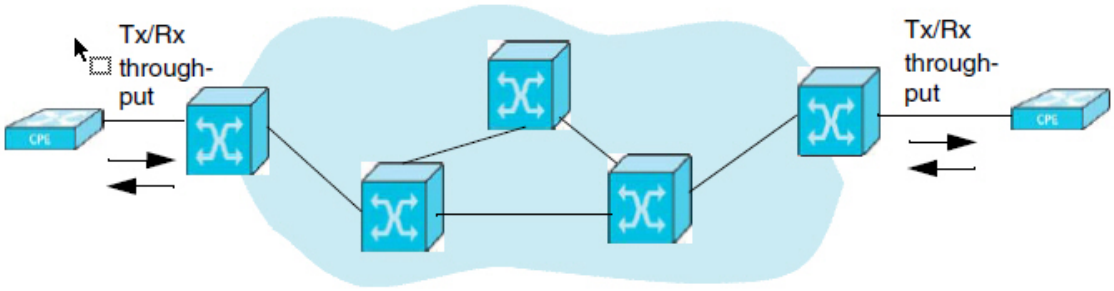
- “Test profile” on page 6-6
- “Test instance” on page 6-6

Throughput test

The throughput test defines the maximum number of frames per second that can be transmitted without any error and dropped packets. The throughput test measures the rate-limiting capability of carrier Ethernet services in a network.

Figure 6-1 shows an example of a throughput test in a network.

Figure 6-1
Throughput test



Frame loss test

The frame loss test measures the network’s response in overload conditions, which is a critical indicator of the network’s ability to support real-time applications in which a large amount of frame loss will rapidly degrade service quality.

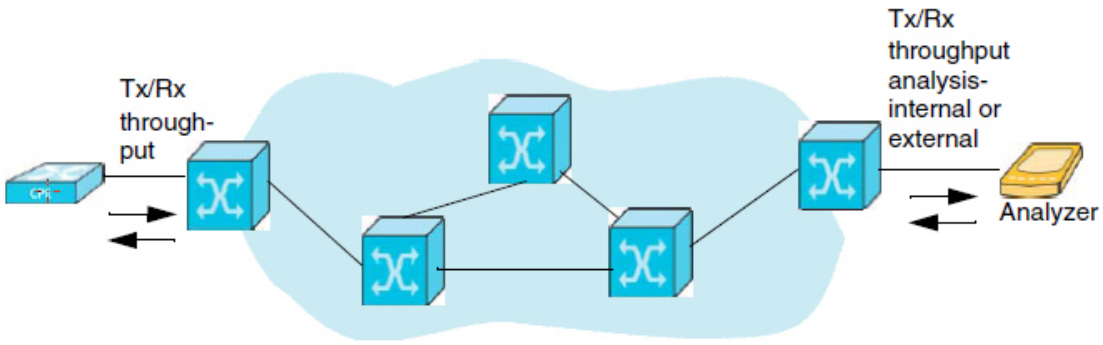
When RFC2544 is enabled, the 39XX/51XX sends traffic at the maximum line rate and then measures to determine whether the network dropped any frames. The sequence continues at reducing ten per cent intervals until there are two successive trials with no frame loss.

If RFC2544 is not enabled, the test starts at the configured bandwidth of the test profile or at the maximum throughput found depending on the setting of the frameloss-start-bw attribute.

Figure 6-2 shows an example of a frame loss test in a network.

Copyright© 2022 Ciena® Corporation

Figure 6-2
Frame loss test



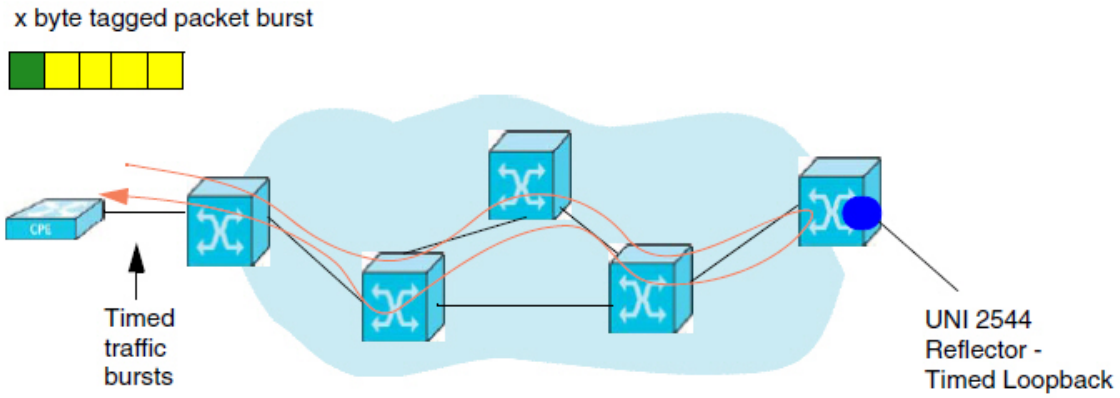
Latency test

The latency test measures the time required for a frame to travel from the originating device through the network to the destination device and back, which is also known as end-to-end testing. Ciena's latency test measures the round-trip time.

When the latency test time varies from frame to frame, it causes issues with real-time services. Long latency can also degrade Ethernet service quality.

Figure 6-3 shows an example of a latency test in a network.

Figure 6-3
Latency test



Packet delay variation test

The packet delay variation (PDV) test uses the latency test measurements to compute an average variation of round trip delay for frames to travel from the originating device through the network to the destination device and back, which is also known as end-to-end testing.

Copyright© 2022 Ciena® Corporation

A PDV value is calculated for different frame sizes. PDV values should be small in order to ensure applications like voice over IP (VoIP) operate without disruption or quality degradation.

Outage test

The outage test is used to detect and measure the service outages during a given period. Test frames are sent at a given rate for the duration of the test. The rate at which the frames are sent during the outage test depends on the tests that are enabled.

If only outage is enabled, then the profile bandwidth is used. If throughput, latency/PDV, or frameloss with a frameloss-start-bw of max-throughput are enabled, then max-throughput is used. If outage and frameloss with frameloss-start-bw configured for profile-bw are enabled, then profile bandwidth will be used.

When a discontinuity in sequence number is detected, an outage is recorded and includes the following information: the start and end time of the outage, the duration in microseconds and the number of frames that were dropped.

An outage is only recorded once the service is up again, since it is based on detecting a discontinuity in sequence number for the test stream.

The outage test is run after all other configured tests for the remaining configure duration. A maximum of 128 outages can be recorded per outage test. If more than 128 outages are detected, the extra outages are counted only; no details will be recorded for these extra outages. There can only be one test instance running outage at any given time.

RFC2544 test

The RFC2544 test runs at full line rate, ignoring the test profile's configured bandwidth. The RFC2544 test is a combination test which executes the following tests sequentially:

- throughput test
- frame loss test
- latency test

Note 1: To configure and run benchmark tests, you need to install the Advanced-OAM license key. To obtain the Advanced-OAM license key, contact Ciena Sales.

The RFC 2544 test suite supports seven pre-defined frame sizes (64, 128, 256, 512, 1024, 1280 and 1518 bytes) to simulate various traffic conditions.

Y.1564 test

Y.1564 defines a test method specific to Ethernet service activation.

Copyright© 2022 Ciena® Corporation

Y.1564 requires the configuration of Ethernet MIX (EMIX). EMIX is a sequence of up to 16 different packet sizes selected from a fixed set, repeated throughout the test stream. Tests are performed in the following order:

- throughput
- frame loss
- latency and PDV

EMIX is configured at the profile level or at the global generator level (default EMIX) if Y.1564 is enabled on the test profile. Y.1564 requires an EMIX to be configured either in the selected test profile or at the global level. If Y.1564 is selected and no EMIX is configured, the start command will fail for the particular test instance; however, if Y.1564 is not set in the profile, but an EMIX is configured, the selected tests will be run with the EMIX instead of using the frame size list.

You can use a pre-defined system-generated EMIX sequence or create a custom EMIX sequence. Pre-defined EMIX sequences cannot be modified.

Table 6-1 lists pre-defined EMIX sequences.

Table 6-1
Pre-defined EMIX sequences

ID	Name	Sequence
1	y1564	abceg
2	y1564-v6	vbceg
3	simple	aaaaaaauuuugg
4	simple-v6	vvvvvvvuuuugg
5	firewall	g
6	tcp	bbbbbbbuuuugg
7	ipv6	vvvvvvvuuuugg

Table 6-2 shows the EMIX character set used to create custom EMIX sequences. You can create multiple custom sequences.

Table 6-2
EMIX character set

a	b	c	d	e	f	g	h	u	v
64	128	256	512	1024	1280	1518	MTU	custom	84

Table 6-3 lists special considerations for the EMIX character set.

Copyright© 2022 Ciena® Corporation

Table 6-3
Special considerations

Character	Note
a	Cannot be used with IPv6 test profiles.
h	Associated with the port under test max-frame-size value. If the max-frame-size of the port is changed, the h frame size is also adjusted for each EMIX using h on the associated benchmark generator instance and entity.
u	Associated frame size defaults to 594. The frame size must be less than or equal to the frame size associated with h. If the frame size for u is set to higher than h, the h frame size is used for u.

Y.1564 also introduces

- Key Performance Indicators (KPIs), which are used to evaluate the pass or failure of a test
- bandwidth allocation profiles, which define how to distribute bandwidth among test streams for each configured Priority Code Point (PCP) to better simulate actual traffic priority distribution

You can configure a total of 32 KPI profiles, 32 EMIX sequences (including pre-defined sequences) and bandwidth allocation profiles.

Test profile

Test profiles are used to configure parameters for the benchmark generator test instance. The 5160 Service Aggregation Switch can support up to 128 enabled/running test instances. All other 39XX/51XX switches support up to 32 enabled/running test instances. Test profiles are associated with test instances.

Changing the configuration of a test profile will cause the statistics and results of all test instances using that profile to be cleared. A test profile cannot be modified if it is used by at least one running test instance.

Test instance

A generator test instance is associated with a test profile, and an optional vtag-stack and destination mac. The optional fields, when specified, override the values configured in the test profile. The test profile is only mandatory for the generator test instance. If the test instance is associated with a reflector entity you cannot specify a test profile.

Table 6-4 lists characteristics of test instances.

Copyright© 2022 Ciena® Corporation

Table 6-4
Test instances

Test instance	Mandatory attributes	Optional attributes
Generator test instance	name profile	vtag-stack vlan-untagged data dst-mac
Reflector test instance	vtag-stack vlan-untagged data	

The state of a test is associated with the test instance as well as the results, that is, statistics. The benchmark generator show command for a specified generator entity shows the status of the generator entity along with a list of all the test instances defined against that generator entity.

The benchmark generator show status command for a specified generator entity shows the status of the generator entity and the test progress and status of the first 10 running test instances.

A test profile configuration cannot be changed while any test instance using that test profile is running.

You can configure and save:

- 128 test instances for each generator or reflector

  Note: Benchmark and TWAMP can only be run at the same time if TWAMP is configured in software mode (that is, hardware assist is disabled).

Operational roles

39XX/51XX switches running benchmark tests operate in operational roles:

- "UNI Generator"
- "UNI Reflector"

UNI Generator

A 39XX/51XX switch in the generator role uses Service Activation test packets.

Copyright© 2022 Ciena® Corporation

Key Performance Indicator (KPI) profiles, bandwidth allocation profiles and EMIX sequences support Y.1564 testing. Benchmark performs an analysis of test results to determine pass or fail according to user-configured KPIs for each test.

Up to 32 KPI profiles can be configured and any test profile can refer to them by means of the kpi-profile attribute. If there is no kpi-profile associated with the test profile, the pass or fail evaluation is not reported. A default KPI profile can also be configured at the generator level. If the KPI profile is not configured under the test profile, but a default is configured at the generator level, the default will be used to evaluate the results for the test instance.

The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142 and 5160 devices can generate IPv4 and IPv6 test traffic.

Note 1: There is a limit for the vid-out-of-service mode. A maximum of 16 unique or distinct C-VLANs can be under test at any time on non-5160 platforms, and a maximum of 32 on the 5160.

Note 2: The vid-out-of-service mode over MPLS based service (VPLS and VPWS) represents that all VLAN IDs bundled for the service-under-test are taken out-of-service. This blocks ingress or egress traffic. All other VLAN-IDs mapped to other services on the port-under test remain able to transmit/receive client traffic. Vid-out-of-service mode over MPLS-based services is equivalent to ac-out-of-service.

UNI Reflector

The UNI reflector mechanism supports the functionality to run a complete test session from a single node in the network by receiving the test packet, swapping various fields within the packet, and returning it to the generator using the original source address found in the packet. Benchmark test frames are subjected to the same ingress and egress traffic conditioning as regular customer traffic. This applies to test traffic in both the generator and the reflector role. Benchmark traffic is treated the same as customer traffic with respect to CoS. Ciena devices in the UNI reflector role inter operate with other vendor RFC2544 test implementations and equipment. The following fields (if they exist) are swapped in the Service Activation test packet during reflection:

- Ethernet Source and Destination MAC Addresses
- IP Source and Destination Addresses
- UDP Source and Destination Port Numbers.

Note: The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms support the UNI reflector role.

Copyright© 2022 Ciena® Corporation

The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms support full reflection of IPv4 and IPv6 packets. When configured as a reflector, the 5060 switch can reflect up to 64 simultaneous sessions. The remaining switches can reflect up to 32 simultaneous sessions.

Port under test

Port under test simulates a reflector or generator as if it was hanging off a UNI port on the platform. The user specifies a port to target as the port under test. The test traffic is subjected to the same ingress and egress traffic conditioning as would the customer traffic ingressing or egressing the selected UNI port under test.

The generator port under test configuration is physical port, LAG, MC-LAG or Y-protection. All SAOS platforms support LAG with 1:1 active-standby protection, 1:1 MC-LAG and dual node Y-protection port as port under test with test mode as vid-oos or out-of-service.

Support is for test mode as vid out-of-service or out-of-service. In-service mode is not supported.

To ensure that benchmark can operate with LAG/MC-LAG/Y-cable as port under test, benchmark must be enabled after LAG is fully operational.

Both active and backup ports involved must have the same configuration although the speed is enforced by software. Other port configuration parameters are not be enforced by the software. It is up to the operator to monitor this to ensure a valid test result.

For 1:1 MC-LAG and dual node Y-protection configuration for reflector seamless test switchover, the operator needs to identically configure the benchmark entity and test instance on both the active and standby node with the reflector entity reflector-mac-validation set to off.

Note 1: In the case of port under test as 1:1 LAG configuration and VID-OOS mode, the scaled limit for the number of simultaneous test instances shall be reduced to half of the default limit for that platform.

Note 2: For a Benchmark test to provide valid test results, the ports involved in a 1:1 protection configuration under-test must have the same configuration.

Static Reflector

The static reflector supports end-to-end testing from a single node in the network by receiving the test packet, modifying it to swap the source and destination MAC addresses, reflecting it back to the network using Layer 3 static IP routing. The static reflector is implemented in software and therefore

Copyright© 2022 Ciena® Corporation

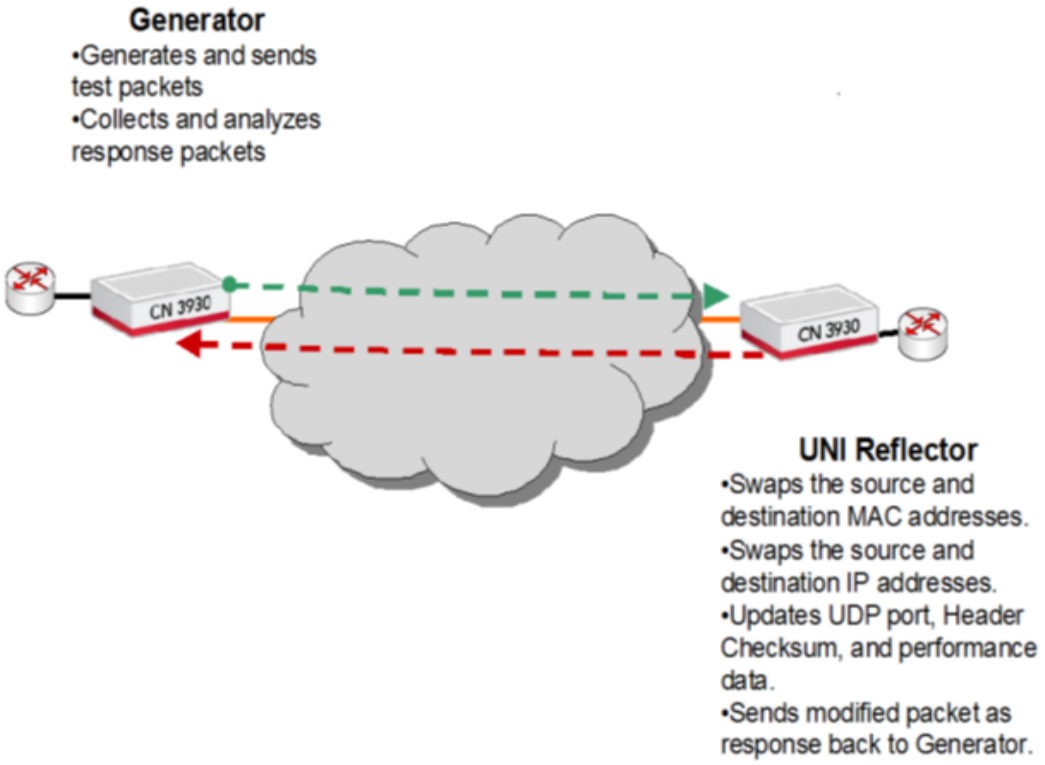
is limited in rate of packets that can be reflected. It does swap all L2 and L3 fields. Ciena devices in the static reflector role inter operate with other vendor RFC2544 test implementations and equipment.

Note: Layer 3 static reflector does not support IPv6.

Generator to UNI Reflector testing

The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms can operate as generators to run tests between 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms operating as UNI reflectors as shown in Figure 5-1.

Figure 6-4
Generator to Uni Reflector

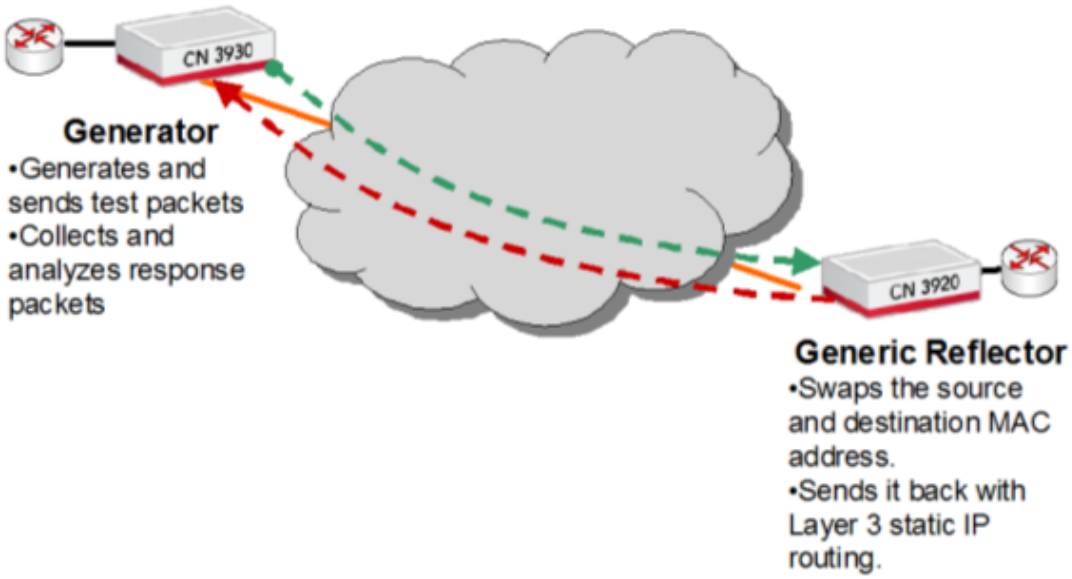


Generator to Static Reflector testing

3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms can operate as generators to test 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, or 5160 platforms operating as static reflectors as shown in Figure 5-2.

Copyright© 2022 Ciena® Corporation

Figure 6-5
Generator to Static Reflector



In addition, Ciena devices interoperate with other vendor service activation testing software or devices.

Each switch can accommodate a reflector entity. Each reflector entity operates independently. A test instance is created for every service that reflects traffic. Multiple services can be tested, that is, reflected, at the same time.

> ***Note:*** The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms can operate as a generator or as a UNI reflector, but not both roles at the same time. They can operate as a generator and a Static Reflector at the same time.

Copyright© 2022 Ciena® Corporation

Benchmark testing scalability by platform

Table 6-5 contains information on the maximum profiles and test instances supported by platform.

Table 6-5
Generator/reflector scalability by platform

Max profiles/ test instances Running	Max profiles/test instances Enabled	Role	Mode	Platform
64	N/A	Reflector	In-service or out-of-service	5160
32	N/A	Reflector	In-service or out-of-service	39XX, 5142
32 distinctive VLAN IDs	Up to 32 reflector test instances can be enabled simultaneously	Reflector	Vid-out-of-service	5160
16 distinctive VLAN IDs	Up to 16 reflector test instances can be enabled simultaneously	Reflector	Vid-out-of-service	39XX, 5142
N/A	128 test sessions or 128 test instances, whichever comes first	Generator	In-service or out-of-service	5160
N/A	32 different C-VID, 128 test sessions, or 128 test instances whichever 32 test sessions or 32 test instances, whichever comes first	Generator	Vid-out-of-service	5160
N/A	32 test sessions or 32 test instances, whichever comes first	Generator	In-service or out-of-service	39XX, 5142
N/A	16 different C-VID, 32 test sessions, or 32 test instances whichever comes firs	Generator	Vid-out-of-service	39XX, 5142

Copyright© 2022 Ciena® Corporation

About test packets

Generator IP address is the source IP address in the packet and the Reflector. IP address is the destination IP address. The content of the test packet can be bare Ethernet, plain IPv4 or IPv6 or UDP echo over IPv4 or IPv6. When sending untagged bare Ethernet traffic, a Type/Len value of 0xFFFF is used.

Testing modes

The 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, 5142, and 5160 platforms provide three operational testing modes for benchmark tests to choose whether customer services currently using the port under test will be disrupted or not during service activation testing. Table 6-6 lists the available operational modes.

Table 6-6
Testing modes

Operational mode	Description
in-service	Performed while customer traffic is being sent in the network with minimal or no disruption to services or traffic. When mode is in-service or vid-out-of-service, the test traffic will flow according to the operational state of the port under test. If the port under test is down, test traffic will not flow. In-service mode impacts customer traffic if the profile configured bandwidth is more than the remaining bandwidth on the NNI port. In-service is the default mode.
out-of-service	Performed while the test port is removed from service causing disruption of services and traffic for the port under test. Starting in SAOS 6.13, out-of-service or vid-out-of-service will block customer traffic only when the test profile (6.13.0 to 6.15.1) or test instance (starting in 6.16.0) is running. If a test is not currently running, customer traffic continues to pass through the port under test in those modes.
vid-out-of-service	Performed while customer traffic that does not belong to the test VLAN flows in and out of the customer port, but any customer traffic belonging to the test VLAN is dropped. Note that in vid-out-of-service test mode, commands are rejected if • the reflector test vid is set to any The vid-out-of-service mode over MPLS based service (VPLS and VPWS) represents that all VLAN IDs bundled for the service-under-test are taken out-of-service. This blocks ingress or egress traffic. All other VLAN-IDs mapped to other services on the port-under test remain able to transmit/ receive client traffic. Vid-out-of-service mode over MPLS-based services is equivalent to ac-out-of-service.

Copyright© 2022 Ciena® Corporation

The out-of-service or vid-out-of-service mode only blocks customer traffic when the test instance is running. If no test is currently running, customer traffic continues to pass through the port under test in those modes.

All platforms only support one benchmark entity. The mode is configured under the entity using the benchmark generator command.

The mode can only be changed when the reflector or generator entity is disabled.

Software upgrades and downgrades

When downgrading to a release prior to 6.14, if benchmark port under test is configured with vs-l2-transform i-stamp:push,e-match-pop:stamp mode, benchmark can remain disabled after downgrade as this support is not backward compatible and requires a configuration change to remove translate-tag members.

If upgrading from release 6.15.1 or older to release 6.16 and the benchmark port is configured, the appropriate entity will be created. In the generator role, all enabled test profiles will result in an equivalent test instance created and enabled. If the node is configured as a reflector and the reflector is enabled, a test instance is created and enabled for the specified reflector vid. If a vid is configured, the reflector test instance is created with an accompanying vid parameter.

If downgrading from 6.16 to an earlier release, all test instances are removed. If a vid is not configured, the reflector test instance is created with as a vtag-stack to reflect all traffic. For the generator, all enabled test instances are converted to an enabled test profile. For the reflector, only the first enabled test instance is used to configure the vid parameter of the reflector in pre-6.16.0 configuration.

Benchmark statistics

Benchmark test statistics report statistics for the test packets that match the configuration of the test instance. The session keys used for the test instance are shown at the bottom of the output of the benchmark test show command for the specified test instance.

Copyright© 2022 Ciena® Corporation

Packets that match the configured profile

For packets that match the configured profile, the total number of received packets (Total) is sub-divided into categories as described in Table 6-7.

Table 6-7
Total section

Category	Description
IPv4, non UDP	All IPv4 packets that are non-UDP and that match the profile and reflector configuration.
IPv4 UDP	All IPv4 UDP packets received that match the profile and reflector configuration.
IPv6, non UDP	All IPv6 packets that are non-UDP and that match the profile and reflector configuration.
IPv6 UDP	All IPv6 UDP packets received that match the profile and reflector configuration.
Non IP	All non-IP packets received. This counter is non-zero when the pdu-type of the profile is set to ethernet.
Unrecognized	All other packets that have a destination MAC address set to that of the benchmark FPGA, and potentially VLAN configured in profile or reflector, but are not IP or UDP echo, and do not have a typelen field that is recognized by the FPGA.

The RX seq num stats section lists the categories described in Table 6-8.

Table 6-8
RX seq num stats section

Category	Description
Dupl seq	Packets received that match the profile but had the same sequence number as the previous packets received.
Out-of-order seq	Packets received that match the profile but had a sequence number that was less than the expected sequence number.
Disc in seq	Packets received that match the profile but had a sequence number that was greater than the next expected sequence number. This indicates that packets are being dropped in the network.

Copyright© 2022 Ciena® Corporation

Note: If any of these counters are prefixed by a * character, the counter overflowed and the count information is therefore not reliable. The 5160 has a 16-bit counter for these values: it overflows at 65535.

RX packets with UDP checksum errors are reported against the generator/reflector entity global statistics along with the RX no match and RX CRC pkts. Note that for the 10GE reflector, any packets received with UDP or CRC checksum errors are dropped and not reflected, even if they match an enabled test instance.

Showing statistics

Statistics provide the measurements gathered through all iterations of the throughput test run for the selected test instance since the last clear command. For frameloss, latency and PDV, results are not cumulative. Only the results for the last completed iteration are reported.

The report provides details on the configuration used to run the test. When the profile KPI is set, a pass or fail is reported for each frame size or EMIX, and for each PCP tested. If there is no KPI profile referenced, a pass/fail is not reported. If a KPI profile is used, but no KPI data is available for the PCP being tested, “---” is displayed to indicate that the KPI was not configured. Results for an iteration are displayed only once all the selected tests have completed. If the test instance has never been run, the report indicates this. If a test instance is stopped by the user, all results accumulated for the current iteration are discarded. Results for previously completed iterations remain available for display while the current iteration is running.

Any changes to the profile attribute configuration automatically clears any saved results for all test instances using that test profile: bandwidth, c-color, c-vid, frame-size-list, EMIX reference, bandwidth allocation profile, encapsulation type or destination MAC. For EMIX and bandwidth allocation profile, if the profile is using the default generator attributes and they are changed at the generator level, it will also clear the statistics for all test instances using test profiles that rely on the generator default EMIX and/or bandwidth allocation profile.

Tests running an IPv4 or IPv6 test frame do not affect the output of the results.

Test results remain available after a test instance is disabled, as well as packet counter statistics. They are available while the test instance is disabled. All results and statistics are cleared once the test instance is re-enabled. When the test instance is re-enabled, the stored statistics are erased. The date and time of the last start command on the test instance is displayed on the last line of the “benchmark profile show name <inst>” command.

Copyright© 2022 Ciena® Corporation

The results for the throughout statistics are the only results that are cumulative over multiple iterations. They are based on the maximum throughput found at each iteration. KPI evaluation is based on the maximum throughput of all iterations and may not reflect the KPI result of the last iteration.

Test results

The latest test instance results are stored to file when an iteration completes.

Saved test instance results remain available as long as the test instance is disabled and there are no configuration changes to the associated test instance or the test profile that it references. Saved test instance results are cleared when the test instance is re-enabled.

Benchmark NETCONF

Benchmark NETCONF is managed using the ciena-sat.yang model. This YANG model is consistent with CIENA-CES-BENCHMARK-MIB and supports multiple benchmark entities and test instances.

Although the YANG model contains operational data, Benchmark NETCONF currently supports configuration only.

For platforms that do not support Benchmark, the sat container is not populated. Any attempt to configure any container/list/leaf under sat will be rejected.

The Replace operation is not supported on any of the containers/leaves within the ciena-sat YANG model.

For more information about the ciena.sat.yang model, refer to *39XX/51XX Switches and Platforms YANG Model Reference*.

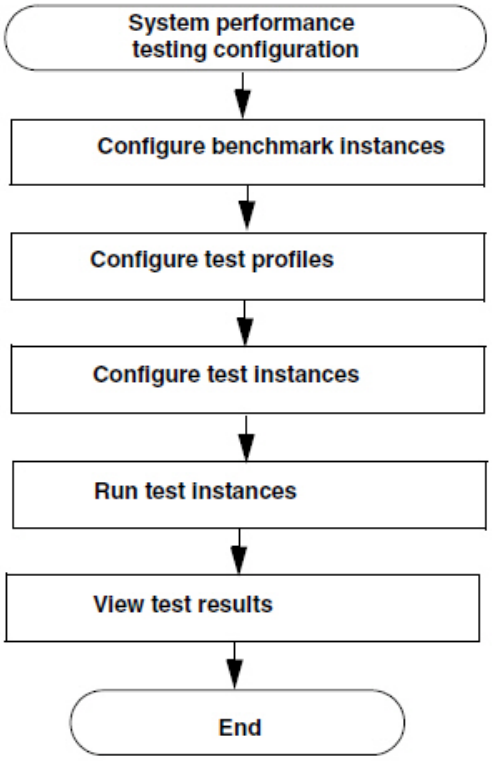
> ***Note:*** Benchmark NETCONF configuration is subject to the same rules as CLI configuration. For example, a test-profile cannot be deleted if it is referenced by a test-profile, and various actions cannot be taken unless benchmark is disabled.

Procedures

Figure 6-6 shows the flow of procedures for configuration of system performance testing with RFC2544 and Y.1564 benchmark services.

Copyright© 2022 Ciena® Corporation

Figure 6-6
Configuration of system performance testing with RFC2544 and Y.1564 benchmark services



Procedures for configuring benchmark instances are:

- "Configuring a custom EMIX sequence" on page 6-22
- "Displaying EMIX sequence information" on page 6-25
- "Configuring benchmark generator KPI profiles" on page 6-27
- "Displaying KPI profile information" on page 6-31
- "Configuring benchmark generator bandwidth allocation profile" on page 6-33
- "Displaying bandwidth allocation information" on page 6-36
- "Configuring a 39XX/51XX switch as a generator" on page 6-38
- "Configuring a 39XX/51XX switch as a reflector" on page 6-40
- "Modifying a generator" on page 6-42
- "Modifying global attributes for a generator" on page 6-43
- "Modifying a reflector" on page 6-44
- "Displaying all benchmark entities" on page 6-46

Copyright© 2022 Ciena® Corporation

- “Displaying generator entity information” on page 6-47
- “Deleting a generator or reflector” on page 6-48

Procedures for configuring test profiles are:

- “Configuring generator test profiles” on page 6-49
- “Displaying generator test profiles” on page 6-53
- “Configuring test attributes” on page 6-55
- “Configuring traffic test types” on page 6-58
- “Configuring payload information” on page 6-61

Procedures for configuring test instances are:

- “Creating test instances” on page 6-65
- “Creating generator test instances” on page 6-67
- “Starting and stopping generator test instances” on page 6-69
- “Generating untagged traffic” on page 6-70
- “Generating single-tagged traffic” on page 6-72
- “Generating double-tagged traffic” on page 6-76
- “Reflecting untagged traffic” on page 6-79
- “Reflecting single-tagged traffic” on page 6-81
- “Reflecting double-tagged traffic” on page 6-83

Procedures for viewing test results are:

- “Displaying benchmark status information” on page 6-86
- “Displaying benchmark test information” on page 6-88
- “Displaying reflector global statistics” on page 6-93
- “Clearing reflector global statistics” on page 6-95
- “Clearing reflector global statistics” on page 6-95
- “Clearing generator test instance statistics” on page 6-97

Example for configuring benchmarking over MPLS

- “Configuration example for MPLS” on page 6-98

Copyright© 2022 Ciena® Corporation

Procedure 6-1
Configuring benchmark support on 3926, 3928, and 5160 switches

Configure benchmark support on 3926, 3928, and 5160 switches *before* configuring a benchmark service on them.

To use benchmark on these switches, first configure the ports listed in this table:

Table 6-9
Benchmark support configuration

Switch	Port	Location	Notes
3926	4	Front panel	Configure this port as an OAM service port. Once configured, this port can only be used by the benchmark feature.
3928	7	Front panel	
5160	20	Front panel	Configure this port as an OAM service port. Once configured, this port is removed from the configuration and display output and is ready for use by the benchmark feature.

When a port is reserved for OAM services, it cannot be used as a front panel port for customer traffic. When a port is reserved for OAM services, the device port is connected to the OAM integrated circuit instead of the front panel port.

Before provisioning a port as a system OAM port, ensure that the port is in the default state, that is, not configured against any services or features. In addition, none of the port attributes should be modified from the default.

After an OAM service port is configured on 3926, 3928, and 5160, proceed with “System performance testing with RFC2544 and Y.1564 benchmark services” on page 6-1.

Step	Action
1	Ensure the port used to configure as the OAM port is in the default state and none of the port attributes have been modified from the default: `port show port <port>`
2	Perform one of the following steps:
	a. On a 3926 switch, configure port 4 as a system-reserved port: `chassis system-rsvd-port add port 4 feature oam-services`

Copyright© 2022 Ciena® Corporation

b. On a 3928 switch, configure port 7 as a system-reserved port:

```
chassis system-rsvd-port add port 7 feature oam-
services
```

c. On a 5160 switch, configure the oam-services-port-role:

```
chassis set oam-services-port-role oam-services
```

Note: Once the above command is entered on the 5160, you are prompted to do a configuration save and reboot. When the system comes back up, you no longer see any references to port 20.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-2
Configuring a custom EMIX sequence

You can

- configure a custom EMIX sequence
- delete a custom EMIX sequence
- modify the sequence or u-frame size for a custom EMIX sequence object
- reset the u-frame size to the default size

Table 6-10 shows the EMIX characters used to compose an EMIX sequence and their corresponding frame sizes.

Table 6-10
EMIX character set

a	b	c	d	e	f	g	h	u	v
64	128	256	512	1024	1280	1518	MTU	custom	84

* The EMIX character “v” is used when IPv6 test PDUs are used for a profile. When an IPv6 test PDU is used, the minimum frame size increases from 64 bytes to 84 bytes. To accommodate EMIX patterns with the character “a” for IPv6 generator test profiles, equivalent EMIX patterns are created (predefined) or when configured the character “v” must be used in place of the character “a”. A generator test profile that is configured for IPv6 test PDUs cannot be configured to use an EMIX pattern with the character “a” or “u” if “u” is less than 84 bytes.

The “h” frame size which is associated with the port under test max-frame-size is adjusted every time the port under test is changed. The u-frame size, if set to a value higher than the current “h” frame size, will generate a warning and the associated EMIX will automatically be adjusted so that “u” is equal to “h”.

Copyright© 2022 Ciena® Corporation

Step	Action

To configure a custom EMIX sequence

1 Configure a custom EMIX sequence:

```
benchmark generator emix-sequence create name <emix-name>
[sequence <String>] [u-frame-size <Integer>]
```

where

name <emix-name>	is the name for the new emix-sequence.
sequence <String>	is the sequence for the new emix-sequence.
u-frame-size <Integer>	is the custom frame size.

To delete a custom EMIX sequence

2 Delete a custom emix-sequence:

```
benchmark generator emix-sequence delete name <emix-name>
```

where

name <emix-name>	is the name of the user-created emix-sequence to delete.

Note: An EMIX sequence cannot be changed or deleted if it is currently in use by a running test instance.

To modify the sequence or u-frame size for a custom EMIX sequence object

3 Modify the sequence or u-frame size for a custom EMIX sequence object:

```
benchmark generator emix-sequence set name <emix-name>
[sequence <string>][u-frame-size <integer>]
```

where

name <emix-name>	is the EMIX name.
[sequence <string>]	is the EMIX sequence.
[u-frame-size <integer>]	is the u-frame size.

Copyright© 2022 Ciena® Corporation

To reset the u-frame size to the default size

4 Reset the u-frame-size to the default of 594 bytes for the specified custom EMIX sequence:

```
benchmark generator emix-sequence unset name <emix-
name>[u-frame-size <integer>]
```

where

name <emix-name>	is the EMIX name.
[u-frame-size <integer>]	is the u-frame size.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-3
Displaying EMIX sequence information

Display EMIX sequence information to verify

- the configuration and status of an EMIX sequence
- all configured EMIX sequences

Step	Action

To display the detailed configuration and status information of an EMIX sequence

1 Display detailed configuration and status information of the specified EMIX sequence (user or system created):

```
benchmark generator emix-sequence show name <emix-name>
```

where

name <emix-name> is the name of the emix-sequence.

To display all configured EMIX sequences

2 Display emix-sequence information:

```
benchmark generator emix-sequence show
```

—end—

Examples

The following example shows output for the benchmark generator emix-sequence show name command for a specific EMIX sequence.

```
> benchmark generator emix show

+------------- BENCHMARK EMIX Sequences Configuration and Status ---------+
|    |                     |                | U frame |         | Number Of  |
| Id |      Name           |  Sequence      |  Size   | Owner   | References |
+----+---------------------+----------------+---------+---------+------------+
|  1 | y1564               | abceg          |  594    | system  |     0      |
|  2 | y1564-v6            | vbceg          |  594    | system  |     0      |
|  3 | simple              | aaaaaaauuuugg  |  594    | system  |     2      |
|  4 | simple-v6           | vvvvvvvuuuugg  |  594    | system  |     0      |
|  5 | firewall            | g              |  594    | system  |     0      |
|  6 | tcp                 | bbbbbbbuuuugg  |  594    | system  |     0      |
|  7 | ipv6                | vvvvvvduuuugg  |  594    | system  |     0      |
|  8 | emix_test           | abch           |  594    | user    |     1      |
+----+---------------------+----------------+---------+---------+------------+
+------------------------- EMIX Allowed Character Set --------+
| Character  | a  | b  | c  | d  | e  | f  |  g | h |  u    | v  |
+------------+----+----+----+----+----+----+----+---+-------+----+
| Frame Size | 64 | 128| 256| 512|1024|1280|1518|MTU|custom| 84 |
+------------+---+----+----+----+----+----+----+---+------+----+
```


Copyright© 2022 Ciena® Corporation

The following example shows output for the benchmark generator emix-sequence show command:

```
+------------------------- BENCHMARK EMIX Sequences Configuration and Status --------------------------+
|    |                                                  |                  | U frame |         | Number Of  |
| Id |                       Name                       |     Sequence     |  Size   | Owner   | References |
+----+--------------------------------------------------+------------------+---------+---------+------------+
|  1 | y1564                                            | abceg            |  594    | system  |     1      |
|  2 | y1564-v6                                         | vbceg            |  594    | system  |     0      |
|  3 | y1564-qinq-v4                                    | wbceg            |  594    | system  |     0      |
…
| 12 | ipv6-qinq                                        | xxxxxxduuuugg    |  594    | system  |     0      |
+----+--------------------------------------------------+------------------+---------+---------+------------+

+-------------------------------- EMIX letter to frame size association --------------------------------+
| Letter             |   a  |   b  |   c  |   d  |   e  |   f  |   g  |   h  |   u  |   v  |   w  |   x  |
+--------------------+------+------+------+------+------+------+------+------+------+------+------+------+
| Frame Size         |   64 |  128 |  256 |  512 | 1024 | 1280 | 1518 |  MTU |custom|   84 |   68 |   88 |
+--------------------+------+------+------+------+------+------+------+------+------+------+------+------+
```

The following example shows the EMIX output in relation to a specific benchmark generator entity/instance named gen1 emix-sequence y1564:

```
+---------------  EMIX Sequence Configuration and Status --------------+
| Parameter        | Value                                             |
+------------------+---------------------------------------------------+
| Id               | 1                                                 |
| Name             | y1564                                             |
| Sequence         | abceg                                             |
| Frame sizes      | 64   128  256  1024 1518                          |
| Avg frame size   | 598                                               |
| U frame size     | 594                                               |
| Num references   | 0                                                 |
| System created   | yes                                               |
+------------------+---------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-4
Configuring benchmark generator KPI profiles

You can

- create a Key Performance Indicator (KPI) profile
- delete a KPI profile
- modify KPI values for a list of PCPs for a KPI profile
- reset the KPI values back to 0 for the given PCPs for the KPI profile.

Step	Action

To create a KPI profile

1 Create a KPI profile:

```
benchmark generator kpi-profile create name <kpi-obj-
name> {{pcp <integer-list>} | untagged} [throughput-min
<string>] [frameloss-max <string>] [latency-max
<integer>] [pdv-max <integer>] [single-outage-max
<integer>] [sum-outages-max <integer>] [max-num-outages
<integer>]}
```

where

name <kpi-obj-name>	is the name for the new kpi-profile.
pcp <integer-list>}	is the list of PCP values for which the following KPI values are associated.
untagged	indicates that the following KPIs are associated with an untagged session.
throughput-min <string>	is a floating point value from 0.0001 to 99.9999 and 100.0% (4 digits after the decimal point are kept) deviation from the specified bandwidth in the profile. The string can be up to 8-characters long, including the end of the string null character
frameloss-max <string>	is a floating point value from 0.0 to 100%. It represents the maximum percentage of frame loss that is allowed for the frame loss test to pass. The frameloss is evaluated only on the 100% of the start of the bandwidth for the frameless test. The string can be up to 10-characters long, including the decimal point.
latency-max <integer>	is an integer representing the maximum number of milliseconds of latency allowed for the test to pass. The latency success is evaluated against the maximum latency result for a given stream.
pdv-max <integer>	is an integer representing the maximum number of milliseconds for the PDV test to succeed.

Copyright© 2022 Ciena® Corporation

where

single-outage-max <integer>	is the maximum number of milliseconds in a single outage duration. Range is 1 to 10000.
sum-outages-max <integer>	is the maximum number of milliseconds for total outages duration. Range is 1 to 30000.
max-num-outages <integer>	is the maximum number of outages for the outage test duration. Range is 0 to 128. A value of 0 is set when a KPI failure event is expected to be generated whenever there is at least one outage detected during the test. The test will only be successful if no outages are detected.

To delete a KPI profile

2 Delete a KPI profile:

```
benchmark generator kpi-profile delete name <kpi-obj-name>
```

where

name <kpi-obj-name>	is the name of the kpi-profile to delete.

Note: A KPI profile cannot be deleted if it is referenced by at least one test profile or at the generator default level.

To modify CPI values for KPI profile and PCP values

3 Modify the KPI values for the KPI profile and PCP values:

```
benchmark generator kpi-profile set name <kpi-obj-name>
{{pcp <integer-list>} | untagged} [throughput-min
<string>] [frameloss-max <string>] [latency-max
<integer>] [pdv-max <integer>] [single-outage-max
<integer>] [sum-outages-max <integer>] [max-num-outages
<integer>]}
```

where

name <kpi-obj-name>	is the KPI-profile name.
pcp <integer-list>	is the list of PCP values for which the following KPI values are associated.
untagged	indicates that the following KPIs are associated with an untagged session.
throughput-min <string>	is the minimum throughput.
frameloss-max <string>	is the maximum frame loss.
latency-max <integer>	is the maximum latency.

Copyright© 2022 Ciena® Corporation

where

pdv-max <integer>	is the maximum PDV.
single-outage-max <integer>	is the maximum number of milliseconds in a single outage duration. Range is 1 to 10000.
sum-outages-max <integer>	is the maximum number of milliseconds for total outages duration. Range is 1 to 30000.
max-num-outages <integer>	is the maximum number of outages for the outage test duration. Range is 0 to 128. A value of 0 is set when a KPI failure event is expected to be generated whenever there is at least one outage detected during the test. The test will only be successful if no outages are detected.

To reset the KPI values back to 0 for the KPI profile and PCP values

4 Reset the KPI values back to 0 for the KPI profile and PCP values:

```
benchmark generator kpi-profile set name <kpi-obj-name>
{{pcp <integer-list>} | untagged} [throughput-min
<string>] [frameloss-max <string>] [latency-max
<integer>] [pdv-max <integer>] [single-outage-max
<integer>] [sum-outages-max <integer>] [max-num-outages
<integer>]}
```

where

name <kpi-obj-name>	is the KPI-profile name.
pcp <integer-list>	is the list of PCP values for which the following KPI values are associated.
untagged	indicates that the following KPIs are associated with an untagged session.
throughput-min <string>	is the minimum throughput rest to 0.0.
frameloss-max <string>]	is the maximum frame loss reset to 0.0.
latency-max <integer>	is the maximum latency reset to 0.0.
pdv-max <integer>	is the maximum PDV reset to 0. A value of 0 for any of the KPI values indicates that the KPI is not enabled for the associated PCP and results will not be evaluated.

Copyright© 2022 Ciena® Corporation

where

single-outage-max <integer>	is the maximum number of milliseconds in a single outage duration. Range is 1 to 10000.
sum-outages-max <integer>	is the maximum number of milliseconds for total outages duration. Range is 1 to 30000.
max-num-outages <integer>	is the maximum number of outages for the outage test duration. Range is 0 to 128. A value of 0 is set when a KPI failure event is expected to be generated whenever there is at least one outage detected during the test. The test will only be successful if no outages are detected.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-5
Displaying KPI profile information

Display KPI profile information to verify the configuration.

You can display

- the configuration and status of a KPI profile
- all configured KPI profiles

Step	Action

To display detailed configuration and status information for a specified KPI profile

1 Display detailed configuration and status information for a specified KPI-profile:

```
benchmark generator kpi-profile show name <kpi-obj-name>
```

where

name <kpi-obj-name> is the name of the kpi-profile.

To display all configured KPI-profiles

2 Display all KPI profiles:

```
benchmark generator kpi-profile show
```

—end—

Example

The following example shows output for the benchmark generator kpi-profile show command.

```
> benchmark generator kpi-profile show

+----------------------- BENCHMARK KPI Profiles Configuration and Status -----------------------+
| ID | Name          | Ref |  PCP   | Thrput | Frmloss | Latency |  PDV   |         Outage         |
|    |               |     |        |        |         |         |        | Single |  Sum   |  Num   |
+----+---------------+-----+--------+--------+---------+---------+--------+--------+--------+--------+
|  1 | test          |   0 | untag  |  Set   |   --    |   --    |   --   |  Set   |  Set   |  Set   |
|    |               |     |   0    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   1    |  Set   |   Set   |   Set   |   Set  |  Set   |  Set   |  Set   |
|    |               |     |   2    |  Set   |   Set   |   Set   |   Set  |  Set   |  Set   |  Set   |
|    |               |     |   3    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   4    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   5    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   6    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   7    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
+----+---------------+-----+--------+--------+---------+---------+--------+--------+--------+--------+
|  2 | test2         |   0 | untag  |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   0    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   1    |  Set   |   Set   |   --    |   --   |  Set   |  --    |  --    |
|    |               |     |   2    |  Set   |   Set   |   --    |   --   |  Set   |  --    |  --    |
|    |               |     |   3    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
|    |               |     |   4    |  --    |   --    |   --    |   --   |  --    |  --    |  --    |
```


Copyright© 2022 Ciena® Corporation

```
|    |              |     |   5   |  --    |  --     |  --     |  --    |  --    |  --    |  --    |
|    |              |     |   6   |  --    |  --     |  --     |  --    |  --    |  --    |  --    |
|    |              |     |   7   |  --    |  --     |  --     |  --    |  --    |  --    |  --    |
+----+--------------+-----+-------+--------+---------+---------+--------+--------+--------+--------+
```

The following example shows output for the benchmark generator kpi-profile show command for a specific KPI profile.

```
>benchmark generator kpi-profile show name test
+--------------------------------- BENCHMARK KPI Profile Configuration and Status ----------------------------+
|      Parameter       |                                        Value                                        |
+----------------------+-------------------------------------------------------------------------------------+
| Id                   | 1                                                                                   |
| Name                 | test                                                                                |
| Number of references | 0                                                                                   |
+----------------------+------------+-----------+--------+----------+---------------+-------------+-----------+
|       PCP            | Throughput | Frameloss | Latency|   PDV    | Single Outage | Sum Outages | NumOutages|
|                      |     %      |     %     |   msec |   msec   |      msec     |      msec   |       #   |
+----------------------+------------+-----------+--------+----------+---------------+-------------+-----------+
|      untagged        | 0.0010     |  --       | --     |  --      |  1            |  2          |  1        |
|          0           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
|          1           | 0.0100     | 0.0100    | 5      |  1       |  3            |  10         |  2        |
|          2           | 0.0100     | 0.0100    | 5      |  1       |  3            |  10         |  2        |
|          3           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
|          4           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
|          5           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
|          6           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
|          7           |  --        |  --       | --     |  --      |   --          |   --        |   --      |
+----------------------+------------+-----------+--------+----------+---------------+-------------+-----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-6
Configuring benchmark generator bandwidth allocation profile

Bandwidth allocation lets you configure up to 32 bandwidth allocation profiles which can be referenced by the configured generator test profiles. A bandwidth allocation profile describes the amount of bandwidth to allocate to each PCP. A generator test profile defines a subset of PCPs to test with: C-PCP for encapsulation type dot1q.

Each PCP can be assigned a ratio of the bandwidth from 0 to 100.

Table 6-11 shows an example of a PCP bandwidth distribution profile.

Table 6-11
PCP bandwidth distribution example

PCP	0	1	2	3	4	5	6	7
Ratio	25	25	10	10	10	8	8	4

If a generator test profile specifies a bandwidth of 100 Mbps and a list of PCPs of 0, 2 and 6, then the 100 Mbps is allocated to each PCP stream as follows:

Sum of ratios for configured PCPs: PCP 0, 2 and 6 = 25 + 10 + 8 = 43
Starting BW for a configured PCP = (PCP ratio / Sum of ratios for configured PCPs) * profile bandwidth
PCP 0 BW = (25 / 43) * 100Mbps = 58.14
PCP 2 BW = (10 / 43) * 100Mbps = 23.26
PCP 6 BW = (8 / 43) * 100Mbps = 18.60

Upon starting this generator test instance, three sessions are created in hardware, one for each PCP, to send traffic simultaneously, according to the calculated bandwidth for each PCP. Results will be provided for each PCP separately.

As these profiles use multiple hardware sessions, the maximum number of generator test instances that can be run simultaneously will be reduced. For a given generator entity and instance, you can view how many hardware sessions are used and available by using the benchmark generator show name command.

PCP bandwidth allocation does not work if the priority of the test packet is changed, as it flows through the network. The generator expects the same PCP value on the reflected packet as the one the test frame was generated with.

Copyright© 2022 Ciena® Corporation

If the C-PCP value of the test traffic is expected to change while the traffic is traveling through the network, you must turn off PCP validation on the test profile. PCP validation can only be turned off if only a single PCP is configured. If PCP validation is off, you can only change the PCP value to a single PCP, not a list of PCPs. An error is displayed if you attempt to configure an invalid combination.

You can:

- create a bandwidth (bw) allocation profile
- delete a bandwidth allocation profile
- modify the bandwidth allocation ratio
- set the ratio back to 0 for the selected PCP values of the targeted PCP bandwidth profile

Configured PCPs in a test profile must have a non-zero ratio in the referred PCP bandwidth distribution profile for a start command to be accepted.

The PCP profile cannot be modified if referred to by a profile or profiles currently used by running test instances.

Step	Action

To create a bandwidth allocation profile

1 Create a bandwidth allocation profile:

```
benchmark generator bw-allocation-profile create name
<name> [pcp <NUMBER>] [bandwidth <NUMBER: 0-100>]
```

where

name <pcp-obj-name>	is the name for the new bandwidth allocation profile. The name can be up to 45 characters long.
pcp <NUMBER>	is the list of PCPs which the bandwidth profile will use.
bandwidth <NUMBER: 0-100>	is the ratio or weight of bandwidth allocation for a particular PCP.

To delete a bandwidth allocation profile

2 Delete a bandwidth allocation profile:

```
benchmark generator bw-allocation-profile delete name
<name>
```

where

name <name>	is the name of the bandwidth profile to delete.

Copyright© 2022 Ciena® Corporation

To modify a bandwidth allocation profile ratio

3 Modify a bandwidth allocation profile ratio for the PCP bandwidth profile and PCP value selected:

```
benchmark generator bw-allocation-profile set name <name>
[pcp <NUMBER>] [bandwidth <NUMBER: 0-100>]
```

where

name <name	is the name for the PCP bandwidth allocation profile being modified.
pcp <NUMBER>	is the list of PCPs which the bandwidth profile will use.
bandwidth <NUMBER: 0-100>	is the ratio or weight of bandwidth allocation for a particular PCP.

To reset the bandwidth allocation profile to 0 for the PCP values for the PCP bandwidth profile

4 Reset the bandwidth allocation profile to 0 for the PCP values of the PCP bandwidth profile:

```
benchmark generator bw-allocation-profile unset name
<name> [pcp <integer-list>]
```

where

name <name>	is the name for the PCP bandwidth allocation profile being reset.
pcp <NUMBER>	is the list of PCPs which the bandwidth profile will use.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-7
Displaying bandwidth allocation information

Display bandwidth allocation information to verify the configuration.

You can

- display detailed configuration and status information for the PCP bandwidth profile
- display all configured bandwidth profiles

Step	Action

To display detailed configuration and status information for the bandwidth profile

1 Display detailed configuration and status for the bandwidth profile:

```
benchmark generator bw-allocation-profile show name
<name>
```

where

name <name> is the name of the bandwidth profile.

To display all bandwidth allocation information

2 Display all bandwidth allocation information:

```
benchmark generator bw-allocation-profile show
```

—end—

Examples

The following example shows output for the benchmark generator bw-allocation-profile show command:

```
>benchmark generator bw-allocation-profile show
+------ BENCHMARK Bandwidth Allocation Profiles Configuration and Status ------+
| ID | Name                                              | Ref | PCP |  BW Ratio   |
+----+---------------------------------------------------+-----+-----+-------------+
|  1 | standard                                          |   0 |   0 |   30        |
|    |                                                   |     |   1 |   25        |
|    |                                                   |     |   2 |   25        |
|    |                                                   |     |   3 |   10        |
|    |                                                   |     |   4 |   10        |
|    |                                                   |     |   5 |   10        |
|    |                                                   |     |   6 |   5         |
|    |                                                   |     |   7 |   5         |
+----+---------------------------------------------------+-----+-----+-------------+
```


Copyright© 2022 Ciena® Corporation

The following example shows output for the benchmark generator bw-allocation-profile show command for a specific bw-allocation profile.

```
>benchmark generator bw-allocation-profile show name test

+--- BENCHMARK Bandwidth Allocation Profile Configuration and Status ---+
|      Parameter       |                      Value                      |
+----------------------+-------------------------------------------------+
| Profile ID           | 1                                               |
| Name                 | test                                            |
| Number of references | 0                                               |
+----------------------+---------+---------------------------------------+
| PCP BW allocation    |   PCP   |            Bandwidth Ratio            |
|                      +---------+---------------------------------------+
|                      |    0    |     20                                |
|                      |    1    |     20                                |
|                      |    2    |     20                                |
|                      |    3    |     20                                |
|                      |    4    |     20                                |
|                      |    5    |     20                                |
|                      |    6    |     7                                 |
|                      |    7    |     7                                 |
+----------------------+---------+---------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-8
Configuring a 39XX/51XX switch as a generator

Configure a switch as a generator when you want the switch to generate Service Activation test packets.

> ***Note:*** Configuration changes related to the port under test are blocked if benchmark is enabled. It is recommended to disable benchmark prior to making configuration changes to ensure proper operation of the switch.

This procedure assumes that you have created the following, if required for Y.1564 testing:

- EMIX sequences. You can use:
  - — pre-defined EMIX sequences. For the list, refer to .
  - — custom EMIX sequences. For the procedure, refer to "Configuring a custom EMIX sequence" on page 6-22.
- KPI profiles. For the procedure, refer to "Configuring benchmark generator KPI profiles" on page 6-27.
- PCP bandwidth allocation profiles. For the procedure, refer to "Configuring benchmark generator bandwidth allocation profile" on page 6-33.

Test traffic is subjected to ingress and egress frame conditioning.

Step	Action
1	Create a generator benchmark entity: `benchmark create generator name <name> port <logicalPortEntity> [mode < out-of-service | in-service | vid-out-of-service >][emix-h-frame-size <uint 64-9216>]` where name <name> — is the name of the generator port <logicalPortEntity> — is the logical port. It can be one of the following: • physical port or a LAG port with a single member • LAG port with 1 active and 1 protected member • port with Y-cable configuration (logical port with 1:1 LAG and Y-cable only support vid-oos and oos mode)

Copyright© 2022 Ciena® Corporation

where

mode <in-service|out-of-service|vid-out-of-service>	indicates how customer traffic is treated while testing is active. • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
emix-h-frame-size <uint 64-9212>	Sets the maximum packet size that the FPGA device will generate. Set this value such that any extra encapsulation bytes added by the Ethernet service or MPLS tunnel before sending the test packet to the reflector over the NNI link will not exceed the maximum frame size that the NNI link can transmit. The default value is the max-frame-size configured on the selected port under test.

2 Enable the generator entity:

```
benchmark generator enable name <name>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-9
Configuring a 39XX/51XX switch as a reflector

Configure a 39XX/51XX as a reflector when you want the switch to receive the test packet, swap fields in the packet, and send the packet back to the generator.

Table 6-12 lists the default values for the reflector.

Table 6-12
Default values for the reflector

Attribute	Default value
mode	in-service
vendor-type	ciena

Test traffic is subjected to ingress and egress frame conditioning.

Step	Action

1 Create a reflector benchmark entity:

```
benchmark create reflector name <name> port
<logicalPortEntity> [mode < out-of-service | in-service |
vid-out-of-service >] [vendor-type <ciena | other>][ mac-
validation <on | off>]
```

where

name <name>	is the reflector
port <logicalPortEntity>	is the logical port. It can be one of the following: • physical port or a LAG port with a single member • LAG port with 1 active and 1 protected member • port with Y-cable configuration (logical port with 1:1 LAG and Y-cable only support vid-oos and oos mode)

Copyright© 2022 Ciena® Corporation

where

mode <in-service| out-of-service| vid-out-of-service>	indicates how customer traffic is treated while testing is active. • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
vendor-type <ciena | other>	Indicates which type of generator device test traffic is expected from. Valid values are: • ciena: test traffic is expected from a Ciena device acting as generator • other: test traffic is expected from a device from another vendor acting as generator
mac-validation <on | off>	When mac-validation is off, the test traffic can be sent to the node with any destination MAC address. This is also called MAC-agnostic reflector. When mac-agnostic is on, the test traffic sent to the reflector node must have the destination MAC address set to the reflector assigned MAC address (value of MAC address field in the output of benchmark reflector show name <refInstance>). The mac-validation can only be turned off when mode is set to either out-of-service or vid-out-of-service. The default value is mac-validation on.

2 Enable benchmark test processing:

```
benchmark reflector enable name <name>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-10
Modifying a generator

Modify a generator as required for testing.

Display the list of test instances associated with the generator to be modified to determine whether any associated test instances are running. Any running test instances associated with the generator are automatically stopped when the generator is disabled prior to modifying the generator. To re-start the test instances, see "Starting and stopping generator test instances" on page 6-69.

Step	Action

1 Display the list of test instances associated with the generator to be modified:

```
benchmark generator show name <name>
```

where

name <name>	is the generator

2 Disable the generator:

```
benchmark generator disable name <name>
```

3 Change the configuration of the attributes associated with the generator:

```
benchmark generator set name <name> [mode <in-
service|out-of-service|vid-out-of-service>] [ h-frame-
size <uint 64..9216> ]
```

where

name <name>	is the generator
mode <in-service| out-of-service| vid-out-of-service>	indicates how customer traffic is treated while testing is active. Valid values are: • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
emix-h-frame-size <uint 64-9216>	Sets the maximum packet size that the FPGA device will generate. Set this value such that any extra encapsulation bytes added by the switch before sending the test packet to the reflector over the NNI link will not exceed the maximum frame size that the NNI link can transmit.

4 Enable the generator:

```
benchmark generator enable name <name>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-11
Modifying global attributes for a generator

Modify global attributes for a generator to set the default KPI profile, EMIX sequence, and bandwidth allocation profile to use when not specified in the test profile used by the test instance.

The default EMIX sequence and bandwidth allocation profile can only be changed if no running test instances are using them.

Step	Action

1 Set the default KPI profile, EMIX sequence, and bandwidth allocation profile to use when not specified in the test profile used by the test instance:

```
benchmark generator set [kpi-profile <Benchmark KPI
Profile>] [emix-sequence <Benchmark EMIX Sequence>] [bw-
allocation-profile <Benchmark Bandwidth Allocation
Profile>
```

where

kpi-profile <Benchmark KPI Profile>	is the default KPI profile. If this value is not set, the equivalent leaf is not populated in the NETCONF database.
emix-sequence <Benchmark EMIX Sequence>	is the default EMIX sequence.If this value is not set, the equivalent leaf is not populated in the NETCONF database.
bw-allocation-profile <Benchmark Bandwidth Allocation Profile>	is the default bandwidth allocation profile. If this value is not set, the equivalent leaf is not populated in the Netconf database.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-12
Modifying a reflector

Modify a reflector as required for testing purposes.

Display the list of test instances associated with the reflector to be modified to determine whether any associated test instances are running. All reflector test instances associated with the reflector are automatically disabled and stop reflecting when the reflector is disabled prior to modifying the reflector.

Reflector test instances associated with the reflector are automatically re-enabled when the reflector entity is re-enabled.

Step	Action

1 Display the list of test instances associated with the reflector to be modified:

```
benchmark reflector show name <name>
```

where

name <name>	is the generator

2 Disable the reflector:

```
benchmark reflector disable name <name>
```

3 Modify reflector test attributes:

```
benchmark reflector set name <name> [mode <in-
service|out-of-service|vid-out-of-service>] [vendor-type
<ciena|other>][mac-validation <on | off>]
```

where

name <name>	is the reflector.
mode <in-service| out-of-service| vid-out-of-service>	indicates how customer traffic is treated while testing is active. Valid values are: • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
vendor-type <ciena|other>	indicates which type of generator device test traffic is expected from. Valid values are: • ciena: test traffic is expected from a Ciena device acting as generator • other: test traffic is expected from a device from another vendor acting as generator

Copyright© 2022 Ciena® Corporation

where

mac-validation <on | off>	When mac-validation is off, the test traffic can be sent to the node with any destination MAC address. This is also called MAC-agnostic reflector. When mac-agnostic is on, the test traffic sent to the reflector node must have the destination MAC address set to the reflector assigned MAC address (value of MAC address field in the output of benchmark reflector show name <refInstance>). The mac-validation can only be turned off when mode is set to either out-of-service or vid-out-of-service. The default value is mac-validation on.

4 Enable the reflector:

```
benchmark reflector enable name <name>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-13
Displaying all benchmark entities

Display all benchmark entities to view the benchmark entities currently configured in the 39XX/51XX switch.

Step	Action
1	Display all benchmark entities: `benchmark show`

—end—

Example

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

```
> benchmark show
+------------------------------ BENCHMARK State Info ------------------------------+
|            Parameter            |                     Value                      |
+---------------------------------+------------------------------------------------+
| Admin State                     |                                       enabled |
| Default EMIX Sequence           |                                 Not configured |
| Default KPI Profile             |                                 Not configured |
| Default BW Allocation Profile   |                                 Not configured |
|                                 +-----------------------+------------------------+
| Benchmark Objects Statistics    |          Max          |        Current         |
|                                 +-----------------------+------------------------+
|    Entities Configured          |                     1 |                      1 |
|    Test Instances Configured    |                   128 |                      1 |
|                   Enabled       |                    32 |                      1 |
|                   Running       |                    32 |                      0 |
|    Profiles Configured          |                   128 |                      4 |
|    EMIX Sequences Configured    |                    32 |                     10 |
|    KPI Profiles Configured      |                    32 |                      3 |
|    BW Alloc Profiles Configured |                    32 |                      7 |
+---------------------------------------------------------------------------------+

+--------------- BENCHMARK Entities Configuration and State Info ---------------+
|                 |           |                    |      |        State        |
|        Name     |   Role    |       Mode         | Port |  Admin   |   Oper   |
+-----------------+-----------+--------------------+------+----------+----------+
| gen2            | generator | vid-out-of-service | 2    | enabled  | disabled |
+-----------------+-----------+--------------------+------+----------+----------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-14
Displaying generator entity information

Display generator entity information to verify the configuration of generator entities.

When no generator entity is specified, the system lists the default generator attributes with a list of configured generator entities and their status. Default generator attributes are

- ENIX sequence
- KPI profile
- bandwidth allocation profile

When a generator entity is specified, the system displays the configuration and status of the generator entity along with a list of test instances currently associated with that entity and the status of the test instances.

Step	Action

To display generator entity information

1 Display default generator attributes with a list of configured generator entities and their status:

```
benchmark generator show
```

To display generator entity information for a specified generator entity

2 Display detailed information for the generator entity:

```
benchmark generator show name <benchmark-generator-
entity> {statistics}
```

where

name <benchmark-generator-entity>	is the name of the benchmark generator entity
statistics	displays the global counters for the targeted generator entity

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-15
Deleting a generator or reflector

Delete a generator or reflector when it is no longer required for test purposes.

Before you can delete a benchmark entity, you have to stop, disable and delete all test instances associated with the benchmark entity, then disable the entity.

Step	Action
1	Stop, disable, and delete all test instances associated with the benchmark entity: `benchmark {reflector|generator} {stop|disable|delete} name <entity> all-test-instances`
2	Disable the entity: `benchmark {reflector|generator} disable name <entity>`
3	Delete the benchmark entity: `benchmark delete name <entity>`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-16
Configuring generator test profiles

You can:

- create a generator test profile
- copy an existing generator test profile

39XX/51XX switches support the configuration of up to 128 test profiles. Starting in release 6.16, the test is a test instance instead of a test profile. The test profile is now a parameter specified when creating the test instance object. Test instances are automatically associated with the created benchmark entity.

Step	Action

To create a generator test profile

1 Create a generator test profile:

```
benchmark profile create name <String[45]>
```

where

name <String[45]> is the user-defined name for the new profile.

2 Set the configuration parameters for the test profile:

```
benchmark profile configuration set name <String[45]>
[bandwidth <INT [0..10000]>] [excess-bandwidth <INT
[0..10000]>] [duration <15Min|1Hr|6Hr|24Hr|Indefinite
|once|custom>] [custom-duration <MINUTES:15..65535>]
[interval <15Min|1Hr|2Hr|6Hr|Completion>] [frame-size-
list <INT 64..9216>[1..10] [max-bw-search <INT 1..16>]
[max-samples <INT 2..20>] [sampling-interval <INT
1..600>] [frameloss-start-bw <profile-bandwidth|max-
throughput>] [emix-sequence <emix-sequence-object>]
[kpi-profile <kpi-profile-object>] [bw-allocation-
profile <bw-allocation-profile-object] [vid-validation
<on|off>] [pcp-validation <on|off>] [color-validation
<on|off>]
```


Copyright© 2022 Ciena® Corporation

where

name <String[45]>	is the name of the profile.
bandwidth <INT [0-10000]>	is the bandwidth in Mbps to start testing with. The default value is the maximum operational speed of the port under test.
excess-bandwidth <INT [0-10000]>	:is the bandwidth in Mbps to use with yellow colored traffic if and only if the profile is set for multi-color testing. The default value is 0.
duration <15Min|1Hr|6Hr|24Hr|Indefinite|Once|Custom>	is the length of time allowed for the tests to run. The default value is once.
custom-duration	is the length of time in minutes (15..65535) allowed for the custom duration tests to run. The duration parameter must be set to “custom” to use this parameter. The default value is 15min.
interval <15Min|1Hr|2Hr|6Hr|Completion> e-size-list <INT 64..9216>[1-10]	:is the amount of time for one iteration of the tests to take. If all selected tests have not completed before the interval timer goes off, the iteration is stopped and the next iteration is started (if duration permits). The default value is completion.
frame-size-list <INT 64..9216>[1-10]	is the list of frame sizes in bytes, to use for the tests. The default list includes the following packet sizes: 64, 128, 256, 512, 1024, 1280, 1518, 2048 and 9216. The last two sizes, 2048 and 9216, are only valid when rfc2544 is not selected as a test in the profile. The maximum number of elements in the list is 10. The first frame size in the default list is adjusted to 84 if IPv6 dot1q is configured.
max-bw-search <INT 1-16>	is the maximum number of searches to perform for a successful bandwidth for a given packet size. This attribute is specific to the throughput test. The default value is 7.
max-samples <INT 2-20>	is the maximum number of timestamp samples taken during the test. This attribute is specific to the latency and pdv tests. The default value is 10.
sampling-interval <INT 1-600>	is the number of milliseconds, in 100ms steps, to wait in between each sample (latency and PDV) or statistics read (throughput and frameloss). The valid range is 1 to 600 steps for a range of 100ms to 60sec. The default value is 1 for a sampling interval of 100ms.

Copyright© 2022 Ciena® Corporation

where

frameloss-start-bw <profile-bandwidth|max-throughput>	indicates which bandwidth to use when starting the frameloss test. This attribute is specific to the frameloss test. Valid values are: • profile-bandwidth: the bandwidth specified in the profile or maximum line rate of the port under test if not specified. • max-throughput: the maximum throughput measured by the throughput test. If throughput is not selected, it will automatically be run prior to running the frameloss test. The default value is max-throughput.
emix-sequence <emix-sequence>	is the EMIX sequence to use for testing. • if RFC2544 is not selected, this attribute is used instead of the frame size list attribute. • If RFC2544 is selected, the EMIX is ignored.
kpi-profile <kpi-profile>	is the KPI profile to use for analyzing the test results.
bw-allocation-profile <bw-allocation-profile>	is the bandwidth allocation profile to use when testing against the configured PCP values.
vid-validation <on|off>	indicates whether vid validation for test packets coming back to the generator is on or off. The default is on. If set to off, color and pcp validation settings are disregarded and automatically turned off.
pcp-validation <on|off>	indicates whether the pcp value of the outer tag is used to classify the returning packets. The default value is on. Set the pcp-validation attribute to off when the PCP is expected to change as the test packet travels through the network.
color-validation <on|off>	indicates whether color (DEI bit value) of the outer tag is used to classify the returning packets. The default value is on. Set the color-validation attribute to off if the color is expected to change as the test packet travels through the network.

Copyright© 2022 Ciena® Corporation

To copy a generator test profile

3 Copy an existing generator test profile to a new generator test profile:

```
benchmark profile clone name <name> to <String[45]>
```

where

name <name>	is the profile that you want to clone.
name <String[45]>	is the user-defined name for the new profile.

4 Modify the payload and traffic parameters for the test profile:

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-17
Displaying generator test profiles

Display generator test profiles when you want to confirm settings or get a list of configured profiles.

The report provides details on the configurations used to run the test. The results are provided by frame size or EMIX and by PCP if a PCP list is provided. When the profile KPI is set, a pass or fail is reported for each frame size and PCP tested. If the KPI profile is not referenced no pass/fail is reported. If a KPI profile is used but no CPI data is available for the PCP being tested, "---" is shown to indicate that no KPI was configured.

You can display

- generator test profile information
- a detailed list of all profiles

Step	Action

To display generator test profile information

1 Display generator test profile information:

```
benchmark profile show
```

To display a detailed list of all profiles

2 Display a detailed list of all profiles:

```
benchmark profile show name <profile-list>
```

where

name <profile-list> is the list of profile names, separated by commas.

—end—

Example

The following example shows sample output for the benchmark profile show command.

```
> ben prof show

+---------------------------- BENCHMARK Test Profiles Config ----------------------------+
| Id  |       Name          | Ref | Bandwidth | HW         | EMIX       | PCP BW   | KPI      |
|     |                     |     |           | Sessions   | Sequence   | Profile  | Profile  |
+-----+---------------------+-----+-----------+------------+------------+----------+----------+
| 1   | dot1q               | 2   | 400.00    |      1     | simple     | none     | base     |
| 2   | untagged            | 1   | 180.00    |      1     | simple     | none     | base     |
| 3   | dot1q-pcp0          | 0   | 30.00     |      1     | emix_test  | none     | base     |
+-----+---------------------+-----+-----------+------------+------------+----------+----------+
```


Copyright© 2022 Ciena® Corporation

The following example shows sample output for the benchmark profile show name command for a profile named test10.

```
+--------------------- Generator Profile Information --------------------+
|         name:  test10                                                  |
|           id:  1                                                       |
|  references:  4                                                        |
|                                                                        |
| Configuration parameters:                                              |
|          interval:  Completion                                         |
|          duration:  Once                                               |
|         bandwidth:  100   Mbps                                         |
|  excess bandwidth:  0     Mbps                                         |
|   frame size list:  64   128  256  512  1024 1280 1518 2048 9216       |
|    vid validation:  on                                                 |
|  color validation:  on                                                 |
|    pcp validation:  on                                                 |
|      max searches:  16                                                 |
|       max samples:  10                                                 |
| sampling interval:  1000   msec                                        |
|      frameLoss BW:  max-throughput                                     |
|       KPI profile:  general                                            |
|    PCP BW profile:  none                                               |
|      EMIX pattern:  tcp                                                |
|   Req HW Sessions:  1                                                  |
|                                                                        |
| Payload parameters:                                                    |
|          dest MAC:  00:23:8a:43:16:4c                                  |
|   vlan encap type:  dot1q                                              |
|               vid:  10                                                 |
|               PCP:  0                                                  |
|             color:  green                                              |
|              TPID:  0x8100                                             |
|    source IP addr:  0.0.0.0                                            |
|      dest IP addr:  0.0.0.0                                            |
|           IP dscp:  0                                                  |
|          PDU type:  UDP Echo                                           |
|                                                                        |
| Custom payload parameters:                                             |
|              size:  0x0000                                             |
|           content:  (first 48 bytes only)                              |
|                     00 00 00 00 00 00 00 00 00 00 00 00                |
|                     00 00 00 00 00 00 00 00 00 00 00 00                |
|                     00 00 00 00 00 00 00 00 00 00 00 00                |
|                     00 00 00 00 00 00 00 00 00 00 00 00                |
|                                                                        |
| Benchmark tests configured:                                            |
|        throughput:  enabled                                            |
|           latency:  enabled                                            |
|               PDV:  enabled                                            |
|         frameloss:  disabled                                           |
|            outage:  disabled                                           |
|           rfc2544:  disabled                                           |
|             y1564:  disabled                                           |
|                                                                        |
| Test instances association:                                            |
|       referencing:  4                                                  |
+------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-18
Configuring test attributes

You can:

- update the test configuration for an existing benchmark generator test profile
- reset the configuration for an existing benchmark generator test profile to the default values
- add or remove a frame size from a frame size list

Update the test configuration if you want the generator to run with a configuration other than the default settings.

A test profile cannot be edited or changed if it is being used by a running test instance. This includes changing the configuration, traffic or payload attributes of a test profile.

Reset the test configuration if you changed the generator configuration but now want it to run with the default settings.

For a throughput test, if traffic profiling (CIR/EIR) is configured on the test port Ciena recommends the following profile configuration to ensure the most accurate results:

- the bandwidth setting is 40% higher than the expected throughput
- the maximum searches is set to 16
- the sampling interval is set to 100

These settings ensure that the traffic profile is tested while providing the most accurate throughput test results.

Step	Action

To update the test configuration for an existing benchmark generator test profile

1 Update the test configuration for an existing benchmark generator test profile:

```
benchmark profile configuration set name <String[45]>
[bandwidth <INT [0..10000]>] [excess-bandwidth <INT
[0..10000]>] [duration <15Min|1Hr|6Hr|24Hr|Indefinite|
Once|custom>] [custom-duration <15min to 65535mins>]
[interval <15Min|1Hr|2Hr|6Hr|Completion>] [frame-size-
list <INT 64..9216>[1..10] [max-bw-search <INT 1..16>]
[max-samples <INT 2..20>] [sampling-interval <INT
1..600>] [frameloss-start-bw <profile-bandwidth|max-
```


Copyright© 2022 Ciena® Corporation

```
throughput>] [emix-sequence <emix-sequence-object>]
[kpi-profile <kpi-profile-object>] [bw-allocation-
profile <bw-allocation-profile-object] [vid-validation
<on|off>] [pcp-validation <on|off>] [color-validation
<on|off>]
```

where

name <String[45]>	is the name of the profile.
bandwidth <INT [0-10000]>	is the bandwidth in Mbps to start testing with. The default value is the maximum operational speed of the port under test.
excess-bandwidth <INT [0-10000]>	:is the bandwidth in Mbps to use with yellow colored traffic if and only if the profile is set for multi-color testing. The default value is 0.
duration <15Min|1Hr|6Hr|24Hr|Indefinite|Once|Custom>	:is the length of time allowed for the tests to run. The default value is Once. A duration of Once cannot be used with the outage test enabled.
custom-duration	is the length of time in minutes (15..65535) allowed for the custom duration tests to run. The duration parameter must be set to “custom” to use this parameter. The default value is 15min.
interval <15Min|1Hr|2Hr|6Hr|Completion> e-size-list <INT 64..9216>[1-10]	:is the amount of time for one iteration of the tests to take. If all selected tests have not completed before the interval timer goes off, the iteration is stopped and the next iteration is started (if duration permits). The default value is completion.
frame-size-list <INT 64..9216>[1-10]	is the list of frame sizes in bytes, to use for the tests. The default list includes the following packet sizes: 64, 128, 256, 512, 1024, 1280, 1518, 2048 and 9216. The last two sizes, 2048 and 9216, are only valid for non-rfc2544 tests. The maximum number of elements in the list is 10. The first frame size in the default list is adjusted to 84 if IPv6 dot1q is configured.
max-bw-search <INT 1-16>	is the maximum number of searches to perform for a successful bandwidth for a given packet size. This attribute is specific to the throughput test. The default value is 7.
max-samples <INT 2-20>	is the maximum number of timestamp samples taken during the test. This attribute is specific to the latency and pdv tests. The default value is 10.

Copyright© 2022 Ciena® Corporation

where

sampling-interval <INT 1-600>	is the number of milliseconds, in 100ms steps, to wait in between each sample (latency and PDV) or statistics read (throughput and frameloss). The valid range is 1 to 600 steps for a range of 100ms to 60sec. The default value is 1 for a sampling interval of 100ms.
frameloss-start-bw <profile-bandwidth| max-throughput>	indicates which bandwidth to use when starting the test. This attribute is specific to the frameloss test. Valid values are: • profile-bandwidth: the bandwidth specified in the profile or 1000Mbps if not specified • max-throughput: the successful bandwidth determined by the throughput test for the packet size being tested. The default value is max-throughput.
emix-sequence <emix-sequence>	is the EMIX sequence to use for testing. When set, this attribute is used instead of the frame size list attribute.
kpi-profile <kpi-profile>	is the KPI profile to use for analyzing the test results.
bw-allocation-profile <bw-allocation-profile>	is the bandwidth allocation profile to use when testing against the configured PCP values.
vid-validation <on|off>	indicates whether vid validation for test packets coming back to the generator is on or off. The default is on. If set to off, color and pcp validation settings are disregarded and automatically turned off.
pcp-validation <on|off>	:indicates whether the pcp value of the outer tag is used to classify the returning packets. The default value is on. Set the pcp-validation attribute to off when the PCP is expected to change as the test packet travels through the network.
color-validation <on|off>	:indicates whether color (DEI bit value) of the putter tag is used to classify the returning packets. The default value is on. Set the color-validation attribute to off if the color is expected to change as the test packet travels through the network.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-19
Configuring traffic test types

Configure traffic test types to control what type of tests you want the generator to run.

You can choose to run one or more traffic test types or the standard RFC2544 or Y1564 test suites.

Benchmarking supports these test types:

- throughput
- latency
- packet delay variation (PDV)
- frame loss
- outage
- RFC 2544, which comprises standard throughput, latency, and frame loss at maximum line rate
- Y.1564, which comprises throughput, latency, frame loss, and PDV. An EMIX must be configured in the profile or at the default generator level to run Y.1564

  Note 1: Y.1564 and RFC2544 are mutually exclusive: they cannot both be enabled at the same time.

  Note 2: The outage test cannot be set if duration is set to once, and vice versa.

  Note 3: The outage test can only be configured with a single PCP and color. It is preferable to use green traffic.

You can

- select the traffic test types for an existing benchmark generator test profile
- clear the selected the traffic test types for an existing benchmark generator test profile

  Note: If the port being tested is down, the system in not able to determine the maximum line rate of the port under test. As a result, it is unable to determine if the generator max rate exceeds the port under test maximum rate/speed.

Copyright© 2022 Ciena® Corporation

At least one test must be configured for the start command to be successful on the associated test instance or test instances.

Step	Action

To select the traffic test types for an existing benchmark generator test profile

1 Select the traffic test types for an existing benchmark generator test profile:

```
benchmark profile traffic set name <name> [throughput]
[latency] [pdv] [frameloss] [outage] [rfc2544] [y1564]
```

where

name <name>	is the profile to configure.
throughput	is the throughput test.
latency	is the latency test.
pdv	is the packet delay variation (PDV) test.
frameloss	is the frame loss measurement test.
outage	is the outage test. ***Note:*** Unnecessary micro-outages may be triggered if the full line rate is used for the outage test.
rfc2544	is a suite of tests that includes throughput, latency, and frame loss. Whenever RFC2544 is enabled, a test will run at full line rate with a sampling interval of 1 minute, 20 samples (latency) and start bandwidth of full line rate for frame loss.
y1564	is a suite of tests that includes Throughput, Frameloss, Latency and PDV. Emix-sequence must be configured either at the profile level or at the generator level.

To clear the selected traffic test types for an existing benchmark generator test profile

2 Clear the selected traffic test types for an existing benchmark generator test profile:

```
benchmark profile traffic unset name <name> {[throughput]
[latency] [PDV] [frameLoss] [outage] [rfc2544] [y1564]
```

where

name <name>	is the profile to configure.
throughput	is the throughput test.
latency	is the latency test.
PDV	is the PDV test.
frameLoss	is the frame loss measurement test.

Copyright© 2022 Ciena® Corporation

where

outage	is the outage test.
rfc2544	is a suite of tests that comprises throughput, latency, and frame loss.
y1564	is a suite of tests the comprises throughput, latency, frame loss and PDV. EMIX needs to be configured to use this test.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-20
Configuring payload information

Configure the Layer 2 and IP payload information to be included in the test packets sent from the generator.

Disabling the validation of vid, pcp and/or color can subject the test to inaccurate measurements if spurious traffic from sources other than the originating generator are directed at the MAC address of the generator/ collector.

Previous statistics for the targeted profile are cleared if any of the following are changed:

- VLAN ID
- destination MAC
- frame size list
- adding a frame size to the list
- removing a frame size from the list
- setting and unsetting rfc2544 test
- changing profile bandwidth
- emix
- bw-allocation-profile
- sampling-interval
- encapsulation-type
- excess-bandwidth

You can:

- update the payload information for an existing benchmark generator test profile
- reset the payload information for an existing benchmark generator test profile to default values

Step	Action

Copyright© 2022 Ciena® Corporation

To update the payload information for an existing benchmark generator test profile

1 Update the payload information for an existing benchmark generator test profile:

```
benchmark profile payload set name <name> [dstmac <MAC
address: XX:XX:XX:XX:XX:XX>] [vlan-encap-type
<untagged|dot1q>] [c-vid <INTEGER 1-4094>] [c-pcp <list
of INTEGER 0-7>] [c-color < color green|yellow|green-
yellow|green-yellow-red>] [tpid <NUMBER: 0x8100|0x88A8]
[pdu-type <ethernet|ip|udp-echo>] [ip-src-addr <IP
address>] [ip-dest-addr <IP address>] [ip-dscp <NUMBER:
0-63>][custom-payload <String>]
```

where

name <name>	is the profile to configure.
dstmac <MAC address: XX:XX:XX:XX:XX:XX>	is the MAC address assigned to the RFC2544 reflector. • If using a Ciena UNI reflector, run the benchmark show command on the UNI reflector. The Local MAC Address of the UNI reflector is the destination MAC address for the generator in an L2 test. When going over an IP cloud, the dst-mac should be that of the edge router connected to the generator. • If using a Ciena static reflector, on the acting device, run the interface show ip-interface <interfaceName> command on the IP interface configured for reflecting RFC2544 test packets. The MAC value displayed by the command is the destination MAC address to configure in the generator. • When running through an IP cloud, the dstmac should be the MAC address on the edge router you are connected to.
vlan-encap-type <untagged| dot1q>	is the L2 encapsulation type. The default is untagged.
c-vid <INTEGER 1-4094>	is the VLAN ID to program in the C-TAG when dot1q. To disable, set to 0 using the c-vid unset.
c-pcp <list of INTEGER 0-7>	is the list of PCPs to test with. This attribute is only used in dot1q configuration. If the outage test is set/enabled, only one PCP can be configured.
c-color <color green|yellow| green-yellow| green-yellow-red>	is the list of colors to test with. This attribute is only used in dot1q configuration. If the outage test is set/enabled, only one color can be configured. It is preferable it use green.
tpid <NUMBER: 0x8100 |0x88A8>	is the Tag Protocol Identifier (TPID) in hexadecimal format. The default value is 0x8100.
pdu-type <ethernet|ip|udp-echo>	is the Layer 2 test PDU type. The default value is ethernet.

Copyright© 2022 Ciena® Corporation

where

ip-src-addr <IP address>	is the IP source address which can be either IPv4 or IPv6; however, both source and destination IP addresses must be of the same type. The IP source address is optional, and will be resolved using the IP address of the benchmark IP interface if it exists or of the management interface. In IPv6, the first global address found is the one used. If both source and destination IP address are not set and the selected PDU type is IP or UDP echo, the default source IP address of 198.18.1.2 and the default destination IP address of 198.18.1.3 are used.
ip-dest-addr <IP address>	is the IP destination address, which can be either IPv4 or IPv6; however, both addresses must be the same type. If both source and destination IP address are not set and the selected PDU type is IP or UDP echo, the default source IP address of 198.18.1.2 and the default destination IP address of 198.18.1.3 are used.
ip-dscp <NUMBER: 0-63>	is the value to program in the DSCP field of the IP header for IP and UDP-echo frames. The default value is 0.
custom-payload <String>	is the custom byte pattern to be used to fill the packet's payload area to the required packet size. It is a string of up to 256 hexadecimal characters. This string can be defined in the form of "\x00" to "\xFF" (with double quotes), and defines a specific bit pattern to be used in the data part of the generated packet. The pattern is repeated as required depending on the size of the packet being tested. You can use \x in front of an hex value if you want a non-printable character in your string but ensure that it is follow by 2 hex digits, such as, "\x01", but not "\x1". For example, a custom PDU payload of the string "\xFFABC\x01def\x00heLLO!" translates to the hex array of FF 41 42 43 01 64 65 66 00 68 65 4C 4C 4F 21.

Copyright© 2022 Ciena® Corporation

To reset the payload information for an existing benchmark generator test profile to default values

2 Reset the payload information for an existing benchmark generator test profile to default values:

```
benchmark profile payload unset name <name> [dstmac]
[vlan-encap-type] [c-vid] [c-pcp] [c-color] [tpid] [pdu-
type] [ip-src-addr] [ip-dest-addr] [ip-dscp][custom-
payload]
```

where

name <name>	is the profile to configure.
dstmac	is the MAC address assigned to the targeted UNI reflector.
vlan-encap-type	is the L2 encapsulation type. The default is untagged.
c-vid	is the VLAN ID to program in the C-TAG when dot1q.
c-pcp	is the list of PCPs to test with. This attribute is only used in dot1q configuration. The default value is PCP 0 only.
c-color	is the list of colors to test with. This attribute is only used in dot1q configuration. The default value is green.
tpid	is the Tag Protocol Identifier (TPID) in hexadecimal format. The default value is 0x8100.
pdu-type	is the Layer 2 test PDU type. The default value is ethernet.
ip-src-addr	is the IP source address which can be either IPv4 or IPv6; however, both source and destination IP addresses must be of the same type. If both source and destination IP address are not set and the selected PDU type is IP or UDP echo, the default source IP address of 198.18.1.2 and the default destination IP address of 198.18.1.3 are used.
ip-dest-addr <IP address>	is the IP destination address, which can be either IPv4 or IPv6; however, both addresses must be the same type. If both source and destination IP address are not set and the selected PDU type is IP or UDP echo, the default source IP address of 198.18.1.2 and the default destination IP address of 198.18.1.3 are used.
ip-dscp <NUMBER: 0-63>	is the value to program in the DSCP field of the IP header for IP and UDP-echo frames. The default value is 0.
custom-payload <String>	is the custom byte pattern to be used to fill the packet's payload area to the required packet size. It is a string of up to 256 hexadecimal characters.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-21
Creating test instances

Create a reflector test instance to indicate which service to reflect.

You can create and enable multiple reflector test instances to support reflection on multiple services simultaneously. See Table 6-5 for maximum number of test instances that can be enabled or running simultaneously.

You can configure 128 test instances for the reflector on a 39XX/51XX switch.

> ***Note:*** The key for a test instance with vtag-stack * is a super set of any other c-vid specific test instance or untagged. Therefore, if such a test instance is already enabled, the user will not be able to enable any other test instances. On the reverse side, if a reflector test instance for a specific vtag-stack/c-vid is enabled or an untagged session, the user will not be able to enable a test instance with vtag-stack *.

Test instance parameters cannot be changed; the test instance has to be disabled, deleted and re-created with different parameters. For a reflector, you can only specify vtag-stack or vlan-untagged-data.

Copyright© 2022 Ciena® Corporation

Reflection for the test instance takes place once the test instance is enabled.

Step	Action

1 Enable the benchmark feature:

```
benchmark enable
```

2 Create a test instance:

```
benchmark test create name <Benchmark Test Instance>
[vtag-stack <cvid : INTEGER 1-4094>]] [vlan-untagged-
data]
```

where

name <BenchmarkTest Instance>	is the name of the benchmark test instance.
vtag-stack <cvid>	:the cvid can be any value from 1 to 4094.
vlan-untagged-data	reflect untagged packets.

3 Enable the test instance or test instances:

```
benchmark test enable name <Benchmark Test Instance>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-22
Creating generator test instances

Create generator test instances. A test instance is created from a test profile and associated with a switch: this is the object against which the test is run. The same test profile can be used simultaneously on multiple test instances.

Note the following:

- Test instance parameters cannot be changed; the test instance has to be disabled, deleted and re-created with different parameters.
- You cannot start a test instance if the session key(s) of the test instance conflict with session key(s) of any currently running test instances on the same generator entity. A test instance can translate into multiple sessions; one session per PCP (0 to 7) per color (green or yellow); max 16 sessions per test instance.
- You cannot change a test profile configuration used by a running test instance.

You can save and configure

- up to 128 test instances for each generator entity/instance or switch

Table 6-5 lists limits on the maximum number of test instances that can be running concurrently.

Step	Action
1	Enable the benchmark feature: `benchmark enable`
2	Create a generator test instance: `benchmark test create name <Benchmark Test Instance> [profile <Benchmark Profile Instance>][vtag-stack <cvid > ] [vlan-untagged-data]` where name <Benchmark Test Instance> is the name of the benchmark test instance. profile <Benchmark Profile Instance> is the test profile to use for testing. This is mandatory for generator test instances only and not required for reflector test instances.

Copyright© 2022 Ciena® Corporation

where

vtag-stack <cvid>	:specifies the cvid to test with. The selected profile must be set to vlan-encap-type dot1q for the test instance with specified vtag-stack to be successfully started.
vlan-untagged-data	generate untagged packets. Profile must be set to vlan-encap-type untagged when selecting vlan-untagged-data on the test instance.

3 Enable the test instance or test instances:

```
benchmark test enable name <Benchmark Test Instance>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-23
Starting and stopping generator test instances

Start and stop generator test instances as required for testing.

Table 6-5 lists limits on the maximum number of generator test instances that can be running concurrently.

Note: If one or more of the test instances on the list cannot be started due to some error (conflicting key or not enabled or other), none of the test instances on the list will be started.

Step	Action

To test connectivity to the reflector note prior to starting the generator test

1 Start the connectivity test:

```
benchmark test trigger name <testInst> connectivity-test
```

To start a specified generator test instance or list of test instances

2 Start the test instance or test instances:

```
benchmark test start name {benchmark-test-instance-list}
```

To stop a specified generator test instance or list of test instances

3 Stop the test instance or test instances:

```
benchmark test stop name {benchmark-test-instance-list}
```

To stop all running test instances associated with a generator

4 Stop all test instances associated with a generator

```
benchmark generator stop name <name> all-test-instances
```

To disable all running test instances associated with a generator

5 Disable all running test instances

```
benchmark generator disable name <name> all-test-
instances
```

To sanitize your benchmark configuration, delte all test distances associated with a generator

6 Delete all test instances

```
benchmark generator delete name <name> all-test-instances
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-24
Generating untagged traffic

Generate untagged traffic according to test requirements.

Step	Action

1 Determine the service to be tested.

2 Create a benchmark profile:

```
benchmark profile create name <name>
```

where

name <name>	is the name of the benchmark profile

3 Set the payload parameters:

```
benchmark profile payload set name <name> dst-mac
<reflector-node-mac-addr> pdu-type udp-echo vlan-encap-
type untagged
```

where

name <name>	is the name of the benchmark profile
dst-mac <reflector-node-mac-addr>	is the MAC address of the target reflector node
pdu-type udp-echo	sets the type of test packet to generate to udp-echo
vlan-encap-type untagged	sets the L2 encapsulation type to untagged

4 Set the general configuration parameters for the profile:

```
benchmark profile configuration set name <name> bandwidth
<INT [0..10000]>
```

where

name <name>	is the name of the benchmark profile
bandwidth <INT [0-10000]>	is the bandwidth in Mbps to start testing with. The default value is maximum operational speed of the port under test of the entity.

Copyright© 2022 Ciena® Corporation

5 Set the traffic parameters for the profile to perform throughput and latency tests:

```
benchmark profile traffic set name <name> throughput
latency
```

where

name <name> is the name of the benchmark profile

6 Create a test instance:

```
benchmark test create name <InstanceName> profile <name>
```

where

name <InstanceName> is the name of the test instance

profile <name> is the profile

7 Enable the test instance:

```
benchmark test enable name <InstanceName>
```

8 Start the test instance:

```
benchmark test start name <InstanceName>
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-25
Generating single-tagged traffic

Generate single-tagged traffic according to test requirements.

A benchmark IP interface is only required when sending IP or UDP echo test traffic over in IPv4 network. A benchmark IP interface is not specific to the encapsulation type used.

Step	Action

1 Determine the service or virtual switch to be tested.

2 Attach a benchmark IP interface to the service or virtual-switch being tested:

```
interface create ip-interface <ip-interface> ip <IP
address with mask> service-mac benchmark vlan <vlanId>
ip-forwarding on
```

where

ip-interface <ip-interface>	is a 15-character string to identify the interface.
ip <IP Address with Mask>	is the IP address with mask.
service-mac	is the service name associated with the MAC address
benchmark	sets the role of the IP interface to benchmark
vlan <vlanId>	is the VLAN ID for this interface (port service). When this occurs the ip-interface will obtain its L2 mapping through the use of virtual-switch member configuration. ***Note:*** Ciena recommends to avoid adding more than one port in this VLAN ID
ip-forwarding <on|off>	determines whether IP forwarding is on or off. The default value is off

3 Create a benchmark profile:

```
benchmark profile create name <name>
```

where

name <name>	is the name of the benchmark profile

Copyright© 2022 Ciena® Corporation

4 Set the payload parameters:

```
benchmark profile payload set name <name> dstmac
<reflector-node-mac-addr> pdu-type udp-echo ip-dest-addr
<IP-Addr> vlan-encap-type dot1q
```

where

name <name>	is the name of the benchmark profile
dst-mac <reflector-node-mac-addr>	is the MAC address of the closest edge router, if running over IP cloud
pdu-type udp-echo	sets the type of test packet to generate to udp-echo
ip-dest-addr <IP-Addr>	is the IP address of the benchmark IP interface on the targeted reflector node, if running over an IP cloud. The destination IP address can be IPv4 or IPv6, but has to be of the same type as the source address.
vlan-encap-type dot1q	sets the L2 encapsulation type to dot1q

Note: When the ip-src-addr is not set, the system looks for a benchmark IP interface configured on the specified virtual switch and use its IP address as the source IP address for the test packet. If you choose to not set a benchmark IP interface for the virtual switch, then you must configure ip-src-addr in this step in order for the test instance to be successfully started, or leave both the source and destination addresses unconfigured to use the default addresses.

5 Set the general configuration parameters for the profile:

```
benchmark profile configuration set name <name> bandwidth
<INT [0-10000]>
```

where

name <name>	is the name of the benchmark profile
bandwidth <INT [0-10000]>	is the bandwidth in Mbps to start testing with. The default value is maximum operational speed of the port under test of the entity.

6 Set the traffic parameters for the profile to perform throughput and latency tests:

```
benchmark profile traffic set name <name> throughput
latency
```

where

name <name>	is the name of the benchmark profile

Copyright© 2022 Ciena® Corporation

7 Create the first test instance:

```
benchmark test create name <InstanceName> [vtag-stack
<cvid >][vlan-untagged-data] profile <name>
```

where

name <InstanceName>	is the name of the test instance
vtag-stack <cvid | untagged >	is the cvid to test with. This over-writes the profile configured c-vid values. This can also be set to untagged. But the vtag-stack entered must conform to the encapsulation type configured in the selected test profile for generator test instances.
profile <name>	is the profile

8 Enable the first test instance:

```
benchmark test enable name <InstanceName1>
```

9 Create the second test instance:

```
benchmark test create name <InstanceName2> vtag-stack
<cvid> profile <name>
```

10 Enable the second test instance:

```
benchmark test enable name <InstanceName>
```

11 Start the tests:

```
benchmark test start name <InstanceName1>,
<InstanceName2>
```

—end—

Example

The following commands configure a service to generate regular dot1q traffic in a VLAN setting.

```
vlan create vlan 8
vlan add vlan 8 port 2,6
port set port 2,6 max-frame-size 9216

benchmark create generator name gen1 port 2 mode out-of-service
benchmark generator enable gen1

benchmark profile create name new-york
benchmark profile traffic set name new-york throughput
benchmark profile payload set name new-york dstmac <reflector-
node-mac-addr>
benchmark profile payload set name new-york pdu-type udp-echo
benchmark profile payload set name new-york vlan-encap-type
dot1q
benchmark profile payload set name new-york vid 8
```

The following commands enable benchmark, create a test instance, then start benchmark testing on the newly created test instance.

Copyright© 2022 Ciena® Corporation

```
benchmark enable
benchmark test create name new-york profile new-york
benchmark test enable name new-york
benchmark test start name new-york
```


Copyright© 2022 Ciena® Corporation

Procedure 6-26
Generating double-tagged traffic

Generate double-tagged traffic according to testing requirements.

Note: In a Q-in-Q benchmark test setup, the results for a given packet size will be slightly below the specified profile bandwidth. This is due to the extra four bytes being added for the S-VLAN at the core switch when the port under test and NNI link interpacket gap (IPG) are both set to the default 12 bytes. For the same benchmark configuration, if the NNI link IPG is reduced to eight bytes, the results will slightly increase since the four bytes removed from the IPG are replaced by the four bytes added for the S-VLAN. The end result is the same total frame size sent by the FPGA (test packet + port under test IPG) as the frame size going out of the NNI port (test packet + SVLAN + NNI link IPG).

Step	Action
1	Determine the service or virtual switch to be tested.
2	Create a benchmark profile: `benchmark profile create name <name>` where name <name> is the name of the benchmark profile
3	Set payload parameters: `benchmark profile payload set name <name> dstmac <reflector-node-mac-addr>` where name <name> is the name of the benchmark profile dst-mac <reflector-node-mac-addr> is the MAC address of the target reflector node ip-dest-addr <IP-Addr> is the IP address to program in the destination IP address field of the IP header for IP and UDP echo frames. The destination IP address can be IPv4 or IPv6, but has to be of the same type as the source address.

Copyright© 2022 Ciena® Corporation

4 Set the general configuration parameters for the profile:

```
benchmark profile configuration set name <name> bandwidth
<INT [0-10000]>
```

where

name <name>	is the name of the benchmark profile
bandwidth <INT [0-10000]>	is the bandwidth in Mbps to start testing with. The default value is maximum operational speed of the port under test of the entity.

5 Set the traffic parameters for the profile to perform throughput and latency tests:

```
benchmark profile traffic set name <name> throughput
latency
```

where

name <name>	is the name of the benchmark profile

6 Create the first test instance:

```
benchmark test create name <InstanceName> [vtag-stack
<cvid>] profile <name>
```

where

name <InstanceName>	is the name of the test instance
vtag-stack <cvid | untagged >	is the cvid to test with. if a vtag-stack is specified a C-VID have to be specified.
profile <name>	is the profile

7 Enable the first test instance:

```
benchmark test enable name <InstanceName>
```

8 Create the second test instance:

```
benchmark test create name <InstanceName> vtag-stack
<cvid> profile <name>
```

9 Enable the second test instance:

```
benchmark test enable name <InstanceName>
```

10 Start the tests:

```
benchmark test start name <InstanceName>, <InstanceName>
```

—end—

Example

This example shows creating the vlan and configuring the virtual circuit and virtual switch needed for the benchmark test.

```
vlan create vlan 100
vlan add vlan 100 port 1
virtual-circuit ethernet create vc vc100 vlan 100
```


Copyright© 2022 Ciena® Corporation

```
virtual-switch ethernet create vs vs100 vc vc100
virtual-switch ethernet add vs vs100 port 2
benchmark create generator name gen2 port 2
benchmark enable
benchmark generator enable name gen2

...

benchmark test create name t10 vtag-stack 10 profile dot1q
benchmark test create name t11 vtag-stack 11 profile dot1q
benchmark test enable name t10,t11
benchmark test start name t10,t11
```


Copyright© 2022 Ciena® Corporation

Procedure 6-27
Reflecting untagged traffic

Reflect untagged traffic according to testing requirements.

Step	Action

1 Create a reflector entity:

```
benchmark create reflector name <name> port
<logicalPortEntity> mode <in-service| out-of-service|
vid-out-of-service> [vendor-type <ciena | other>]
```

where

name <name>	is the name of the generator
port <logicalPortEntity>	is the logical port. An aggregate port can be selected only if it the aggregate port does not have more than one member.
mode <in-service| out-of-service| vid-out-of-service>	indicates how customer traffic is treated while testing is active. • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
vendor-type<ciena | other>	Indicates which type of generator device test traffic is expected from. Valid values are: • ciena: test traffic is expected from a Ciena device acting as generator • other: test traffic is expected from a device from another vendor acting as generator

2 Enable the reflector entity:

```
benchmark reflector enable name <name>
```

3 Determine the service to be tested.

4 Associate the reflector entity with the service by creating a test instance:

```
benchmark test create name <benchmark-test>
```

where

name <benchmark-test>	is the name of the benchmark test instance.

5 Enable the test instance:

```
benchmark test enable name <benchmark-test>
```


Copyright© 2022 Ciena® Corporation

—end—

Example

To reflect untagged traffic coming in from the NNI port, the NNI port and the UNI port under test have to be part of a private vlan.

```
vlan create vlan 8
vlan add vlan 8 port 2,6
port set port 2 acceptable-frame-type all
port set port 2,6 max-frame-size 9216

benchmark enable
benchmark reflector enable

benchmark create reflector name ref2 port 2 mode out-of-service

benchmark enable
benchmark reflector enable name ref2
```

Create a benchmark test instance for untagged traffic and enable it

```
benchmark test create name untagged vlan-untagged-data
benchmark test enable name untagged
```


Copyright© 2022 Ciena® Corporation

Procedure 6-28
Reflecting single-tagged traffic

Reflect single-tagged traffic according to testing requirements.

Step	Action

1 Enable the benchmark feature:

```
benchmark enable
```

2 Create a reflector entity:

```
benchmark create reflector name <name> port
<logicalPortEntity> mode <in-service| out-of-service|
vid-out-of-service> [vendor-type <ciena | other>]
```

where

name <name>	is the name of the generator
port <logicalPortEntity>	is the logical port. An aggregate port can be selected only if it the aggregate port does not have more than one member.
mode <in-service| out-of-service| vid-out-of-service>	indicates how customer traffic is treated while testing is active. • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
vendor-type<ciena | other>	Indicates which type of generator device test traffic is expected from. Valid values are: • ciena: test traffic is expected from a Ciena device acting as generator • other: test traffic is expected from a device from another vendor acting as generator

3 Enable the reflector entity:

```
benchmark reflector enable name <name>
```

4 Determine the service to be tested.

Copyright© 2022 Ciena® Corporation

5 Associate the reflector entity with the service by creating a test instance:

```
benchmark test create name <benchmark-test> [ vtag-stack
<cvid> ]
```

where

name <benchmark-test> is the name of the benchmark test instance.

vtag-stack <cvid> :specifies the cvid to test with.

6 Enable the test instance:

```
benchmark test enable name <benchmark-test>
```

—end—

Example

To reflect tagged traffic, the NNI port and the UNI port under test have to be part of same VLAN as the generator on the remote node.

```
vlan create vlan 8
vlan add vlan 8 port 2,6
port set port 2,6 max-frame-size 9216

benchmark create reflector name ref2 port 2 mode out-of-service

benchmark enable
benchmark reflector enable name ref2

benchmark test create name dot1qV8 vid 8
benchmark test enable name dot1qV8
```


Copyright© 2022 Ciena® Corporation

Procedure 6-29
Reflecting double-tagged traffic

Reflect double-tagged traffic according to testing requirements.

Step	Action
1	Enable the benchmark feature: `benchmark enable`
2	Create a reflector entity: `benchmark create reflector name <name> port <logicalPortEntity> mode <in-service| out-of-service| vid-out-of-service> [reflection-level <L2-only | L2-to-L4-IPv4-only | L2-to-L4>}>] [vendor-type <ciena | other>` where name <name> is the name of the generator port <logicalPortEntity> is the logical port. An aggregate port can be selected only if it the aggregate port does not have more than one member.

Copyright© 2022 Ciena® Corporation

where

mode <in-service|out-of-service|vid-out-of-service>	indicates how customer traffic is treated while testing is active. • in-service: customer traffic is not blocked • out-of-service: all customer traffic is blocked • vid-out-of-service: customer traffic is blocked only for the service under test The default value is in-service.
reflection-level <<L2-only | L2-to-L4-IPv4-only | L2-to-L4>}>	Indicates which packet headers require swapping of fields on reflection for reflected test packets to correctly return to the generator. Valid values are: • L2-only: only the source and destination MAC addresses are swapped. Use this value for test traffic over an L2 network. • L2-to-L4-IPv4-only: the system assigns the 10GE reflector and swaps MAC addresses, IPv4 addresses and UDP source and destination ports. • L2-to-L4: the system assigns the 10GE reflector and swaps MAC addresses, IP addresses and UDP source and destination ports.
vendor-type<ciena | other>	Indicates which type of generator device test traffic is expected from. Valid values are: • ciena: test traffic is expected from a Ciena device acting as generator • other: test traffic is expected from a device from another vendor acting as generator

3 Enable the reflector entity:

```
benchmark reflector enable name <name>
```

4 Determine the service to be tested.

5 Associate the reflector entity with the service by creating a test instance:

```
benchmark test create name <benchmark-test> [ vtag-stack
<cvid> ]
```

where

name <benchmark-test>	is the name of the benchmark test instance.
vtag-stack <cvid>	:specifies the cvid to test with. This attribute overwrites the c-vid values configured in the profile.

6 Enable the test instance:

```
benchmark test enable name <benchmark-test>
```

—end—

Copyright© 2022 Ciena® Corporation

Example

To reflect double-tagged traffic, the NNI port and UNI port have to be part of the same virtual switch as the remote generator. The reflector has to be set to reflect using the inner-tag VLAN.

```
vlan create vlan 100
vlan add vlan 100 port 6
virtual-circuit ethernet create vc vc100 vlan 100
virtual-switch add reserved-vlan 200
virtual-switch ethernet create vs vs100 vc vc100
virtual-switch ethernet add vs vs100 port 2 vlan 8 port set port
2,6 max-frame-size 9216

benchmark create reflector name ref2 port 2 mode out-of-service

benchmark enable
benchmark reflector enable name ref2

benchmark test create name dot1qV8 vid 8
benchmark test enable name dot1qV8
```


Copyright© 2022 Ciena® Corporation

Procedure 6-30
Displaying benchmark status information

Display benchmark status information to learn the global status of benchmark and view the list of all configured benchmark entities on the chassis or to learn the configuration and status of a specified entity and view the list of test instances created under the specified entity.

You can display benchmark status information for

- all configured benchmark entities
- a specific benchmark entity

Step	Action

To display benchmark status information for all configured benchmark entities

1 Display benchmark status information for all configured benchmark entities:

```
benchmark show
```

To display benchmark status information for a specified benchmark entity

2 Display benchmark status information for a specified benchmark entity

```
benchmark show name <Benchmark Instance>
```

where

name <Benchmark Instance> is the benchmark entity to show information for

—end—

Example

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

```
>benchmark show
+------------------------------ BENCHMARK State Info -------------------------------+
|            Parameter            |                      Value                      |
+---------------------------------+-------------------------------------------------+
| Admin State                     |                                         enabled |
| Default EMIX Sequence           |                                  Not configured |
| Default KPI Profile             |                                  Not configured |
| Default BW Allocation Profile   |                                  Not configured |
|                                 +-----------------------+-------------------------+
| Benchmark Objects Statistics    |          Max          |        Current          |
|                                 +-----------------------+-------------------------+
|    Entities Configured          |                     1 |                       1 |
|    Test Instances Configured    |                   128 |                       1 |
|                  Enabled        |                    32 |                       1 |
|                  Running        |                    32 |                       0 |
|    Profiles Configured          |                   128 |                       4 |
|    EMIX Sequences Configured    |                    32 |                      10 |
|    KPI Profiles Configured      |                    32 |                       3 |
|    BW Alloc Profiles Configured |                    32 |                       7 |
```


Copyright© 2022 Ciena® Corporation

```
+-------------------------------------------------------------------------------+

+--------- BENCHMARK Entities Configuration and State Info -------------+
|            |           |                   |       |  State   |           |
|   Name     |  Role     |   Mode            | Port  |  Admin   |   Oper    |
+-----------+----------+-------------------+------+----------+----------+
| gen2       |generator | vid-out-of-service| 2    | enabled  | disabled |
+-----------+----------+-------------------+------+----------+----------+
```

The following example shows sample output for a generator benchmark entity named gen1.

```
> benchmark generator show name gen1

+-------------- BENCHMARK Generator Config and State Info --------------+
|       Parameter        |          Value                                |
+-----------------------+-----------------------------------------------+
| ID                     | 1                                             |
| Name                   | gen1                                          |
| Mode                   | vid-out-of-service                            |
| Port                   | 2                                             |
| Emix H Frame Size      | 1526                                          |
| Type                   | Physical Port                                 |
| Admin State            | enabled                                       |
| Oper State             | disabled                                      |
| Local MAC Address      | 2c:39:c1:de:91:ba                             |
| Test Instances         |                                               |
|         Configured     | 1                                             |
|         Enabled        | 1                                             |
|         Running        | 0                                             |
| Bandwidth              |                                               |
|         Available      | 1000.0                                        |
|         Used           | 0.0                                           |
| Hardware Sessions      |                                               |
|         Free           | 31                                            |
|         Used           | 1                                             |
+-----------------------+-----------------------------------------------+

+----------------- BENCHMARK Generator Test Instances ----------------+
|   Name    |   State    |  vtag-stack    |    DA MAC     |   Profile     |
+----------+-----------+---------------+--------------+---------------+
| t10       | stopped    | 10             | ---           | dot1q         |
+----------+-----------+---------------+--------------+---------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-31
Displaying benchmark test information

Display benchmark test information on a generator or a reflector.

You can display benchmark test status information only on a generator to determine if

- any protection switch events are detected while a test is running
- the port under test has a 1:1 LAG/MC-LAG or Y-protection configuration

  Note: For a Benchmark test to provide valid test results, the ports involved in a 1:1 protection configuration under-test must have the same configuration.

Step	Action

To display benchmark test information for all configured benchmark entities on a generator or a reflector

1 Display benchmark test information:

```
benchmark test show name <name>
```

where

name <name> is the benchmark entity to show information for

To display benchmark test status information for all configured benchmark entities on a generator

2 Display benchmark test information:

```
benchmark test show name <name> status
```

—end—

Example

The following example shows sample output for the benchmark generator test show command for the benchmark entity new-york.

```
>benchmark test show name new-york

+---------------- BENCHMARK Test Instance Config and State Info -----------+
|             Parameter                |                    Value             |
+----------------------------------+----------------------------------------+
| ID                                 | 1                                      |
| Name                               | new-york                               |
| Vtag-stack                         | ---                                    |
| Destination MAC Address            | ---                                    |
| Admin State                        | enabled                                |
| Oper State                         | stopped                                |
| Suspect Flag                       | True                                   |
| Port Protection Switch Count       | 4                                      |
| Port Last Protection Switch Time   | Fri Jan  7 18:39:48 2000               |
```


Copyright© 2022 Ciena® Corporation

```
| Last Time Started                 | Never started                          |
| Profile running config            | new-york                               |
|    Interval                       | Completion                             |
|    Duration                       | 15Min                                  |
|    Bandwidth                      | 500    Mbps                            |
|    Excess bandwidth               | 0      Mbps                            |
|    Frame size list                | 84                                     |
|    vid validation                 | on                                     |
|    color validation               | on                                     |
|    pcp validation                 | on                                     |
|    max searches                   | 7                                      |
|    max samples                    | 10                                     |
|    sampling interval              | 100    msec                            |
|    frameloss start BW             | max-throughput                         |
|    KPI Profile                    | none                                   |
|    Required HW sessions           | 1                                      |
|    Destination MAC                | 00:23:8a:8f:1d:f6                      |
|    VLAN encapsulation             | dot1q                                  |
|    C-VID                          | 1001                                   |
|      PCP                          | 0                                      |
|      color                        | green                                  |
|    TPID                           | 0x8100                                 |
|    PDU type                       | UDP Echo                               |
|    source IP address              | 198.18.1.2                             |
|    destination IP address         | 198.18.1.3                             |
|    IP dscp                        | 0                                      |
|    Tests configured               | throughput                             |
+-----------------------------------+----------------------------------------+

+--------------------------- Session Keys ---------------------------------+
| Entity ID |        Dest MAC    |  cVid  | cPCP | cCFI | untagged |  Mask  |
+-----------+--------------------+--------+------+------+----------+--------+
| 1         | 00:23:8a:8f:1d:f6 |  1001  |   0  |   0  |     0    | 11111  |
+-----------+--------------------+--------+------+------+----------+--------+
```

The following example shows sample output for the benchmark test show status command for the benchmark entity new-york.

```
>benchmark test show name new-york status
+------------------------- BENCHMARK Test Instance Status Info -------------+
| Name                                | new-york                            |
| Test Instance Oper State            | stopped                             |
| Test Instance Suspect Flag          | False                               |
| Test session id 0                   |                                     |
|    PCP                              | 0                                   |
|    Color                            | green                               |
|    Throughput                       | Idle                                |
|    FrameLoss                        | Idle                                |
|    Latency                          | Idle                                |
|    Packet Delay Variation           | Idle                                |
|    RFC2544                          | Idle                                |
|    Y1564                            | Idle                                |
|    Outage                           | Idle                                |
|    Current Interval                 | 0                                   |
|    Total Intervals                  | Unknown                             |
+-------------------------------------+-------------------------------------+
```

The following example shows sample output for the benchmark reflector test show command for the benchmark entity test1.

Copyright© 2022 Ciena® Corporation

```
>benchmark test show name test1

+----------------- BENCHMARK Test Instance Config and State Info ----------+
|              Parameter              |                    Value             |
+-------------------------------------+--------------------------------------+
| ID                                  | 2                                    |
| Name                                | test1                                |
| Vtag-stack                          | 1002                                 |
| Admin State                         | enabled                              |
| Oper State                          | reflecting                           |
| Suspect Flag                        | True                                 |
| Port Protection Switch Count        | 1                                    |
| Port Last Protection Switch Time    | Fri Oct 11 11:43:07 2019             |
| Running Configuration               |                                      |
|    Vtag-stack                       | 1002                                 |
+-------------------------------------+--------------------------------------+


  +--------------------------------- Session Keys ---------------------------------+
  | Entity ID |        Dest MAC         |  cVid  | cPCP | cCFI | untagged |  Mask  |
  +-----------+-------------------------+--------+------+------+----------+--------+
  | 1         | c4:83:6f:82:2c:fa       |  1002  |   0  |   0  |     0    |  11001 |
  +-----------+-------------------------+--------+------+------+----------+--------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-32
Displaying benchmark test statistics

Display benchmark test statistics on a generator to learn more about the test results.

Step	Action
1	Display benchmark test statistics: `benchmark test show name <name> statistics` where name <name> is the benchmark entity to show information for

—end—

Example

The following example shows sample statistics output for the benchmark test show command for the benchmark entity generator new-york.

```
>benchmark test show name new-york statistics

+------------------------------------------- BENCHMARK Test Results and Statistics ---------------------------------------------+
| Test instance new-york using profile new-york dest MAC 00:23:8a:8f:1d:f6 and vtag-stack 1001                                  |
|---------------------+-------------------------------------------------------------------------------------------------------|
| Suspect Flag        |False                                                                                                  |
|---------------------+-------------------------------------------------------------------------------------------------------|
|                     | Results for green traffic based on requested bandwidth of 500 Mbps                                    |
|                     |-----+-----------------+----------+----------+----------+-----------------------------+-------------------+
|                     |     |      Frame      |          |          |          |          KPI                |                   |
|                     | PCP |      Size       |   Min    |   Avg    |   Max    |   %     (Mbps)      Result  |        Iter       |
|                     |-----+-----------------+----------+----------+----------+-------------------+---------+-------------------+
| Throughput (Mbps)   |  0  |      0          |  --      |  --      |  --      |  --    (   --   ) |  --     |       0           |
|                     |-------------------------------------------------------------------------------------------------------+
| Statistics          |                                                                                                       |
| Matching Test       |                                                                                                       |
|   RX pkts           |    0                                                                                                  |
|     IPv4 all        |      0                                                                                                |
|       IPv4 UDP      |        0                                                                                              |
|     IPv6 all        |      0                                                                                                |
|       IPv6 UDP      |        0                                                                                              |
|     non IP          |      0                                                                                                |
|     unrecognized    |      0                                                                                                |
|   RX seq num stats  |    0                                                                                                  |
|     Dupl seq        |      0                                                                                                |
|     Out-of-order seq |      0                                                                                                |
|     Disc in seq     |      0                                                                                                |
|   TX pkts           |    0                                                                                                  |
+---------------------+-------------------------------------------------------------------------------------------------------+
```

The following example shows sample statistics output for the benchmark test show command for the benchmark entity reflector test1.

```
>benchmark test show name test1 statistics

+----------------------+-------------------------------------------------+
| Statistics           |                                                 |
| Matching Test        |                                                 |
|   RX pkts            |    0                                            |
|     IPv4 all         |      0                                          |
|       IPv4 UDP       |        0                                        |
|     IPv6 all         |      0                                          |
|       IPv6 UDP       |        0                                        |
```


Copyright© 2022 Ciena® Corporation

```
|     non IP            |      0                                          |
|     unrecognized      |      0                                          |
|   TX pkts             |    0                                            |
+----------------------+-------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-33
Displaying reflector global statistics

Display benchmark reflector statistics.

Information for a reflector instance provide a sum of all the test packets and bytes received and transmitted, along with the number of packets received with no match, CRC errors, or UDP checksum errors.

Step	Action

To display reflector information

1 Display reflector information:

```
benchmark reflector show
```

To display port information

2 Display port information:

```
benchmark reflector show name <name> {statistics}
```

where

name <name>	is the name of the reflector instance to show information for
statistics	shows port information

—end—

Example

The following example shows sample output for the benchmark reflector show command.

```
> benchmark reflector show

+---- BENCHMARK Reflector Entities Configuration and State Info --+
|              |                              |        State        |
|    Name      |   Mode                 | Port  |  Admin   |   Oper   |
+--------------+--------------------+-------+----------+----------+
| refDefault   | vid-out-of-service | 2     | enabled  | enabled  |
+--------------+--------------------+-------+----------+----------+
```

The following example shows sample output for the benchmark reflector show name command for a reflector named ref3.

```
> benchmark reflector show name ref3

+-------------- BENCHMARK Reflector Config and State Info --------------+
|       Parameter       |          Value                                |
+-----------------------+-----------------------------------------------+
| ID                    | 1                                             |
| Name                  | refDefault                                    |
| Mode                  | vid-out-of-service                            |
| Port                  | 2                                             |
| Type                  | Physical Port                                 |
```


Copyright© 2022 Ciena® Corporation

```
| Generator Vendor Type | ciena                                          |
| MAC Validation        | on                                             |
| Admin State           | enabled                                        |
| Oper State            | enabled                                        |
| Local MAC Address     | 00:03:18:86:17:ae                              |
| Test Instances        |                                                |
|         Configured    | 1                                              |
|         Enabled       | 1                                              |
| Bandwidth Available   | 1000.0                                         |
| Hardware Sessions     |                                                |
|         Free          | 0                                              |
|         Used          | 1                                              |
+-----------------------+------------------------------------------------+
+------------------ BENCHMARK Reflector Test Instances ------------------+
|                   Name                    |   State    |   vtag-stack   |
+-------------------------------------------+------------+----------------+
| t100                                      | reflecting | 100            |
+-------------------------------------------+------------+----------------+
+-------------- BENCHMARK Reflector Config and State Info --------------+
|       Parameter        |          Value                                |
+------------------------+-----------------------------------------------+
| ID                     | 2                                             |
| Name                   | ref3                                          |
| Mode                   | in-service                                    |
| Port                   | 3/1                                           |
| Type                   | Physical Port                                 |
| Generator Vendor Type  | ciena                                         |
| Reflection Level       | L2-to-L4                                      |
| Admin State            | disabled                                      |
| Oper State             | disabled                                      |
| Local MAC Address      | 00:23:8a:09:4b:d8                             |
| Test Instances         |                                               |
|         Configured     | 0                                             |
|         Enabled        | 0                                             |
| Bandwidth Available    | 10000.0                                       |
| Hardware Sessions      |                                               |
|         Free           | 512                                           |
|         Used           | 0                                             |
+------------------------+-----------------------------------------------+
+--------------- BENCHMARK Reflector Test Instances ----------------+
|        Name      |     Sub-port     |   State    |   vtag-stack   |
+------------------+------------------+------------+----------------+
| No test instance configured for this benchmark entity             |
+------------------+------------------+------------+----------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 6-34
Clearing reflector global statistics

Clear benchmark reflector statistics.

Note: In releases prior to 6.16, running the benchmark reflector clear statistics command resets the next expected sequence number to 1.

Step	Action
1	Disable the reflector to disable all reflecting test instances and clear their statistics: `benchmark reflector disable name <name>`
2	Clear benchmark reflector global statistics on the 10GE reflector: `benchmark reflector clear name <name> statistics` where name <name> — name of reflector instance to clear statistics for statistics — clears benchmark reflector global statistics on the 10GE reflector. Clearing reflector stats clears global counters such as rx no match, udp checksum errors, crc errors and total number of packets received and transmitted.
3	Enable the reflector to disable all reflecting test instances and clear their statistics: `benchmark reflector enable name <name>`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-35
Clearing benchmark reflector test instance statistics

Clear benchmark reflector test instance statistics.

Step	Action
1	Disable the reflector test instance: `benchmark test disable name <name>`
2	Clear statistics for the benchmark reflector test instance: `benchmark test clear name <name> statistics` where name <name> name of reflector instance to clear statistics for statistics
3	Enable the reflector test instance: `benchmark test enable name <name>`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 6-36
Clearing generator test instance statistics

Clear benchmark generator test instance statistics. Only the statistics specific to the generator are cleared.

Running the benchmark test instance clear statistics command resets the sequence number of the next packet to be generated to 1. Accompany this command with a reflector clear stats command which also resets the next expected sequence number to 1. If the reflector is used to reflect traffic from multiple generators/sessions at the same time, then the reflector sequence number related statistics are meaningless.

The statistics displayed by a test instance show statistics command are: test results (specific to the profile) and FPGA statistics counters (related to the active test instance). Issuing the clear command against a disabled test instance clears all saved results and statistics. Issuing the clear command against the enabled but stopped test instance clears all saved results as well as current hardware session FPGA counters.

Step	Action

1 Stop the generator test:

```
benchmark test stop name <test-instance-list>
```

where

name <profile-list>	is the profile being stopped. You can supply at list of profile names already running to be stopped, separated by a comma.

2 Clear benchmark generator test profile statistics:

```
benchmark test clear name <test-instance-list> statistics
```

where

name <test-instance-list>	clears the accumulated results and statistics for the specified list of test instances.
statistics	clears test instance statistics and results.

—end—

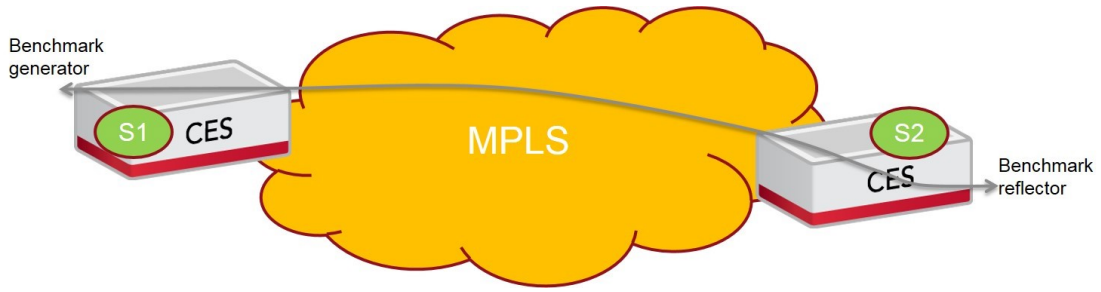
Copyright© 2022 Ciena® Corporation

Procedure 6-37
Configuration example for MPLS

This example shows a reflector and generator configuration example based on the connection shown in Figure 6-7. For more information on MPLS functionality, see the *39XX/51XX Switches and Platforms MPLS Configuration Guide*.

> ***Note:*** The vid-out-of-service mode over MPLS based service (VPLS and VPWS) represents that all VLAN IDs bundled for the service-under-test are taken out-of-service. This blocks ingress or egress traffic. All other VLAN-IDs mapped to other services on the port-under test remain able to transmit/receive client traffic. Vid-out-of-service mode over MPLS-based services is equivalent to ac-out-of-service.

Figure 6-7
Sample configuration



Setup of the benchmark generator and a MAC agnostic reflector (no generator MAC address is configured on the reflector) to test traffic for a service running over MPLS:

```
S1>
gmpls tp-tunnel create rsvp-ingress-corout tnl_50-52 dest-ip
11.11.11.11

mpls l2-vpn create dynamic-vc vpws_EPL fec-129 agi vpws_EPL saii
s3 taii s11 peer 11.11.11.11 tp-tunnel-ingr-corout tnl_50-52

virtual-switch ethernet create vs vpws_EPL mode vpws
virtual-switch ethernet add vs vpws_EPL port 1
virtual-switch ethernet attach mpls-vc vpws_EPL vs vpws_EPL

benchmark create generator name GenP1 port 1
benchmark generator set name GenP1 mode out-of-service
benchmark generator enable name GenP1
benchmark enable
```


Copyright© 2022 Ciena® Corporation

```
benchmark profile create name TestProfile
benchmark profile traffic set name TestProfile throughput
benchmark profile payload set name TestProfile dst-mac
2c:39:c1:84:2c:f5
benchmark profile payload set name TestProfile vlan-encap-type
dot1q
benchmark test create name Test123 profile TestProfile vtag-
stack 123
benchmark test enable name Test123

S2>
mpls l2-vpn create dynamic-vc vpws_EPL fec-129 agi vpws_EPL saii
s11 taii s3 peer 3.3.3.3 tp-tunnel-egrs-corout-dynamic tnl_50-
52

virtual-switch ethernet create vs vpws_EPL mode vpws
virtual-switch ethernet add vs vpws_EPL port 1
virtual-switch ethernet attach mpls-vc vpws_EPL vs vpws_EPL

benchmark create reflector name RefP1 port 1
benchmark reflector set name RefP1 mode out-of-service
benchmark reflector enable name RefP1
benchmark enable
benchmark test create name Test123 vtag-stack 123
benchmark test enable name Test123
```

Verification

1 Start the benchmark generator:

```
S1> benchmark test start name Test123
```

2 Verify the stats of the benchmark generator:

```
> benchmark generator show name GenP1 statistics

+-------------------- BENCHMARK Entity Statistics ---------------------+
| Entity:             GenP1                                            |
| Admin State:        enabled                                          |
| Oper State:         enabled                                          |
+----------------------------------------------------------------------+
| Statistic          | Value                                           |
+----------------------------------------------------------------------+
| RX CRC pkts        | 0                                               |
| RX Udp Chksm pkts  | 0                                               |
| RX no match pkts   | 0                                               |
| RX pkts            | 327990                                          |
| TX pkts            | 327990                                          |
+----------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

Network management IP interface

This chapter shows the commands for configuring static IP routing. 39xx/51xx switches support IPv4 and IPv6.

Note 1: To configure and run IP static routing, you need to install the Advanced-OAM license key. To obtain the Advanced-OAM license key, contact Ciena Sales.

Note 2: For an example of configuring Static IP routing to support RFC 2544 benchmark testing refer to *Fault and Performance Management*.

Static IP routing comprises the following components:

- IP Interface ending and receiving.
- IP Loopback, which enables IP packets to ingress and egress over the same interface.
- Static IP routes, which defines static IP routes.
- Forward Information Base (FIB), which stores static route and forwarding information.
- Static Address Resolution Protocol routes, which defines ARP static routes.
- Adjacency Information Base (AIB), which stores ARP static route and adjacency information.

IPv6

IPv6 is the successor to IPv4. IPv6 provides a larger address space and greater flexibility when assigning addresses.

IPv6 address format

IPv6 addresses have the following characteristics:

- Addresses are 128-bits in length and are written as eight groups of 4 hexadecimal digits. For example:
  0001:0002:0003:0004:0005:0006:0007:0008
- Fields are separated by colons (:)
- Numeric field values are 0-FFFF

Copyright© 2022 Ciena® Corporation

- Two colons together (::) can be used as a shorthand to represent some number of all-zeros hexadecimal fields. The doubled colon can appear at the beginning, the middle, or at the end of the address. Only one pair of doubled colons can be used in an address. For example: ::1 or f:: are both valid addresses.

Ciena platforms accept most address forms called out in RFC4291, and emit only address forms called out in RFC5952, but (per this RFC section 4.2.2) Ciena platforms do not accept a double-colon that does not compress away more than 16 bits of address, that is, 1:2:3:4:5:6::8 is not legal.

IP address usage

On an IPv6-enabled network, each network element can have multiple multicast, anycast, and unicast addresses. IPv6 is most secure when used in a unicast deployment, that is, one host to another host. Multicast and anycast use one-to-many connections and are not recommended in a secure environment.

Table 7-1 summarizes IPv6 address types.

Table 7-1
IPv6 address types and IPv4 equivalent

IPv6 name	Description	IPv4 equivalent	Description
Anycast	One-to-nearest. Uses Global Unicast Addresses. Routers only. Discovery uses.	Unique protocols in IPv4, for example, IGMP.	Addresses are indistinguishable from a normal unicast address. Anycast (router-to-router) is also used with IPv4 addresses, specifically with DNS root servers, though there may be other instances.
Global Unicast	Globally unique. Fully routable. Assigned by IANA/ Regional Internet Registries (RIRs).	Global IP address	IPv6 and IPv4 similar but IPv6 can have other scoped addresses.
Link-Local	Local LAN only. Automatically assigned based on MAC. Cannot be routed outside local LAN. Scoped address concept new to IPv6. Multicast can also be scoped to link.	No real equivalent. Assigned IPv4 over ARP'd MAC.	Scoped address concept new to IPv6. Multicast may also be scoped to link-local (RFC 4489).

Copyright© 2022 Ciena® Corporation

Table 7-1
IPv6 address types and IPv4 equivalent

IPv6 name	Description	IPv4 equivalent	Description
Loopback	Local interface scope.	Same as IPv4 127.0.0.1	Same function
Multicast	One-to-many. Hierarchy of multicasting.	Similar to IPv4 Class D	Significantly more powerful than IPv4 version. No broadcast in IPv6, replaced by multicast. Multicast may also be scoped to link-local (RFC 4489).
Site-Local	Optional. Local Site only. Cannot be routed over Internet. Assigned by user.	Private network address with multi-homed interface is closest equivalent.	Scoped address concept new to IPv6. Unlike the IPv4 private network address the IPv6 device can have, Link-Local, Site-Local and a Global Unicast address. Site-Local while continuing to exist in the IPv6 specification is currently not supported.

IPv6 architecture allows an interface to have multiple addresses, for example, link-local or global. 39xx/51xx switches also support IPv6 and IPv4 addresses. The rules for selecting the address to use in a particular situation are the following:

- Address pairs of the same scope or type (link-local, global) are preferred.
- A smaller scope for the Destination address is preferred, that is, use the smallest scope possible.
- A non-deprecated address is preferred.
- Transitional addresses, that is, IPv6 to IPv4 addresses, are not used if native IPv6 addresses are available.
- If all criteria are similar, address pairs with the longest common prefix are preferred.
- For source addresses, global addresses are preferred over temporary addresses.
- The attribute “interface” when adding a gateway is only required if the gateway address is an IPv6 link-local address.

Each interface can have multiple IPv6 addresses in addition to the IPv4 addresses. 39xx/51xx switches support the use of up to 16 IPv6 addresses per interface.

Copyright© 2022 Ciena® Corporation

IPv4 and IPv6 dual stack

The addition of IPv6 capability in the dual stack mode allows for the assignment of multiple addresses per interface. TCP timestamps can be configured on or off, reset to default values or displayed.

Multiple IPv6 addresses

Multiple IPv6 addresses can be configured per interface. The number of addresses that can be assigned to an interface is up to 13:

- One IPv4 address
- One link-local IP v6 address
- Eight IPv6 auto-created addresses
- Two manually configured IPv6 addresses

Multiple gateways

IPv6 allows for the assignment of multiple gateways. Unlike IPv4, the configuration of the default gateway is not mandatory, as hosts can automatically determine the existence of a router on the local network via the router advertisement. The manual configuration of a single IPv6 gateway is also allowed. A configured default gateway has a higher precedence over an automatically advertised gateway.

This chapter provides the following procedures for IP management:

- "Creating interfaces" on page 7-27
- "Deleting an IP or loopback interface" on page 7-30
- "Modifying an IP or loopback interface" on page 7-31
- "Enabling and disabling an IP interface" on page 7-32
- "Configuring IPv6 interfaces manually" on page 7-33
- "Displaying an IP interface" on page 7-35
- "Creating an IPv6 interface" on page 7-38
- "Configuring IPv6 stack settings" on page 7-40
- "Setting IPv6 stack settings to default values" on page 7-42
- "Enabling and disabling an IPv6 stack" on page 7-43
- "Displaying IPv6 stack settings" on page 7-44
- "Configuring IPv4 stack settings" on page 7-45
- "Setting IPv4 stack settings to default values" on page 7-46
- "Displaying IPv4 stack settings" on page 7-47
- "Configuring interface TCP stack settings" on page 7-48
- "Setting interface TCP stack settings to default values" on page 7-49

Copyright© 2022 Ciena® Corporation

- “Displaying TCP stack settings” on page 7-50
- “Adding an IP route” on page 7-55
- “Removing an IP route” on page 7-56
- “Displaying the routing table” on page 7-57
- “Displaying FIB entries” on page 7-58
- “Enabling Layer 3 switching” on page 7-60
- “Disabling Layer 3 switching” on page 7-61
- “Adding a static ARP entry” on page 7-66
- “Removing static ARP entries” on page 7-67
- “Displaying static ARP entries” on page 7-101
- “Displaying the AIB table” on page 7-102

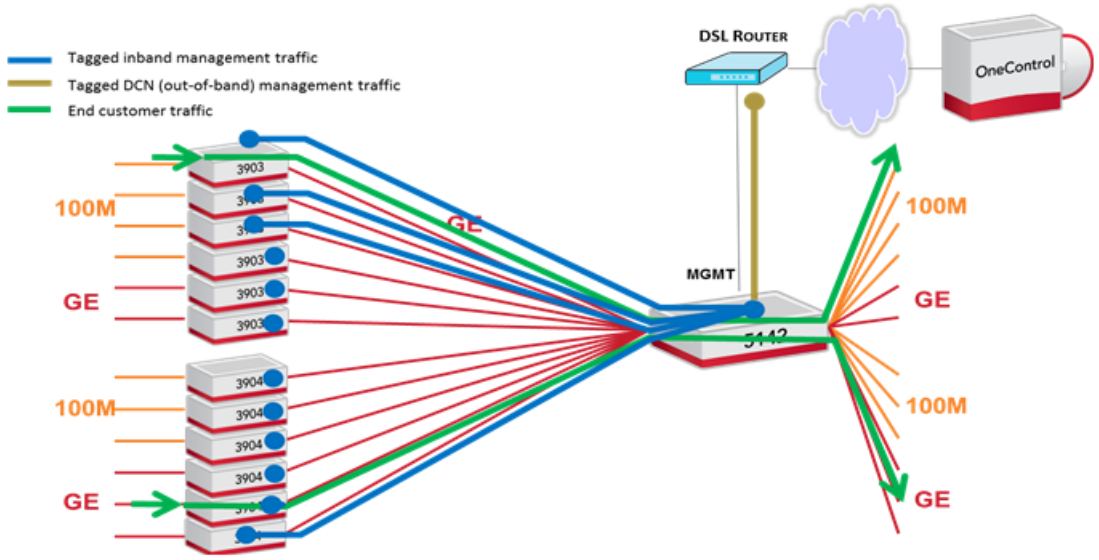
In-band management bridging

In-band management bridging allows in-band management traffic to be sent over the local management port. This frees up traffic from the remote interface that is sent to a DSL router over a faceplate data port. The number of ports dedicated to management plane traffic is reduced, and traffic and port usage is increased.

Figure 7-1 shows how management traffic is aggregated from multiple subtended devices and sent over a local interface (MGMT in the example).

Copyright© 2022 Ciena® Corporation

Figure 7-1
In-band management example



The operator cannot enable the in-band management function using a connection session (such as Telnet) running over the local port. In-band management bridging can only be enabled or disabled by accessing the device by means of the remote interface or the console port. When it is enabled, the local interface cannot be configured directly. You cannot associate a management virtual switch on the remote interface.

> ***Note:*** On initial boot-up, In-band management bridging is disabled by default. If you wish to have it enabled to use Secure Zero Touch Provisioning (SZTP), contact your Ciena sales person.

In-band and out-of-band management traffic has a default VID tag of 127 where the head-end device brings together the remote management traffic from the subtended edge devices and forwards it by means of the local interface. This configurable VID tag value is used when the node is initialized.

> ***Note:*** In-band management bridging is supported on 3903, 3903x, 3904, 3906, 3924, 3926, 3928, 3942, 5142, and 5160.

Copyright© 2022 Ciena® Corporation

Table 7-2 shows the engineering guidelines for in-band management bridging.

Table 7-2
Engineering guidelines

Device	Maximum Number of Subtended Edge Devices	Supported as a head-end device	Supported as subtended edge device
3903	0	*	yes
3903x	0	*	yes
3904	0	*	yes
3906	0	*	yes
3924	12	yes	yes
3926	12	yes	yes
3928	12	yes	yes
3942	12	yes	yes
5142	12	yes	yes
5160	12	yes	yes

Note: * The 3903, 3903x, 3904, 3905 and 3906 can be supported as a head-end device by means of the data faceplate port.

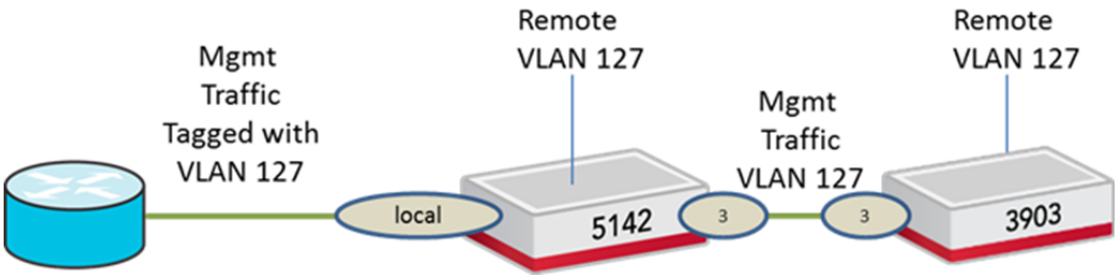
Topology setup

Figure 7-2 shows an example topology setup for in-band management bridging. Management traffic going to the remote interface of the aggregator must be tagged. When a node is initialized, a default management VID tag value of 127 is assigned. The management traffic is tagged with 127, although you can use a different value. The VLAN must be updated to ensure that there is connectivity between the subtended edge devices and head-end devices if they were activated with VLAN 127.

The 5142 acts as the head-end aggregator and the 3903 is one of possibly multiple subtended devices.

Copyright© 2022 Ciena® Corporation

Figure 7-2
Topology setup



VLAN management

The remote interface supports one VLAN which means subtended nodes need to be managed to ensure that they do not get isolated. Subtended nodes can also be added or removed anytime and can execute DHCP and Secure Zero Touch Provisioning (SZTP) using VLAN 127.

Network operators can use a VID other than 127 which could cause the following problems to occur:

- If the head-end device is changed to the new VLAN, subtended devices will not be able to communicate with the head-end device.
- If the subtended edge devices are changed to the new VLAN, they are unable to communicate with the remote interface of the head-end device until the head-end device switches to the new VLAN.
- When the subtended edge devices and the head-end device are migrated to the new VLAN, a new subtended edge device cannot be added on VLAN 127 since the remote interface is no longer associated with VLAN 127.

When migrating from one management VLAN to another, a new reserved IP interface “SubtendedRemote” is automatically added when enabling in-band management bridging and always remains on VLAN 127. This reserved interface allows new nodes to be added after the remote VLAN has been changed from VLAN 127. Subtended devices can also have management data continuity during the VLAN migration.

Local interface interaction

When the management port interface is set to the remote interface, the local interface can no longer be configured. This ensures that the local interface’s configuration does not interfere with the bridge. The admin state of the local interface must be enabled to ensure that the management port is enabled. Since the management port is not available under the port component, the management port can be enabled and disabled from the local interface.

Copyright© 2022 Ciena® Corporation

DHCP client interaction

When in-band management bridging is enabled, the DHCP client first verifies the local port's state. If the port is up, DHCP starts on the local port. If the local port is down, DHCP starts on the remote interface.

DHCP relay interaction (option 82)

The head-end device acts as a DHCP relay agent when configuring the subtended devices. Traffic received from the subtended devices on the remote interface is bridged to the local port. When out-of-band traffic is received on the local port, it is bridged back to the remote interface.

Private forwarding group interaction

In-band management traffic sourced by an edge device is prevented from being forwarded to another edge device in the cluster through the private forwarding group feature.

Traffic profiling

It is important that the management port does not exceed its capacity and that the CPU can process all the management traffic. It is recommended that the committed information rate (CIR) be set to 600.

Limitations

Table 7-3 outlines limitations with in-band management bridging.

Table 7-3
Limitations

Limitation	Description
Remote interface	The IP address and VLAN of the remote interface can be changed when in-band bridging is enabled. If the VLAN is changed, complete the procedure "Modifying the VLAN for in-band management bridging" on page 7-53.
Local interface	You cannot change the local interface parameters when in-band-bridging is enabled. The local interface must be enabled to ensure the local port is enabled.
Traffic rate	The management port is a low bandwidth interface and the traffic rate is limited to 2500 packets per second.

Copyright© 2022 Ciena® Corporation

Table 7-3
Limitations

Limitation	Description
IPv4	When in-band management bridging is enabled, only IPv4 management traffic is forwarded to/from the subtended nodes.
In-band and out-of-band VLAN	Both must have the same VID tag value. The default VID is 127, but the attribute is configurable.
Management VS	A management VS cannot be created and associated with the management interface.
Maximum transmission unit (MTU)	The MTU on the remote interface is limited to 1500 bytes due to the limitation on the local port.
Private forwarding group	Private forwarding group is not supported on the local port.
Traffic looping	Traffic looping is not detected on the local port.
Quality of service	Quality of service is not supported on the local port. Traffic is untagged while going through the bridge. The only data path section where quality of service is supported is when the traffic does out the remote interface. The traffic is then prioritized according to the priority set in the remote interface CLI configuration. The default remote interface does not have a configurable priority and the default is set to 7.

The following protocols/features are not supported on the local management port:

- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- G.8032 rings
- Link Level Discovering Protocol (LLDP)
- aggregation
- TWAMP/RFC 2544

Copyright© 2022 Ciena® Corporation

This chapter provides the following procedures for in-band management bridging:

- “Configuring in-band management bridging” on page 7-51
- “Modifying the VLAN for in-band management bridging” on page 7-53

EVC ping

EVC ping is used by network operators to test connectivity through end-to-end networks through an Ethernet Virtual Connection (EVC). Network operators can initiate a ping of the remote EVC endpoint (NTE-2) before scheduling deployment and testing of new equipment. EVC ping is configured using IP interface and virtual switch members.

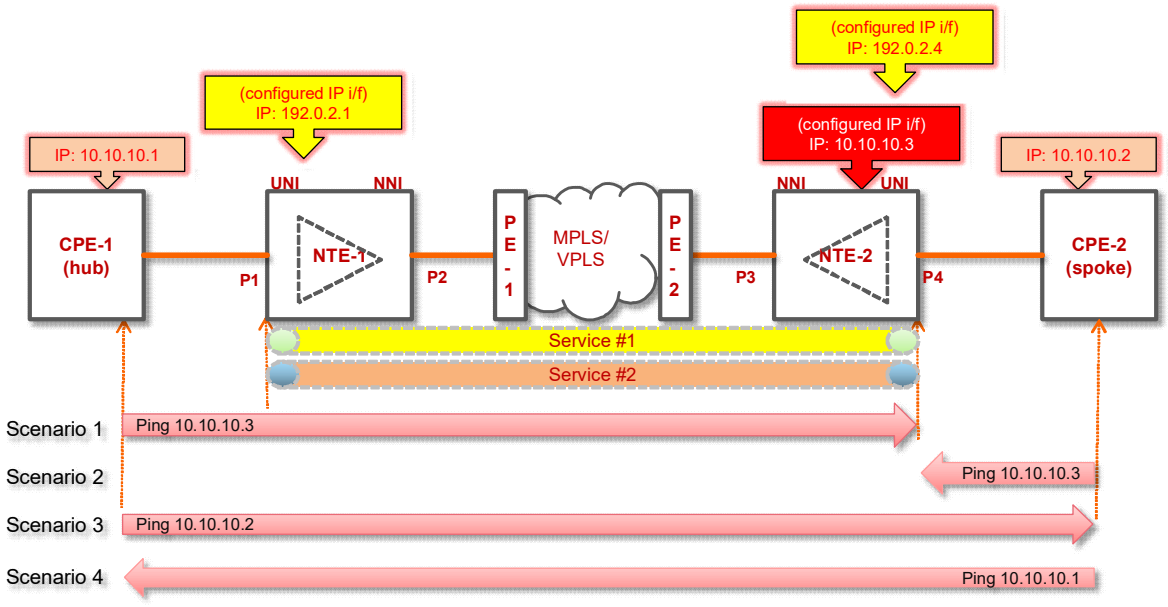
EVC ping can be used for EVPL and EPL services in IPv4-based and IPv6-based networks.

When EVC ping is enabled, the NTE must be configured with an IP interface whose IP address is coordinated with the network operator. Each IP interface must be in its own subnet, and must not already be configured on the NTE.

Frames with any DSCP priority are accepted: frame treatment is subject to the provisioned SLAs in the network. No special priority is given to this ping traffic.

Figure 7-3 and Figure 7-4 show EVC ping in the end-to-end network.

Figure 7-3
EVC ping in the end-to-end IPv4 network



Copyright© 2022 Ciena® Corporation

Figure 7-4
EVC ping in the end-to-end IPv6 network

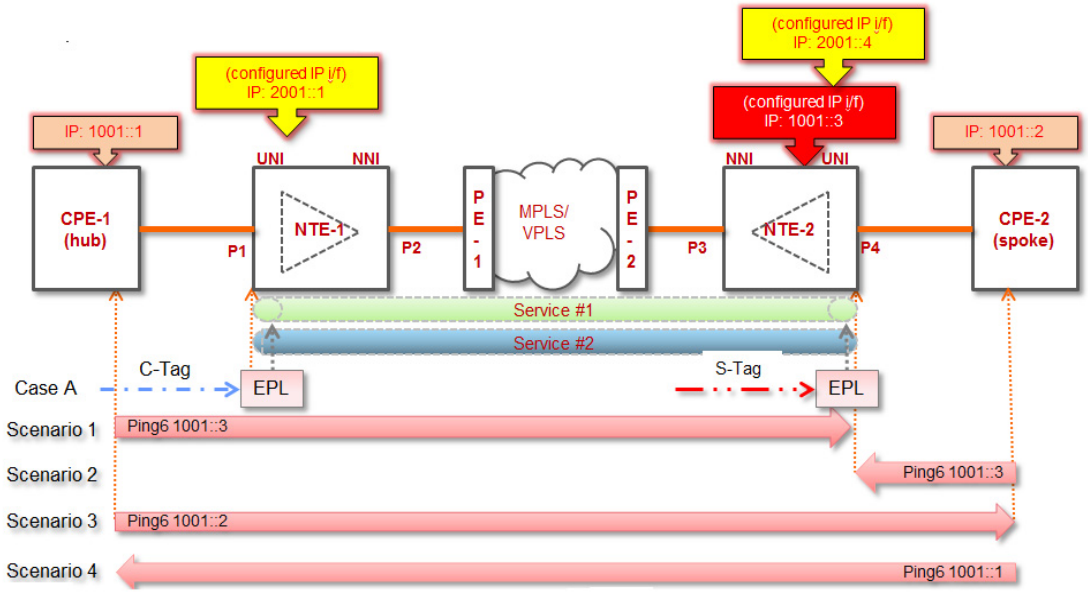


Table 7-4 lists EVC ping use cases. Port-based service can have tagged or untagged traffic sent from the network operator. VLAN-based service must have tagged traffic, coordinated with the network operator.

Table 7-4
EVC ping use cases

Use case	Service on NTE-1 (hub)	Ping/ARP packet on NTE-1 UNI	Service on NTE-2 (spoke)	VLAN tag stack depth at NTE-2 NNI	Ping/ARP packet on NTE-2 UNI
A	port-based	tagged	port-based	2	tagged
B	port-based	untagged	port-based	1	untagged
C	VLAN-based	tagged	port-based	1	untagged
D	port-based	untagged	VLAN-based	2	tagged
E	VLAN-based	tagged	VLAN-based	2	tagged

EVC ping can be configured for

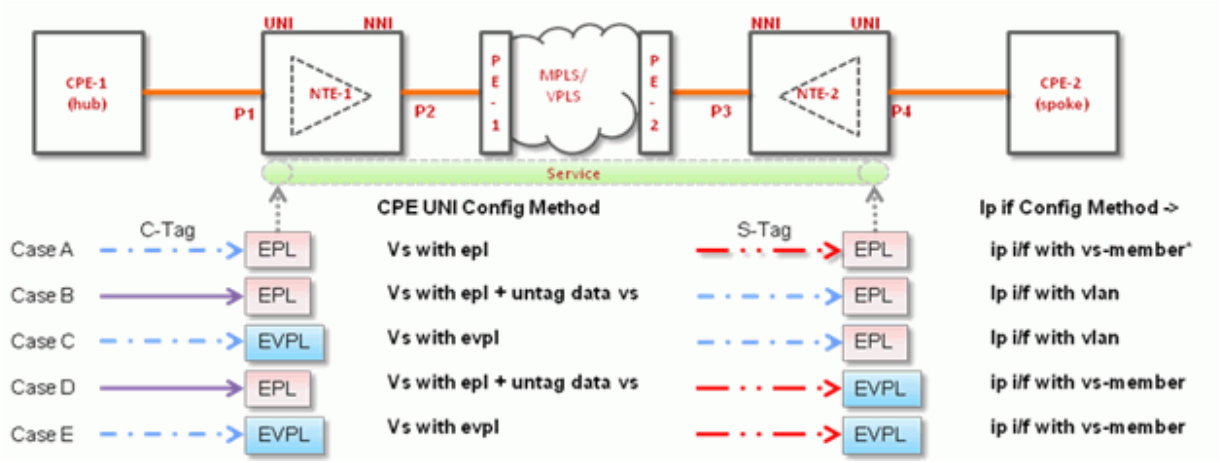
- Use case A: virtual switch with EPL to IP interface with virtual switch member
- Use case B: virtual switch with EPL and untagged data virtual switch to IP interface with VLAN

Copyright© 2022 Ciena® Corporation

- Use case C: virtual switch with EVPL to IP interface with VLAN
- Use case D: virtual switch with EPL and untagged data virtual switch to IP interface with virtual switch member
- Use case E: virtual switch with EVPL to IP interface with virtual switch member

Figure 7-5 shows EVC ping use cases.

Figure 7-5
EVC ping use cases



This chapter provides the following procedures for EVC ping:

- “Configuring EVC ping for use case A” on page 7-68
- “Configuring EVC ping for use case B” on page 7-73
- “Configuring EVC ping for use case C” on page 7-78
- “Configuring EVC ping for use case D” on page 7-82
- “Configuring EVC ping for use case E” on page 7-88

Local EVC ping

A local EVC interface ping is an ICMP request and reply stream between an external device connected by means of membership in an EPL or EVPL virtual switch. The ip-interface that responds is located at the nearest EPL or EVPL member access to the virtual switch. For a remote EVC interface ping request, the ip-interface that responds is located at the far-end EPL or EVPL member access to the virtual switch.

Figure 7-6 and Figure 7-7 show local and remote EVC ping in IPv4 and IPv6 networks.

Copyright© 2022 Ciena® Corporation

Figure 7-6
Local and remote EVC ping in an IPv4 network

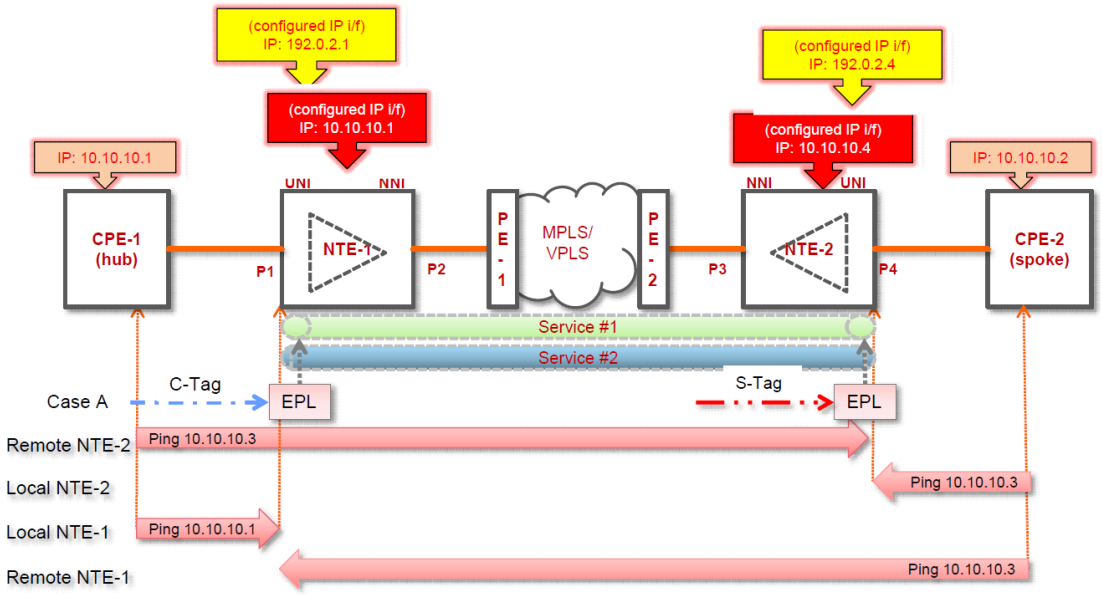
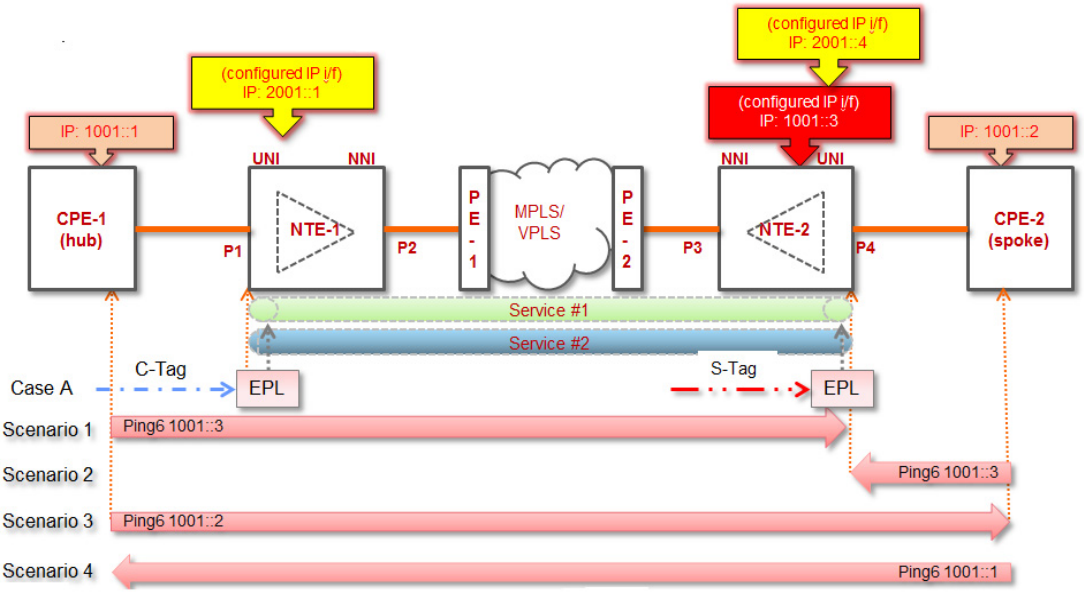


Figure 7-7
Local and remote EVC ping in an IPv6 network



Local EVC interface ping and remote interface EVC ping are handled differently when the IP interface pinged is configured as an SVLAN interface or a virtual switch member interface, that is, double-tagged.

Copyright© 2022 Ciena® Corporation

When the virtual switch member is used as EPL, the virtual switch member can require the following configuration on the UNI port to ensure proper datapath and VLAN flooding domain:

- untagged-data-vs, which is used when untagged traffic is used into a virtual switch.
- untagged-data-vid, which is used when untagged traffic is used in to a virtual switch and a specific ip-interface can be requested to be the recipient of the ICMP traffic.

Table 7-5 summarizes EVC ping from a local virtual switch member with SVLAN ip-interface.

Table 7-5
EVC ping from local virtual switch member with SVLAN ip-interface

Use case	Default port configuration	untagged-data-vs configured	Explanation
Untagged traffic	No replies to ARP and ICMP traffic	ARP and ICMP traffic are replied to normally	When untagged-data-vs is set, the traffic is accepted and replied by the SVLAN ip-interface.
Normal tagged traffic any CVID	No replies to ARP and ICMP traffic	No replies to ARP and ICMP traffic	The CVID traffic is not matched to the ip-interface.

Table 7-6 summarizes EVC ping from local virtual switch member with virtual switch member ip-interface.

Table 7-6
EVC ping from local virtual switch member with virtual switch member ip-interface

Use case	Default port configuration	untagged-data-vs configured	Explanation
Untagged traffic	ARP and ICMP traffic are replied to normally	ARP and ICMP traffic are replied to normally	When untagged-data-vs and untagged-data-vid are set, the traffic is accepted and replied by the virtual switch member ip-interface.
Normal tagged traffic any CVID	No replies to ARP and ICMP traffic	No replies to ARP and ICMP traffic	The CVID traffic is not matched to the ip-interface.

Copyright© 2022 Ciena® Corporation

Note: Inserting Static ARP entries can lead to undesired behavior of ICMP traffic. Do not use static ARP entries in an EVC ping testing environment.

Auxiliary ping

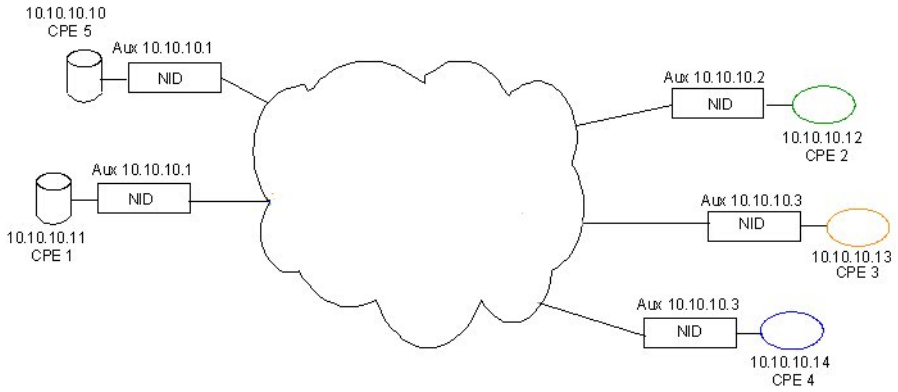
Auxiliary ping provides a special IP interface called the auxiliary interface. This interface is used to "ping" from the customer premises equipment (CPE) to the network interface (NID). The auxiliary IP interface can be targeted as the ping destination, regardless of the service used, or even if there are no services configured on the NID. Traffic to and from the auxiliary IP interface cannot be routed. An auxiliary interface does not need to be unique within the network. Any two nodes that wish to ping each other cannot have the same auxiliary IP address. For example, if Node A pings Node B, they cannot both have the IP address 10.10.10.1.

Auxiliary ping is supported on 3903, 3903x, 3904, 3905, 3906, 3924, 3926, 3928, 3942, and 5142 devices.

Auxiliary ping scope

Figure 7-8 illustrates a typical network. Ciena NTEs act as NID devices.

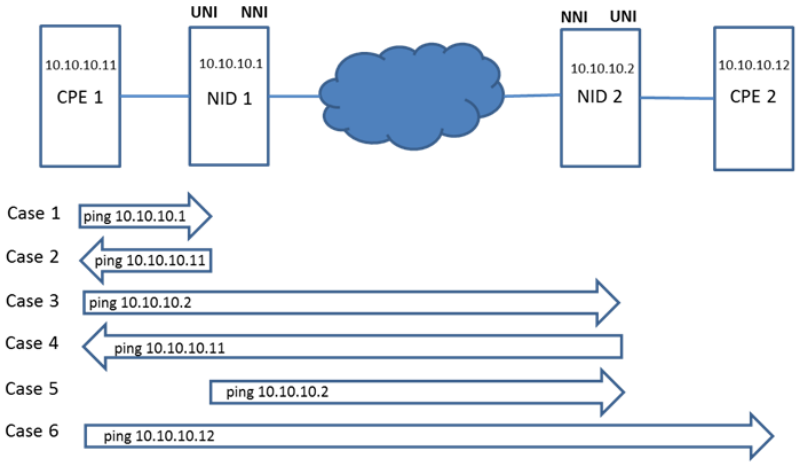
Figure 7-8
Typical network



Within the network in Figure 7-9, there are several auxiliary ping use case scenarios.

Copyright© 2022 Ciena® Corporation

Figure 7-9
Use cases



The use cases show traffic arriving at a NID which is addressed to the auxiliary IP interface of that NID being extracted from the normal data path. This is necessary, as the VLAN the packets are tagged with may not exist on the port that the packet arrived on. Normal Ethernet forwarding behavior drops such a packet. As all incoming ARP/ICMP echo packets targeted at the auxiliary IP interface address are extracted from the normal forwarding path before they can be dropped, any operations that would usually be performed by the normal forwarding path such as ingress transforms and translations are not performed on those packets.

When a NID responds to a packet that was targeted at the auxiliary IP interface, the response packet is generated with the same tag header information as the corresponding request packet. It will be sent directly out of the same port the corresponding request packet was received on. These response packets must bypass the normal forwarding path, or the packet will be dropped if the VLAN is not configured on the device. No egress transforms or translations are applied to the response packet as may have happened if it had used the normal forwarding path.

Copyright© 2022 Ciena® Corporation

Table 7-7 outlines the use cases described in Figure 7-9.

Table 7-7
Use cases

Use case number	Description
1 — local test, CPE to NID	When a NID is dropped at a customer site, the EVCs are not yet configured. The connectivity to the local NID must be verified by initiating a ping to the local NID. You can also ping the local NID if connectivity is lost to all remote sites. Any VLAN or even untagged frames could be used in this ping request.
2 — local test, NID to CPE	The NID can also originate a ping to the local CPE to allow the NOC to confirm connectivity issues observed in use case 1. Any VLAN or untagged frames can be used in this ping request, so the normal forwarding path is not used. The NOC engineer specifies the exact VLAN tag header information to be placed on the AROP/ICMP echo packets as a “vtag-stack” parameter in the ping command, and specifies the UNI port that the ARP/ICMP echo packets are sent out on using the “egress-port” parameter in the ping command.
3 — remote test, CPE to NID	If you are at a host site and you want to check the connectivity to a remote NID, initiate a ping using the VLAN assigned to the EVC that connects to the remote NID, and the remote NID’s IP address. The packet passes through the local NID transparently using the normal forwarding path, as it is not targeted at the auxiliary IP address of that NID. Any transforms or translations configured on the local NID for this services are applied. At the remote NID, the packets (which are targeted at the auxiliary IP interface of that device) are extracted from the normal forwarding path before any transforms/translations are applied, and the corresponding response packets also bypass the normal forwarding path and are transmitted back out of the same port, with the same vlan tag header.

Copyright© 2022 Ciena® Corporation

Table 7-7
Use cases

Use case number	Description
4 — remote test, NID to CPE	The NID may also originate a ping to the remote CPE to allow the NOC to confirm any connectivity issue observed in use case 3. The NOC engineer specifies the exact VLAN tag header information to be placed on the ARP/ICMP echo packets as a “vtag-stack” parameter in the ping command, and also specifies the UNI port that the ARP/ICMP echo packets are sent out on using the “egress-port” parameter in the ping command. The NOC engineer provides the “vtag-stack” parameter as the VLAN tag(s) assigned to the EVC that connects to the remote CPE (as seen on the wire at the NNI link), and specifies the egress port (the NNI port on which that EVC connection exists). The packets generated by the initiating NID bypass the normal forwarding path, so any transforms/translations normally being performed on the packets within this EVC must be reflected in the vtag-stack parameter information provided in the command. The ping traffic passes through the other NID transparently (as it is addressed to the IP of the CPE, not to the auxiliary IP address of the other NID). The response packets pass through the local NID transparently using the normal forwarding path. The remote NID (where they are targeted at the auxiliary IP interface) are again extracted from the normal forwarding path and processed regardless of any tagging information.
5 — NID to NID	The NID can also originate a ping to another NID for troubleshooting purposes. The normal forwarding path is bypassed on both the originating and terminating NID devices. The tag header and port to be used is specified in the ping command on the originating NID.
6 — CPE to CPE	Pings may be performed from CPE to CPE, but this is not actually an auxiliary ping scenario, and ping traffic passes through the NID devices transparently, as it is neither originated nor terminated on an auxiliary IP interface.

This chapter provides the following procedures for auxiliary ping:

- “Configuring an auxiliary IP interface” on page 7-103
- “Generating a ping” on page 7-104

Connectivity

The auxiliary ping shows that there is physical connectivity between two devices over the port specified as the egress port in the originating auxiliary ping command. It does not prove that there is complete end-to-end connectivity over an EVC. In the case of a CPE that is directly connected to a local NID, a ping originated over the port that connects to that CPE succeeds even if no such EVC was configured on the NID.

Copyright© 2022 Ciena® Corporation

If a CPE originates a ping to the auxiliary interface of a remote NID, the EVC must exist across the network between the CPE and the node prior to the remote NID, but the remote NID successfully responds even if the EVC is not properly configured for that EVC in which case a CPE-to-CPE ping needs to pass through that remote NID on the normal forwarding path or fail. This results because the auxiliary interface (remote NID) must be able to respond to a ping even if there is no such EVC/service configured on that NID.

SNMP

There is no MIB that captures Ping output". The only configuration item that is relevant is the new role type of "auxiliary" on the IP interface, within the WWP-LEOS-IP-INTERFACE-MIB. The WWP-LEOS-IP-INTERFACE-MIB does not support SNMP "set" operations on the WwpLeosIpDataInterfaceTable, so the only activity relevant here is that a get of the wwpLeosIpDataInterfaceRole object within the WwpLeosIpDataInterfaceEntry will return a value of "auxiliary" if the interface entry being retrieved is that of the auxiliary interface.

Security

The auxiliary interface traffic is not limited in being sent to the CPU. It will, however be placed on a separate, lower priority, CPU queue from all of the CPU destined traffic. This ensures that a denial of service attack launched at the auxiliary IP interface will not affect other features on the device.

Traffic bearing the auxiliary interface MAC are placed on this CPU queue, regardless of the packet type. Once packets reach the CPU, auxiliary interface packets that are not ARP or ICMP Echo are dropped. The number of ARP and ICMP Echo requests/response packets that are accepted on a per-port basis using the existing "flow cpu-rate-limit" feature may be limited through software.

TPID

Acceptable TPID value(s) on auxiliary ping packets are dependent on the box-wide TPID setting and the port type.

Ports which have a QiQ VS member configured on them can only accept untagged or single tagged auxiliary ping traffic. For single-tagged packets with the box-wide TPID feature enabled ("vlan enable inner-tpid"), then the acceptable TPID is the value which is configured under "vlan set inner-tpid". If the feature is not enabled, then the only acceptable TPID value is 0x8100.

If auxiliary ping packets bearing any other TPID arrives on a QiQ VS member port it will be dropped.

Ports which do not have a QiQ VS member configured on them can accept untagged, single-tagged or double-tagged auxiliary ping traffic. For single-tagged packets, the TPID can take any of these values: 0x8100, 0x88a8 or

Copyright© 2022 Ciena® Corporation

0x9100. For double-tagged packets, the outer TPID can be either 0x8100, 0x88a8 or 0x9100. The inner-tpid must match the configured box-wide TPID setting if the box-wide TPID feature is enabled. Otherwise, it must be 0x8100.

Access control lists

Hardware access control list (ACL) profiles can be associated with a layer 2 or layer 3 entity. Layer 2 entities include port, vlan and vs. Layer 3 entities include remote-if, local-if and ip interfaces. The auxiliary interface is not a standard IP interface and it cannot have an ACL profile associated with it. Hardware ACL profile rules that are associated with a port, VLAN or VS are applied to the auxiliary interface traffic that traverses that port, VLAN or VS. Hardware ACLs can be applied to block auxiliary ping traffic from specific sources or on specific ports in the event of a denial of service attack.

Limitations

This section contains the following limitations for auxiliary ping:

- Auxiliary ping supports IPv4 addressing only.
- The auxiliary IP interface address must be within a unique subnet on the device. This means that it cannot have an IP address that is within the same subnet as the remote, local, or any other IP interface configured on that same device.
- Only untagged, single0tagged and double-tagged frames are supported. Triple tagging is not supported.
- Traffic to and from the auxiliary IP interface must not be routed. All auxiliary ping type pings originating from the auxiliary IP interface can only be targeted at devices within the same subnet.
- Packets that originated on or terminated from an auxiliary IP interface will not pass through the normal forwarding path on that device. Normal data path functions, such as the application of translations and transforms, cannot be applied to such packets.
- Any individual device can support the termination of only 10 simultaneous ping sessions. If ping sessions from 11 different originators overlap each other, then some packets may be dropped.
- An individual device cannot support two or more simultaneous ping sessions from the same originator. For example, if the same originating CPE initiates two simultaneous ping sessions on different VLANS some packets may be dropped.
- An individual device cannot support two or more simultaneous/ overlapping ping sessions from the same originating IP address, even if these originated from two or more difference devices that happen to have duplicate IP addresses.

Copyright© 2022 Ciena® Corporation

- An individual device cannot support two or more simultaneous/ overlapping ping sessions to the same destination IP address where there are two or more different destination devices on different VLANs with duplicate IP addresses.
- The maximum size of ping supported is 12,288 bytes. This number includes the Ethernet header with however many tags that may contain.
- The D/F bit cannot be specified in the ping command since the auxiliary IP interface traffic must not be routed at layer 3. Both the source and destination IP address of the ping must be in the same subnet. There is no node along the path of the ping that looks into the IP header to determine the setting of the D/F bit. The D/F bit is set to 1 by the auxiliary ping originating node. Response packets sent to the reflecting node contain the same D/F bit setting as the corresponding request packet.

Double-tagged management interface

Double-tagged management interface allows the virtual switch interface to carry management traffic and not only ICMP traffic. The “role” attribute differentiates between the EVC Ping configuration and the double-tag management configuration.

The role attribute is only available during the creation of the IP interface. The default value for role is “evc-ping” to ensure that previous behavior is maintained. The role attribute is only available for virtual switch member IP interfaces, meaning IP interfaces with no VLAN specified.

Limitations

The following features/protocols are not supported in double-tagged interfaces:

- Triple tagging in frames
- LLDP
- Dying gasp
- Zero Touch Provisioning (ZTP)
- DHCP

See the following procedures:

- “Configuring double-tagged management” on page 7-94.

Configuring egress packet priority on IP interfaces

The egress packet priority can be configured for single and double-tagged interfaces through the CLI. In the case of double-tagged IP interfaces, which include EVC Ping and Double-Tagged Management interfaces, the outer S-VLAN priority can be configured separately from the inner C-VLAN priority. This allows the user to configure S-VLAN and C-VLAN priorities on a per-IP

Copyright© 2022 Ciena® Corporation

interface basis, which provides more control and flexibility over the QoS prioritization of egress IP interface traffic based on a network's demand and capabilities.

The S-VLAN priority on single and double-tagged IP interfaces can specified at the time creation of the interface and modified after creation, as described in the procedures listed at the end of this section.

If not explicitly configured through the CLI, the S-VLAN priority (or pcp) value on single- and double-tagged IP interfaces is set to a value of 7 by default. The C-VLAN priority value on double-tagged interfaces is set to 0 by default if not explicitly configured.

Limitations

Egress packet priority configuration is subject to the following limitations:

- If multiple IP interfaces share the same S-VLAN, the S-VLAN priority is set by the first created and operational IP interface. The user must ensure that all IP interfaces sharing the same S-VLAN have the same S-VLAN priority value or an error will be returned. This is applicable in the following situations:
    - A virtual switch-member IP interface with a parent S-VLAN interface
    - Several virtual switch-member IP interfaces without a parent S-VLAN interface, but that are using the same S-VLAN and different C-VLANs
- If the S-VLAN priority of an IP interface is to be modified, and the interface shares its S-VLAN with other IP interfaces, all other IP interfaces sharing the S-VLAN must be removed before the S-VLAN of the remaining IP interface can be modified.
- The following protocols generate their own custom packets and do not adhere to the S-VLAN or C-VLAN priority values set on the IP interface, even when their packet traffic is egressing the interface:
    - NTP - the S-VLAN and C-VLAN priority values are permanently set to 0.
    - IS-IS - the S-VLAN priority value is permanently set to 7.
    - PTP - for single-tagged PTP traffic, the S-VLAN priority can be set via the PTP CLI and overrides the user-configured IP interface S-VLAN priority. For double-tagged PTP traffic, the C-VLAN priority can be set via the PTP CLI and overrides the user-configured IP interface C-VLAN priority; the S-VLAN priority follows the user-configured IP interface S-VLAN priority.

Copyright© 2022 Ciena® Corporation

- MPLS - all MPLS-generated outgoing packets have their S-VLAN priority values set to 7. If the reply mode is set to IPV4, the reply packet from the target DUT will have the same S-VLAN priority value as the IP interface S-VLAN priority. If the reply mode is set to LSP, the reply packet will have an S-VLAN priority value of 7.

See the following procedures:

- "Creating interfaces" on page 7-27
- "Modifying an IP or loopback interface" on page 7-31
- "Creating an IPv6 interface" on page 7-38
- "Configuring double-tagged management" on page 7-94
- "Creating an unnumbered IP interface" on page 7-97
- "Modifying an unnumbered IP interface" on page 7-100

IP unnumbered interfaces

An IP unnumbered interface (IPUI) is an interface that does not own an IP address. These interfaces borrow IP addresses from other IPv4 interfaces with assigned IP addresses (numbered IP interfaces) or from loopback interfaces. This mechanism allows the network manager to conserve IP addresses, of which there is a limited and declining supply. IPUIs are of particular value in large networks.

A numbered IP interface or loopback interface can be assigned as the donor interface to multiple IPUIs.

The operational state of an IPUI is determined by the state of its donor interface and the IPUI interface's own state. For an IPUI to be in an "up" operational state, both the donor interface state and the IPUI interface state must be "up"; otherwise the operational state of the IPUI is "down". If the donor interface is a numbered IP interface, and the state of the IPUI interface is "up", the operational state of the IPUI will change as the operational state of its donor interface changes. If the donor interface is a loopback interface, the IPUI operational state is determined by the IPUI interface state since the operational status of loopback interfaces is always "up". For this reason, loopback interfaces are recommended, where possible, as donor interfaces for IPUIs.

IPUIs are supported with ospf, ip ping and traceroute commands and with static and dynamic ARP and Link Aggregation (LAG). The "interface show", "interface enable" and "interface disable" commands are supported with IPUIs as they are for numbered IP interfaces.

The following management applications are supported on IPUI:

- Telnet

Copyright© 2022 Ciena® Corporation

- SSH
- xFTP
- SNMP
- Radius
- TACACS
- RMON
- NTP
- DNS
- Syslog

The following management applications are not supported on IPUI:

- LLDP
- Dying Gasp
- ZTP
- DHCP

Limitations

IPUIs are subject to the following limitations:

- IPUI can only be point-to-point interfaces - only one device can be connected to the interface at any time
- the peer end of the connection must also be unnumbered
- the subnet mask of an IPUI connection must be /32 (255.255.255.255)
- an IPUI must have an attached VLAN
- the VLAN attached to an IPUI cannot be modified after it is set
- management interfaces cannot be used as donor interfaces for IPUIs
- static routes over IPUI are not supported
- IS-IS, RSVP and LDP over IPUI are not supported
- Bidirectional Forwarding Detection (BFD) for IP and MPLS Label Switched Paths (LSP) over IPUIs are not supported
- IPUI cannot be used as local or remote management interfaces
- a numbered interface cannot be changed to an unnumbered interface, and vice versa, without first deleting the interface
- IPv6 is not supported for IPUI

See the following procedures:

- “Creating an unnumbered IP interface” on page 7-97
- “Deleting an unnumbered IP interface” on page 7-99

Copyright© 2022 Ciena® Corporation

- “Modifying an unnumbered IP interface” on page 7-100

Virtual switch transform

The benchmark port under test supports i-stamp:push and e-match-pop:stamp. The customer CVID from the UNI side is stamped with a specified value and SVID is pushed before going out to the NNI interface. From the NNI side, SVID in frames is popped out and the original CVID is restored before being sent towards the UNI port.

Copyright© 2022 Ciena® Corporation

Procedure 7-1
Creating interfaces

You can create

- an IP interface
- a loopback interface

Create an IP interface to enable the sending and receiving of Layer 3 traffic. You can differentiate between EVC Ping configuration and double-tagged management configuration.

Create a loopback interface when you need the Layer 3 traffic to ingress and egress from the same interface.

IP and loopback interfaces are used mainly for control plane and MPLS tunnels. Along with MPLS tunnels, IP interface configuration is also required for MPLS-TP. MPLS-TP facilitates

- decoupled control and data plane
- non-IP forwarding interfaces to carry MPLS-TP and LSPs

This results in the configuration of interfaces that are data-only, signaling-only or data and signaling.

IP loopback address uses include router identifier for routing protocols, LDP identifier and MPLS tunnel peer address.

> ***Note 1:*** The IP address and subnet mask for an IP interface cannot define a subnet that is already in use by a local or remote interface.
>
> ***Note 2:*** In SAOS 6.10.2 the ip-forwarding setting is truncated and is not saved in the configuration file. Any SAOS 6.10.2 interfaces with ip-forwarding set to on will have ip-forwarding set to off in the configuration file.
>
> ***Note 3:*** Adding more than one port in the IP Interface can potentially form a loop in the network. Avoid such configurations or enable loop avoidance features on them. Otherwise, the system can enter a bad state.

Copyright© 2022 Ciena® Corporation

Step	Action

To create an IP interface

1 Create an IP interface.

```
interface create ip-interface <ip-interface> {ip <IP
address with mask>} [vlan <VLAN>] [mtu <NUMBER: 1500-
9216>] [mac <MAC address: XX:XX:XX:XX:XX:XX>]
[ip-forwarding <on|off>] [service-mac <benchmark | local-
mgmt | remote-mgmt>][role <evc-ping | device-mgmt>]
[priority <NUMBER: 0-7>]
```

where

ip-interface <ip-interface>	is a 15-character string to identify the interface. The following characters cannot be used: • ! • “ • % • , • / • ? • :
ip <IP address with mask>	is the IP address with mask.
vlan <VLAN>	is the VLAN ID for this interface (port service). The VLAN is optional. When this occurs the ip-interface will obtain its L2 mapping through the use of virtual-switch member configuration. ***Note:*** Ciena recommends to avoid adding more than one port in this VLAN ID.
[mtu <NUMBER: 1500-9216>]	is the interface MTU.
[mac <MAC address: XX:XX:XX:XX:XX:XX>]	is the MAC address.
ip-forwarding <on|off>	determines whether IP forwarding is on or off. The default value is off.

Copyright© 2022 Ciena® Corporation

where

service-mac <benchmark | local-mgmt | remote-mgmt>]	is the service name associated with the MAC address. Alternate way of specifying the MAC address.
[role <evc-ping | device-mgmt>]	configures double-tagged management or EVC Ping. The default is EVC Ping to ensure previous behavior is maintained. If device-mgmt is selected, the management protocols are rated limited to 2500 packets per second and include • ICMP • SSH • SNMP • Telnet • TWAMP If the interface role is set to evc-ping, only the ICMP and PTP protocols are allowed.
[priority <NUMBER:0-7>]	is the egress priority (or pcp) value on packets egressing this interface. The default value is 7.

To create a loopback interface

2 Create a loopback interface:

```
interface create loopback <loopback> {ip <IP address>}
```

where

loopback <loopback>	is the loopback interface name.
ip <IP address>	is the interface IP address.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-2
Deleting an IP or loopback interface

Delete an IP or loopback interface when it is no longer required.

When an interface is deleted, there are dynamic objects, internal to the SAOS software, which are deleted on their own after a dynamic timer expires. An example of a dynamic object is IP-Adjacency.

If you wish to create another interface immediately, use the port disable command before you delete the interface. After you delete the interface, use the port enable command. This ensures that the dynamic objects will be deleted immediately.

Note 1: IP and loopback interfaces are used mainly for control plane and MPLS tunnels. IP loopback address uses includes router identifier for routing protocols, LDP identifier and MPLS tunnel peer address.

Note 2: An IP or loopback interface cannot be deleted until the unnumbered IP interface(s) (IPUI) attached to it are deleted.

Step	Action
1	Delete an IP or loopback interface: `interface delete ip-interface <ip-interface>` where ip-interface <ip-interface> is the name of the interface to be deleted.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-3
Modifying an IP or loopback interface

Modify an IP or loopback interface to change the setting, for example, to increase the maximum frame size to allow bigger frames.

Note 1: IP and loopback interfaces are used mainly for control plane and MPLS tunnels. IP loopback address uses includes router identifier for routing protocols, LDP identifier and MPLS tunnel peer address.

Note 2: The IP address of an IP interface cannot be modified while unnumbered IP interface(s) (IPUI) are attached to it.

Note 3:

Step	Action

1 Modify an IP or loopback interface:

```
interface set ip-interface <Interface> {[ip <IpAddress>],
[ip-forwarding <on|off>], [mtu <NUMBER: 1500-9216>],
[priority <NUMBER: 0-7>]}
```

where

ip-interface <Interface>	is the IP or loopback interface to be modified.
ip <IpAddress>	is the IP address.
ip forwarding <on|off>	determines whether IP forwarding is on or off. The default value is off.
mtu <NUMBER: 1500-9216>	is the maximum transmission unit in bytes (maximum frame size). The default value is 1500.
priority <NUMBER: 0-7>	is the egress priority (pcp) value on packets egressing this interface. The default value is 7. The priority attribute does not apply to loopback interfaces.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-4
Enabling and disabling an IP interface

Enable or disable an IP interface.

Note: IP interfaces are used mainly for control plane and MPLS tunnels.

Step	Action

To enable an IP interface

1 Enable an IP interface:

```
interface enable ip-interface <Interface>
```

where

<Interface> is the IP interface to be enabled.

To disable an IP interface

2 Disable an IP interface:

```
interface disable ip-interface <Interface>
```

where

<Interface> is the IP interface to be disabled.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-5
Configuring IPv6 interfaces manually

Manually configure IPv6 interfaces.

Step	Action

To add the local interface IPv6 address and subnet mask

1 Add the local interface IPv6 address and subnet mask:

```
interface local add ip <ip>
```

where

ip <ip> is the IPv6 address of interface.

To remove the local interface IPv6 address and subnet mask

2 Remove the local interface IPv6 address and subnet mask:

```
interface local remove ip <ip>
```

where

ip <ip> is the IPv6 address of interface.

To add the remote interface IPv6 address and subnet mask

3 Add the remote interface IPv6 address and subnet mask:

```
interface remote add ip <ip>
```

where

ip <ip> is the IPv6 address of interface.

To remove the remote interface IPv6 address and subnet mask

4 Remove the remote interface IPv6 address and subnet mask:

```
interface remote remove ip <ip>
```

where

ip <ip> is the IPv6 address of interface.

Copyright© 2022 Ciena® Corporation

To add an IPv6 gateway address

5 Add an IPv6 gateway address:

```
interface add { [gateway <gateway>] [interface
<local|remote>] }
```

where

gateway <gateway>	is the IPv6 gateway to be added. It is best practice to use the link-local address of the router (starting with FE80::) as a gateway rather than the global address of the router, as this allows ICMPv6 type 137 redirect messages to work correctly, thus enhancing network reachability.
interface <local|remote>	is the management interface.

To remove an IPv6 gateway address

6 Remove an IPv6 gateway address:

```
interface remove { [gateway <gateway>] [interface
<local|remote>] }
```

where

gateway <gateway>	is the IPv6 gateway to be added.
interface <local|remote>	is the management interface.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-6
Displaying an IP interface

Display an IP interface to verify the configuration.

The Interface show command shows only operational addresses. The Interface Management Table includes local, remote and IP interfaces. IP interfaces are only IPv4 supported. Local and remote interfaces support both IPv4 and IPv6.

The interface show command for local and remote interfaces displays the source of configuration of the specified IP address, as shown in Table 7-8.

Table 7-8
Source of configuration of the specified IP address

Source	Description
Manual	Specifies configuration by user
SLAAC	Configured with Stateless Auto configuration through Router Advertisement messages
DHCP	Configured through DHCP Server
Local	Local Addresses including Link Local Addresses

Step	Action

To display IP interfaces

1 Display IP interfaces:

```
interface show
```

To display local IP interfaces

2 Display local IP interfaces:

```
interface local show
```

To display remote IP interfaces

3 Display remote IP interfaces:

```
interface remote show
```


Copyright© 2022 Ciena® Corporation

To display an IP interface

4 Display an IP interface:

```
interface show [ip-interface <Interface>]
```

where

<Interface> is the IP interface to be displayed.

—end—

Example

The following example shows sample output for the interface show ip-interface <interface-name> command.

```
interface show ip-interface <interface-name>

+------------------IP INTERFACE ENTRY-----------------+
| Parameter                 | Value                   |
+---------------------------+-------------------------+
| Index                     | 2                       |
| Name                      | fred                    |
| Admin State               | Enabled                 |
| Oper State                | Disabled                |
| RTD Index                 | 3                       |
| System IfIndex            | 0                       |
| Domain                    | n/a                     |
| MTU                       | 1500                    |
| Type                      | VS Member               |
| IPv4 Forwarding           | on                      |
| MAC                       | 00:02:5a:01:da:2a       |
| LDP State                 | Disabled                |
| Interface RSVP            | Disabled                |
| Tunnel Entities           | Absent                  |
| L2VPN Association         | Absent                  |
| VCCV Profile Association  | Absent                  |
| OSPF                      | Detached                |
| ISIS                      | Detached                |
| Static ARP                | Detached                |
| PTP                       | Disabled                |
| Role                      | Device Mgmt             |
+---------------------------+-------------------------+

+------------------------ ADMIN INTERFACE ADDRESSES -------------------------+
| Parameter           | Value                                                 |
+---------------------+-------------------------------------------------------+
| IPv4 Addr/Mask      | 20.20.20.111/21                                       |
| IPv6 Addr/Mask      | Not configured                                        |
+---------------------+-------------------------------------------------------+

+---------------------- OPERATIONAL INTERFACE ADDRESSES ----------------------+
| Parameter           | Value                                       | Source  |
+---------------------+---------------------------------------------+---------+
| No Entries found                                                            |
+---------------------+---------------------------------------------+---------+
```

The following example shows sample output for the interface remote show command.

```
interface remote show
```


Copyright© 2022 Ciena® Corporation

```
+-------- INTERFACE OPERATIONAL STATE --------+
| Parameter            | Value                |
+----------------------+----------------------+
| Name                 | remote               |
| Index                | 15                   |
| Admin State          | Enabled              |
| Oper State           | Enabled              |
| MAC Address          | 00:02:5a:01:b9:1f    |
| Management Domain    | VLAN 123             |
| Priority             | 7                    |
| MTU                  | 1500                 |
+----------------------+----------------------+


+------------------------- ADMIN INTERFACE ADDRESSES --------------------------+
| Parameter            | Value                                                 |
+----------------------+-------------------------------------------------------+
| IPv4 Addr/Mask       | Not configured                                        |
| IPv6 Addr/Mask       | Not configured                                        |
+----------------------+-------------------------------------------------------+

+---------------------- OPERATIONAL INTERFACE ADDRESSES -----------------------+
| Parameter            | Value                                       | Source   |
+----------------------+---------------------------------------------+----------+
| IPv6 Addr/Mask       | fe80::202:5aff:fe01:b91f/64                 | Local    |
+----------------------+---------------------------------------------+----------+
```

The following example shows sample output for the show ip-interface command.

```
interface show ip-interface

+------------------------------ IP INTERFACE TABLE ------------------------------+
| Name                 |  State   | Management          | MTU   | IP Address/Prefix  |
|                      |Adm |Oper | Domain              |       |                    |
+----------------------+----+-----+---------------------+-------+--------------------+
| joe                  |Ena |Dis  | VLAN 100            | 1500  | 19.34.34.1/21      |
| fred                 |Ena |Ena  | VS Abcde67890abcde  | 1500  | 5.5.5.1/24         |
+----------------------+----+-----+---------------------+-------+--------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-7
Creating an IPv6 interface

Create an IPv6 interface.

Step	Action
1	Create an IPv6 interface: `interface create ip-interface auto-ipv6 [vlan <VLAN>] [mtu <NUMBER: 1500-9216>] [mac <MAC address: XX:XX:XX:XX:XX:XX>] [ip-forwarding <on|off>] [service-mac <benchmark | local-mgmt | remote-mgmt>][role <evc-ping | device-mgmt>] [priority <NUMBER: 0-7>]` where vlan <VLAN> — is the VLAN ID for this interface (port service). The VLAN is optional. When this occurs the ip-interface obtains its L2 mapping through the virtual-switch member configuration. [mtu <NUMBER: 1500-9216>] — is the interface MTU. [mac <MAC address: XX:XX:XX:XX:XX:XX>] — is the MAC address. ip-forwarding <on|off> — determines whether IP forwarding is on or off. The default value is off.

Copyright© 2022 Ciena® Corporation

where

service-mac <benchmark | local-mgmt | remote-mgmt>]	is the service name associated with the MAC address. Alternate way of specifying the MAC address.
[role <evc-ping | device-mgmt>]	configures double-tagged management or EVC Ping. The default is EVC Ping to ensure previous behavior is maintained. If device-mgmt is selected, the management protocols are rated limited to 2500 packets per second and include • ICMP • SSH • SNMP • Telnet • TWAMP If the interface role is set to evc-ping, only the ICMP and PTP protocols are allowed.
[priority <NUMBER: 0-7>]	is the egress priority (pcp) value on packets egressing this interface. The default value is 7.

Copyright© 2022 Ciena® Corporation

Procedure 7-8
Configuring IPv6 stack settings

An ICMP redirect is a mechanism for routers to convey routing information to hosts. This is usually done by gateways attached to hosts. ICMP redirects are used by routers to specify better routing paths out of one network, based on the host choice. Through ICMP redirects, a host can find out which networks can be accessed from within the local network, and what routers are used for each network.

ICMP echoes request packets to the target host and wait for an ICMP response. It measures the time from transmission to reception and records packet loss.

Configure IPv6 stack settings by setting icmp-accept-redirects, accept-router-advertisement, and icmp-echo-ignore-broadcasts.

> ***Note:*** The default value for accept-router-advertisement is off, however, if you are upgrading from a pre-6.13 configuration, the config file will add the accept-router-advertisement to On to ensure that the previous behavior is preserved.

Step	Action

1 Configure IPv6 stack settings:

```
interface ipv6-stack set {[icmp-accept-redirects
<on|off>] [icmp-echo-ignore-broadcasts <on|off> [accept-
router-advertisement <on|off>] [stack-preference
<IPv4|IPv6>] [icmp-port-unreachable <on|off>]}
```

where

icmp-accept-redirects <on | off>	sets icmp-accept-redirects to on or off.
icmp-echo-ignore-broadcasts <on|off>	sets icmp-echo-ignore-broadcasts to on or off.

Copyright© 2022 Ciena® Corporation

where

accept-router-advertisement <on|off>	sets the IPv6 accept router advertisement. The default value is off.
stack-preference <IPv4|IPv6>	sets the stack preference to IPv4 or IPv6.
icmp-port-unreachable <on|off>	specifies whether the ICMP port is reachable.

—end—

Example

The following example shows configures IPv6 stack settings:

```
interface ipv6-stack set icmp-accept-redirects off, icmp-echo-ignore-
broadcasts off, accept-router-advertisement on stack-preference IPv6 icmp-
port unreachable on
```


Copyright© 2022 Ciena® Corporation

Procedure 7-9
Setting IPv6 stack settings to default values

Set IPv6 stack settings to default values.

Step	Action
1	Set IPv4 stack settings to default. `interface ipv6-stack unset {[icmp-accept-redirects] [icmp-echo-ignore-broadcasts] [accept-router-advertisement][stack-preference]}` where icmp-accept-redirects — resets icmp-accept-redirects to default value. icmp-echo-ignore-broadcasts — resets icmp-echo-ignore-broadcasts to default value. accept-router-advertisement — resets accept-router-advertisement to default value. stack-preference — resets the stack-preference to default value. **—end—**

Copyright© 2022 Ciena® Corporation

Procedure 7-10
Enabling and disabling an IPv6 stack

Enable or disable an IPv6 stack.

Step	Action

To enable an IPv6 stack

1 Enable an IPv6 stack:

```
interface ipv6-stack enable
```

To disable an IPv6 stack

2 Disable an IPv6 stack:

```
interface ipv6-stack disable
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-11
Displaying IPv6 stack settings

Display IPv6 stack settings.

Step	Action
1	Display IPv6 stack settings: `interface ipv6-stack show`

—end—

Example

The following example shows the output for the interface ipv6-stack show command:

```
interface ipv6-stack shows

+---------------------- IPV6 STACK STATE -----------------------+
| Parameter                     | Value                        |
+-------------------------------+------------------------------+
| IPv6 Stack                    | Enabled                      |
| Stack Preference              | IPv6                         |
| Accept Router Advertisement   | On                           |
| ICMP Accept Redirects         | On                           |
| ICMP Echo Ignore Broadcasts   | Off                          |
+-------------------------------+------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-12
Configuring IPv4 stack settings

Configure IPv4 stack ICMP- related settings to set ICMP-related settings for Common Critiera.

Step	Action
1	Configure IPv4 stack ICMP-related settings: `interface ipv4-stack set {[icmp-accept-redirects <on|off>] [icmp-echo-ignore-broadcasts <on|off>][icmp-port-unreachable <on|off}}` where icmp-accept-redirects <on|off> specifies whether the system accepts ICMP redirects, ICMP redirect is a mechanism for routers to convey routing information to hosts. ICMP redirect is typically unsecured and could be used for unintended or malicious purposes. icmp-echo-ignore-broadcasts <on|off> specifies whether the system responds to ICMP echoes sent to a broadcast address. Responding to broadcast ICMP echoes facilitates networking mapping and provides a vector for amplification attacks. icmp-port-unreachable <on|off> specifies whether the ICMP port is unreachable.

—end—

Example

The following example shows configures IPv4 stack settings:

```
interface ipv4-stack set icmp-accept-redirects on icmp-echo-ignore-broadcasts
off icmp port-unreachable on
```


Copyright© 2022 Ciena® Corporation

Procedure 7-13
Setting IPv4 stack settings to default values

Set IPv4 stack settings to default values.

Step	Action
1	Set IPv4 stack settings to default. `interface ipv4-stack unset {[icmp-accept-redirects] [icmp-echo-ignore-broadcasts]}`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-14
Displaying IPv4 stack settings

Display IPv4 stack settings.

Step	Action
1	Display IPv4 stack settings: `interface ipv4-stack show`

—end—

Example

The following example shows the output for the interface ipv4-stack show command:

```
interface ipv4-stack show

+---------------------- IPV4 STACK STATE -----------------------+
| Parameter                    | Value                          |
+------------------------------+--------------------------------+
| ICMP Accept Redirects        | On                             |
| ICMP Echo Ignore Broadcasts  | Off                            |
+------------------------------+--------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-15
Configuring interface TCP stack settings

Configure interface TCP stack settings.

Step	Action
1	Configure interface TCP stack settings: `interface tcp-stack set {[tcp-timestamps <on|off>]}` where tcp-timestamps <on|off> sets tcp-timestamps on or off.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-16
Setting interface TCP stack settings to default values

Set interface TCP stack settings to default values.

Step	Action
1	Set interface TCP stack settings to default. `interface tcp-stack unset {[tcp-timestamps]}`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-17
Displaying TCP stack settings

Display TCP stack settings.

Step	Action
1	Display TCP stack settings: `interface tcp-stack show`

—end—

Example

The following shows output for the interface tcp-stack show command:

```
interface tcp-stack show

+----------------------- TCP STACK STATE ------------------------+
| Parameter                     | Value                          |
+-------------------------------+--------------------------------+
| TCP Timestamps                | On                             |
+-------------------------------+--------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-18
Configuring in-band management bridging

In-band management bridging is disabled by default to ensure there is no impact to current remote or local interfaces in use. In-band management bridging must only be configured on the head-end device.

You can configure the VLAN associated with the remote interface. Since the remote interface only needs to be configured, the in-band and out-of-band VLAN have the same VID tag value.

Once the management port interface is set to the remote interface, it is no longer possible to configure the local interface. This ensures that the local interface's configuration does not interfere with the bridge. The admin state of the local interface must be enabled to ensure that the management port is enabled. Since the management port is not available under the port component, you can enable and disable the management port by the local interface.

Step	Action

To configure in-band management bridging

1 Configure in-band management bridging:

```
interface set mgmt-port interface <local | remote>
```

where

mgmt-port interface <local | remote>	configures in-band management bridging on the remote or local interface. To enable bridging, enter remote. To disable bridging, enter local.

2 Enable the administrative state of the local interface to ensure that the management port is enabled:

```
interface local enable
```

To disable in-band management bridging

3 Disable in-band management bridging:

```
interface set mgmt-port-interface local
```

Example

The following example enables in-band management bridging:

```
> interface set mgmt-port-interface remote
>interface local enable:
```


Copyright© 2022 Ciena® Corporation

The following example disables the in-band management function and sets the mgmt-port-interface back to its default value (local):

```
> interface unset mgmt-port-interface
```


Copyright© 2022 Ciena® Corporation

Procedure 7-19
Modifying the VLAN for in-band management bridging

The VID for VLAN management is set to a default of 127 on the subtended edge device to ensure management traffic continuity. This value can be modified. When it is changed, all subtended edge devices must still be able to communicate with the head-end device during the transition period.

The default VID tag value is 127, but its value can be changed when in-band management bridging is enabled.

When in-band management bridging is enabled, a reserved subtended management interface is automatically created on VLAN 127. This reserved interface is not visible.

The subtended remote interface allows the migration to new VLANs without losing connectivity to the subtended nodes.

The following procedure describes how to migrate the management VLAN to ensure management traffic continuity.

Step	Action
1	Configure the remote interface VLAN to the default VLAN 127 on the subtended edge devices: `interface remote set vlan 127`
2	Create the VLAN: `vlan create vlan <newVlan>` where vlan <newVlan> is the new VLAN.
3	Add the new VLAN and its associated ports on the subtended edge device: `vlan add vlan <newVlan> port <portNum>>` where port <portNum> is the new VLAN and its associated ports being added on the subtended device.
4	Create the VLAN: `vlan create vlan <newVlan>`

Copyright© 2022 Ciena® Corporation

5 Add the new VLAN and its associated ports on the head-end device:

```
vlan add vlan <newVlan> port <portNum>
```

where

port <portNum> is the new VLAN and its associated ports being added on the head-end device.

6 Configure the remote interface VLAN to the VLAN on the head-end device.

```
interface remote set vlan <newVlan>
```

7 Configure the remote interface VLAN to the VLAN on the subtended edge devices.

```
interface remote set vlan <newVlan>
```

Example

The following example migrates the management VLAN between the VLAN on the subtended device and the VLAN on the head-end device. I

On the subtended node:

```
interface remote set vlan 127
vlan create vlan 300
vlan add vlan port 5
```

On the head-end node:

```
vlan create vlan 300
vlan add port 5
interface remote set vlan 300
```

On the subtended node:

```
interface remote set vlan 300
```


Copyright© 2022 Ciena® Corporation

Procedure 7-20
Adding an IP route

Add an IP route.

Step	Action

1 Add an IP route:

```
ip route add {destination <IpAddressWithMask>} {gateway
<IpAddress>} [metric <#>] [domain-name <routing-domain-
name>]
```

where

destination <IpAddressWithMask>	is the destination route IP address in CIDR notation.
gateway <IpAddress>	is the gateway IP address for the associated IP or loopback interface.
metric <#>	is the interface route cost metric. The default value is 0.
[domain-name <routing-domain-name>]	is the routing domain.

—end—

Example

The following example adds an IP route with a destination IP address of 5.5.5.0/24, a gateway address of 6.6.6.6, and an interface route cost metric of 10.

```
ip route add destination 5.5.5.0/24 gateway 6.6.6.6 metric 10
```


Copyright© 2022 Ciena® Corporation

Procedure 7-21
Removing an IP route

Remove an IP route when the IP route is no longer needed.

Step	Action

1 Remove an IP route:

```
ip route remove [destination <IpAddressWithMask>],
[gateway <IpAddress>], |[metric <#>] [domain-name
<routing-domain-name>]
```

where

destination <IpAddressWithMask>	is the destination route IP address in CIDR notation.
gateway <IpAddress>	is the gateway IP address for the associated IP or loopback interface.
metric <#>	is the interface route cost metric. The default value is 0.
[domain-name <routing-domain-name>]	is the routing domain.

—end—

Example

The following example removes a static IP route with a destination IP address of 5.5.5.0/24, a gateway address of 6.6.6.6, and an interface route cost metric of 10.

```
ip route remove destination 5.5.5.0/24 gateway 6.6.6.6 metric 10
```


Copyright© 2022 Ciena® Corporation

Procedure 7-22
Displaying the routing table

Display the routing table to verify configuration.

Step	Action

1 Display the routing table:

```
ip route show [domain-name <routing-domain-name>]
```

where

[domain-name <routing-domain-name>]	is the routing domain.

—end—

Example

The following example shows sample output for the ip route show command.

```
> ip route show
+------------------------------ ROUTING TABLE -------------------------------+
|Act| Destination     | Gateway         | Genmask         |Metric    |Intf|Prot|
+---+-----------------+-----------------+-----------------+----------+----+----+
|   | 10.0.0.0        | 1.1.1.1         | 255.0.0.0       | 0        | 5  | Inv|
+---+-----------------+-----------------+-----------------+----------+----+----+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-23
Displaying FIB entries

After creating a static IP route, the forwarding information is stored in the FIB. The summary view is displayed by default.

You can display:

- the FIB entry for the default route
- a summary of FIB entries
- details for each FIB entry

—end—

Step	Action

To display the FIB entry for the default route

1 Display the FIB entry for the default route:

```
ip fib show [destination <Ip Address with mask>] [default]
```

where

destination <Ip Address with mask>	is the destination route IP address/mask.
[default]	displays the default route, if any configured.

To display a summary of FIB entries

2 Display a summary of FIB entries:

```
ip fib show [destination <Ip Address with mask>][summary]
```

where

destination <Ip Address with mask>	is the destination route IP address/mask.
[summary]	displays summary.

Copyright© 2022 Ciena® Corporation

To display details for each FIB entry

3 Display details for each FIB entry:

```
ip fib show [destination <Ip Address with Mask>][details]
[summary]
```

where

destination <Ip Address with Mask>	is the destination route IP address.
[details]	displays details.

—end—

Example

The following example shows sample output for the ip fib show command. The summary view is displayed by default.

```
> ip fib show

+------------------+----------------+----------+---+----+------+-----------+
| Destination/     |   NexthopIp    |oifIdx/   |Act|Path|Entry |Path Cost  |
|  NetMaskLen      |                |TnlGrpId  |ion|Type|Id    |(AdmDist.) |
+------------------+----------------+----------+---+----+------+-----------+
|0.0.0.0/ 0        |-               |-         |loc|ADJ |0     |0          |
|1.1.1.1/32        |172.16.26.1     |11        |fwd|I1I |0     |115        |
|2.2.2.2/32        |172.16.26.1     |11        |fwd|I1I |0     |115        |
|3.3.3.3/32        |172.16.26.1     |11        |fwd|I1I |0     |115        |
|4.4.4.4/32        |172.16.26.1     |11        |fwd|I1I |0     |115        |
|5.5.5.5/32        |-               |-         |loc|IF  |0     |0          |
|172.16.26.0/24    |-               |-         |loc|IF  |0     |0          |
|172.16.26.0/32    |-               |-         |loc|IF  |0     |0          |
|172.16.26.1/32    |172.16.26.1     |11        |loc|ADJ |0     |0          |
|172.16.26.2/32    |-               |-         |loc|IF  |0     |0          |
|172.16.26.255/32  |-               |-         |loc|IF  |0     |0          |
+------------------+----------------+----------+---+----+------+-----------+
| oif: Outgoing Interface                                                  |
| entryId: Internal Id from Route Module (=0 local)                        |
| Action: fwd: Forward, loc: Local, rej: Reject, bck: BlackHole            |
| C: Conn, LC: LocalConn, DC: DirectlyConn, Sta: Static                    |
| PathType: I1I: Isis L1 Int, I2I: Isis L2 Int                             |
|  I1E: Isis L1 Ext, I2E: Isis L2 Ext, O: Ospf IntraArea                   |
|  OIA: Ospf InterArea, OE1: Ospf Type1 Ext, OE2: Ospf Type2 Ext           |
|  IC: Icmp, Oth: Other, IF: Local Interface, ADJ: Adjacency               |
|  BGP: BGP, LFA: Loop Free Alternate,                                     |
|  RLFA: Remote Loop Free Alternate, unk: Unknown                          |
+--------------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-24
Enabling Layer 3 switching

FIB Layer 3 switching is enabled by default. In order for static IP routing to support layer 3 traffic, such as for RFC 2544 and MPLS, FIB Layer 3 switching must be enabled.

Step	Action
1	Enable Layer 3 switching: `ip fib l3-switching enable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-25
Disabling Layer 3 switching

Disable Layer 3 switching when MPLS and benchmarking are no longer required.

Step	Action
1	Disable Layer 3 switching: `ip fib l3-switching disable`

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-26
Displaying the status of Layer 3 switching

Display the status of Layer 3 switching to learn whether Layer 3 switching is enabled or disabled.

Step	Action
1	Display the status of Layer 3 switching: `ip fib l3-switching show`

—end—

Example

The following example shows sample output of the ip fib l3-switching show command.

```
> ip fib l3-switching show

L3-Switching Enabled
```


Copyright© 2022 Ciena® Corporation

Procedure 7-27
Clearing all FIB or AIB entries

Clear all FIB or AIB entries as part of a clean up operation, or when troubleshooting.

Step	Action

To clear all FIB entries

1 Clear all FIB entries:

```
ip fib flush
```

To clear all AIB entries

2 Clear all AIB entries

```
ip aib flush
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-28
Enabling logging of FIB or AIB events

Enable logging of FIB or AIB events for troubleshooting.

Step	Action

To enable logging of FIB events

1 Enable logging of FIB events:

```
ip fib debug events on
```

To enable logging of AIB events

2 Enable logging of AIB events:

```
ip aib debug events on
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-29
Displaying FIB information

Display FIB information for troubleshooting purposes. You can display the following information for the FIB:

- log
- interfaces
- interface IP addresses
- static resolutions

Step	Action

To display the FIB log

1 Display the FIB log:

```
ip fib log show
```

To display the FIB interfaces

2 Display the FIB interfaces:

```
ip fib interfaces show [summary] [details]
```

where

summary	displays a summary of FIB information for interfaces.
details	displays detailed FIB information for interfaces.

To display the FIB interface IP addresses

3 Display the FIB interface IP addresses:

```
ip fib interfaceIpAddresses show [summary] | [details]
```

where

summary	displays a summary of FIB information for interface IP addresses.
details	displays detailed FIB information for interface IP addresses.

To display the FIB static resolutions

4 Display the FIB static resolutions:

```
ip fib staticResolutions show [summary] | [details]
```

where

summary	displays a summary of FIB information for static resolutions.
details	displays detailed FIB information for static resolutions.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-30
Adding a static ARP entry

ARP maps an IP address to a physical MAC address. Entries can be learned dynamically, such as when a device sends an ARP request or ping, but for the entries to be permanent, as in the case of using a device as a static reflector for RFC 2544, you can add a static entry.

Step	Action
1	Add a static ARP entry: `arp static add {destination <IpAddress>} {mac <MacAddress>} {ip-interface <Interface>}` where destination <IpAddress> — is the destination host IP address. mac <MacAddress> — is the destination MAC address. ip-interface <Interface> — is the IP interface routed to the destination.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-31
Removing static ARP entries

Remove static ARP entries when they are no longer needed. You can remove

- one static ARP entry
- all static ARP entries

Step	Action

To remove a static ARP entry

1 Remove a static ARP entry.

```
arp static remove {destination <IpAddress>} {ip-interface
<Interface>}
```

where

destination <IpAddress>	is the destination host IP address.
ip-interface <Interface>	is the IP interface routed to the destination.

To remove all static ARP entries

2 Remove all static ARP entries.

```
arp static remove-all
```

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-32
Configuring EVC ping for use case A

Configure EVC ping for a virtual switch with EPL to IP interface with virtual switch member configuration.

Step	Action

Configure NTE-1

1 Create the VLAN:

```
vlan create vlan <vlan>
```

where

vlan <vlan> is the VLAN ID.

2 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

where

port <port> is the port to add to the VLAN.

3 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

where

vc <vc> is the virtual circuit name.

4 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

where

vs <vs> is the virtual switch.

vc <vc> is the virtual circuit.

5 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <PortList>}
{vlan <VLAN list>} {ip-interface <interface-name>}
{encap-cos-policy <fixed |port-inherit | vs-inherit>}
{encap-fixed-dot1dpri <NUMBER: 0-7>} [statistics <on |
off>] [translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-
7>]
```

where

vs <vs> is the virtual switch name.

port <PortList> is the subscriber port list.

vlan <VLAN> is the subscriber VLAN id.

Copyright© 2022 Ciena® Corporation

where

ip-interface <interface-name>	is the name of the IP interface.
encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.
pcp <NUMBER: 0-7>	is the pcp.

6 Create the IP interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-7>]
```

where

ip-interface <ip-interface>	is the interface name.
ip <ip address> / <subnet-mask>	is the IP address or subnet-mask.
vlan <vlan>	is the VLAN ID.
priority <NUMBER: 0-7>	The egress priority (pcp) value on packets egressing this interface. The default is 7.

Configure NTE-2

7 Create the VLAN:

```
vlan create vlan <vlan>
```

8 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```


Copyright© 2022 Ciena® Corporation

9 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

10 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

11 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER:0-7>]
```

12 Create the IP interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

13 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```

The ip-interface is operational.

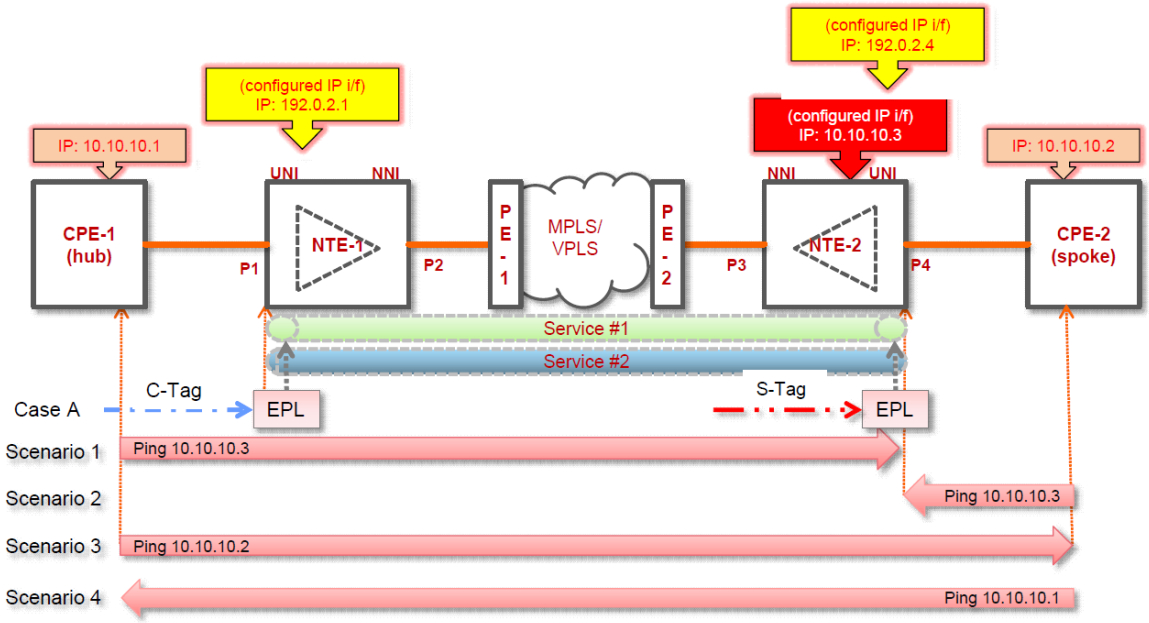
—end—

Example

Figure 7-10 and Figure 7-11 show a sample virtual switch with EPL to IP interface with virtual switch member configuration in an IPv4 and IPv6 network.

Copyright© 2022 Ciena® Corporation

Figure 7-10
Use case A IPv4 configuration example



To configure the example shown in Figure 7-11:

Configure NTE-1.

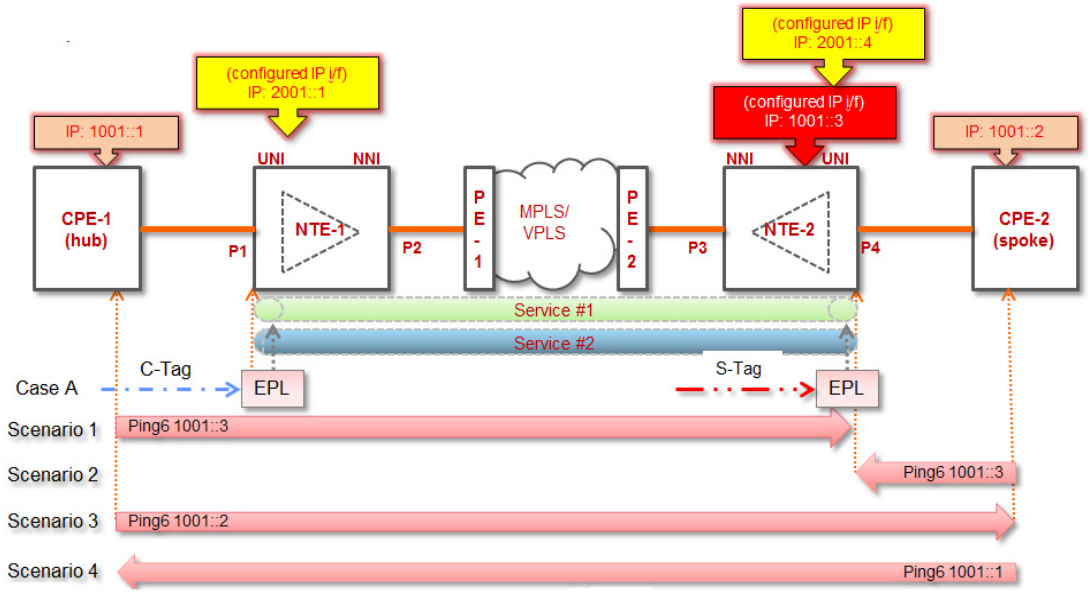
```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1
interface create ip-interface ipvs8 ip 192.0.2.1/24 vlan 8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4

interface create ip-interface ipvs8 ip 20.20.20.4/24 vlan 8
interface create ip-interface ip24 ip 10.10.10.3/24
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan 24
```


Copyright© 2022 Ciena® Corporation

Figure 7-11
Use case A IPv6 configuration example



To configure the example shown in Figure 7-11:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1
interface create ip-interface ipvs8 ip 2001::1/64 vlan 8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4

interface create ip-interface ipvs8 ip 2001::4/64 vlan 8
interface create ip-interface ip24 ip 1001::3/64
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan
24
```


Copyright© 2022 Ciena® Corporation

Procedure 7-33
Configuring EVC ping for use case B

Configure EVC ping for a virtual switch with EPL and untagged data virtual switch to IP interface with VLAN configuration.

Step	Action

Configure NTE-1

1 Create the VLAN:

```
vlan create vlan <vlan>
```

where

vlan <vlan> is the VLAN ID.

2 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

where

port <port> is the port to add to the VLAN.

3 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>>
```

where

vc <vc> is the virtual circuit name.

4 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

5 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]]
```

where

vs <vs>	is the virtual switch name.
port <PortList>	is the subscriber port list.
vlan <VLAN>	is the subscriber VLAN id.
ip-interface <interface-name>	is the name of the IP interface.

Copyright© 2022 Ciena® Corporation

where

encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.
pcp <NUMBER: 0-7>	is the pcp.

6 Set the virtual switch for untagged data frames:

```
port set port <port> untagged-data-vs <vs>
```

where

port <port>	is the port to set.
untagged-data-vs <vs>	sets the virtual switch for untagged data frames.

Configure NTE-2

7 Create the VLAN:

```
vlan create vlan <vlan>
```

8 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

9 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

10 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```


Copyright© 2022 Ciena® Corporation

11 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>]
```

12 Create the IP interface for the virtual switch and EPL:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

where

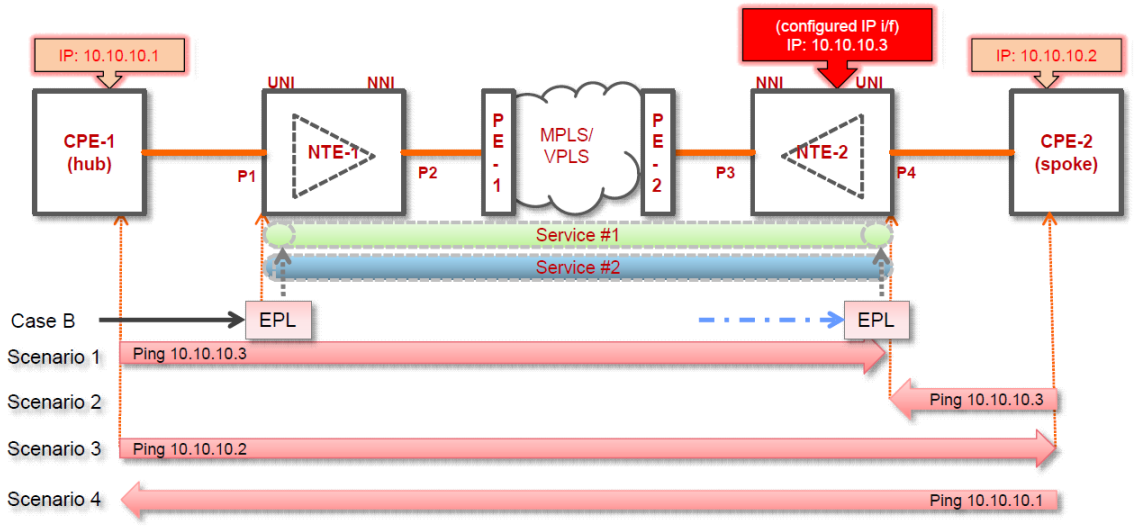
ip-interface <ip-interface>	is the interface name.
ip <ip address> / <subnet-mask>	is the IP address or subnet-mask.
vlan <vlan>	is the VLAN ID.
priority <NUMBER: 0-7>	The egress priority (pcp) value on packets egressing this interface. The default is 7.

—end—

Example

Figure 7-12 and Figure 7-13 show a sample virtual switch with EPL and untagged data virtual switch to IP interface with VLAN configuration in an IPv4 and IPv6 network.

Figure 7-12
Use case B IPv4 configuration example



To configure the example shown in Figure 7-12:

Copyright© 2022 Ciena® Corporation

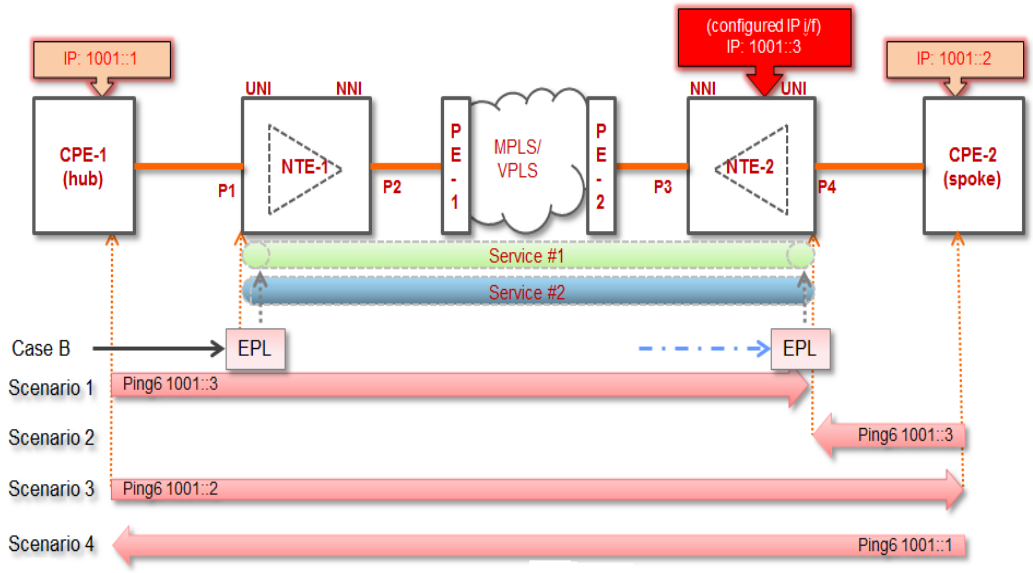
Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1

port set port 1 untagged-data-vs vs8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4

interface create ip-interface ipvs8 ip 10.10.10.3/24 vlan 8
```

Figure 7-13
Use case B IPv6 configuration example



To configure the example shown in Figure 7-12:

Configure NTE-1.

Copyright© 2022 Ciena® Corporation

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1

port set port 1 untagged-data-vs vs8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4

interface create ip-interface ipvs8 ip 1001::3/64 vlan 8
```


Copyright© 2022 Ciena® Corporation

Procedure 7-34
Configuring EVC ping for use case C

Configure EVC ping for a virtual switch with EVPL to IP interface with VLAN configuration.

Step	Action

Configure NTE-1

1 Create the VLAN:

```
vlan create vlan <vlan>
```

where

vlan <vlan> is the VLAN ID.

2 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

where

port <port> is the port to add to the VLAN.

3 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

where

vc <vc> is the virtual circuit name.

4 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>>
```

where

vc <vc> is the virtual circuit name.

5 Add subscriber members to the virtual switch (EVPL):

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]]
```

where

vs <vs> is the virtual switch name.

port <PortList> is the subscriber port list.

vlan <VLAN> is the subscriber VLAN id.

Copyright© 2022 Ciena® Corporation

where

ip-interface <interface-name>	is the name of the IP interface.
encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.
pcp <NUMBER: 0-7>	is the PCP number.

Configure NTE-2

6 Create the VLAN:

```
vlan create vlan <vlan>
```

7 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

8 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

9 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

10 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```


Copyright© 2022 Ciena® Corporation

11 Create the IP interface for the virtual switch and EPL:

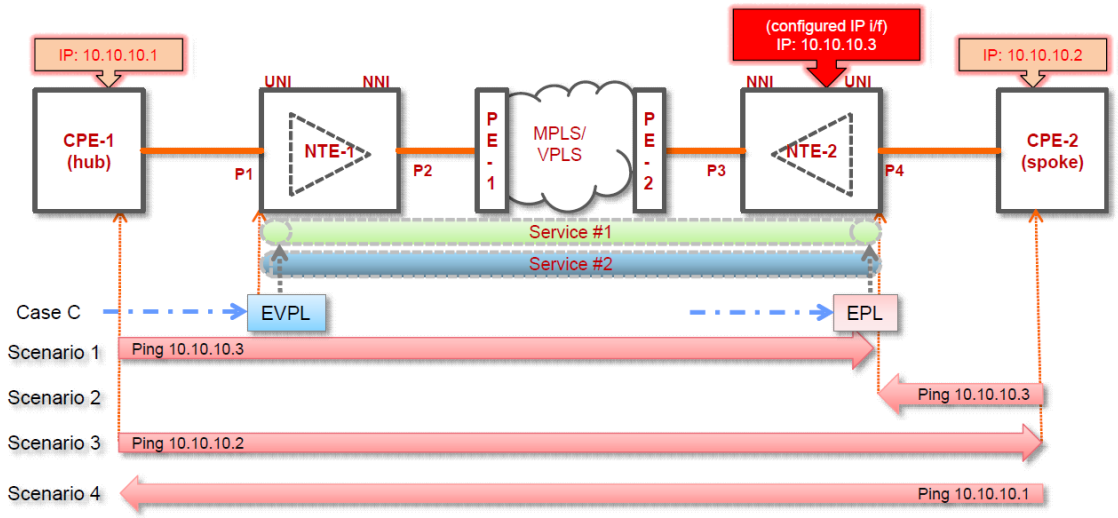
```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

—end—

Example

Figure 7-14 and Figure 7-15 show a sample virtual switch with EVPL to IP interface with VLAN configuration in an IPv4 and IPv6 network.

Figure 7-14
Use case C IPv4 configuration example



To configure the example shown in Figure 7-14:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1 vlan 24 translate-tag
0
port set port 1 vs-l2-transform i-stamp:push,e-match-pop:stamp
```

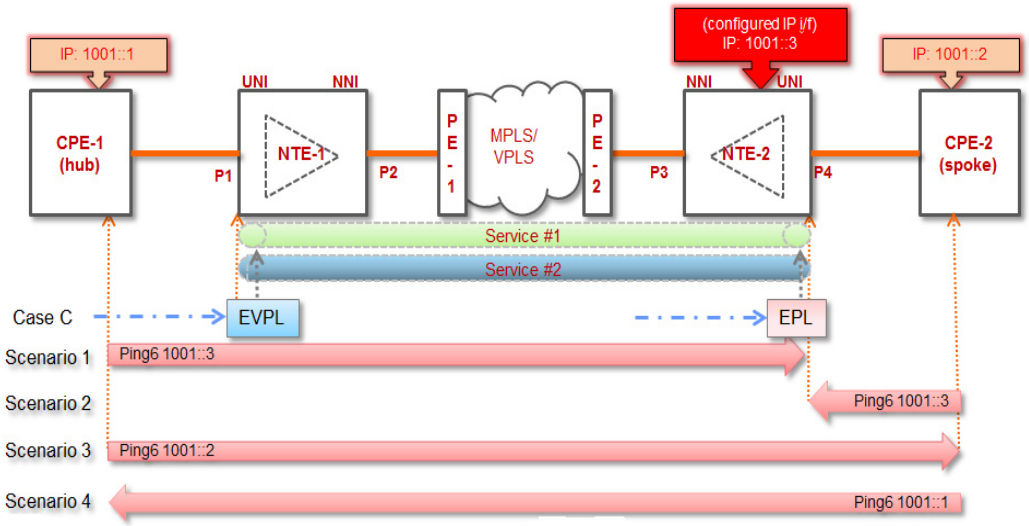
Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4
```


Copyright© 2022 Ciena® Corporation

```
interface create ip-interface ipvs8 ip 10.10.10.3/24 vlan 8
```

Figure 7-15
Use case C IPv6 configuration example



To configure the example shown in Figure 7-15:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1 vlan 24 translate-tag
0
set port 1 vs-l2-transform i-stamp:push,e-match-pop:stamp
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4

interface create ip-interface ipvs8 ip 1001::3/64 vlan 8
```


Copyright© 2022 Ciena® Corporation

Procedure 7-35
Configuring EVC ping for use case D

Configure EVC ping for virtual switch with EPL and untagged data virtual switch to IP interface with virtual switch member configuration.

Step	Action

Configure NTE-1

1 Create the VLAN:

```
vlan create vlan <vlan>
```

where

vlan <vlan> is the VLAN ID.

2 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

where

port <port> is the port to add to the VLAN.

3 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

where

vc <vc> is the virtual circuit name.

4 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

where

vc <vc> is the virtual circuit name.

5 Set the virtual switch for untagged data frames and set push/pop for the specified VLAN ID for untagged data frames:

```
port set port <port> untagged-data-vs <vs> untagged-data-
vid <vlan>
```

where

port <port> is the port to set.

untagged-data-vs <vs> sets the virtual switch for untagged data frames.

vid <vlan> sets the VID.

Copyright© 2022 Ciena® Corporation

6 Create the ip-interface for the virtual switch:

```
interface ip create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan>]
```

where

ip-interface <ip-interface>	is the interface name.
ip <ip address> / <subnet-mask>	is the IP address or subnet-mask.
vlan <vlan>	is the VLAN ID.

Configure NTE-2

7 Create the VLAN:

```
vlan create vlan <vlan>
```

8 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

9 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

10 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

11 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>]
```

where

vs <vs>	is the virtual switch name.
port <PortList>	is the subscriber port list.
vlan <VLAN>	is the subscriber VLAN id.
ip-interface <interface-name>	is the name of the IP interface.

Copyright© 2022 Ciena® Corporation

where

encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.

12 Create the IP interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

13 Create the IP interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

14 Create the IP interface:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> [priority <NUMBER: 0-7>]
```

15 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```

where

pcp <NUMBER: 0-7>	is the PCP number.

The ip-interface is operational.

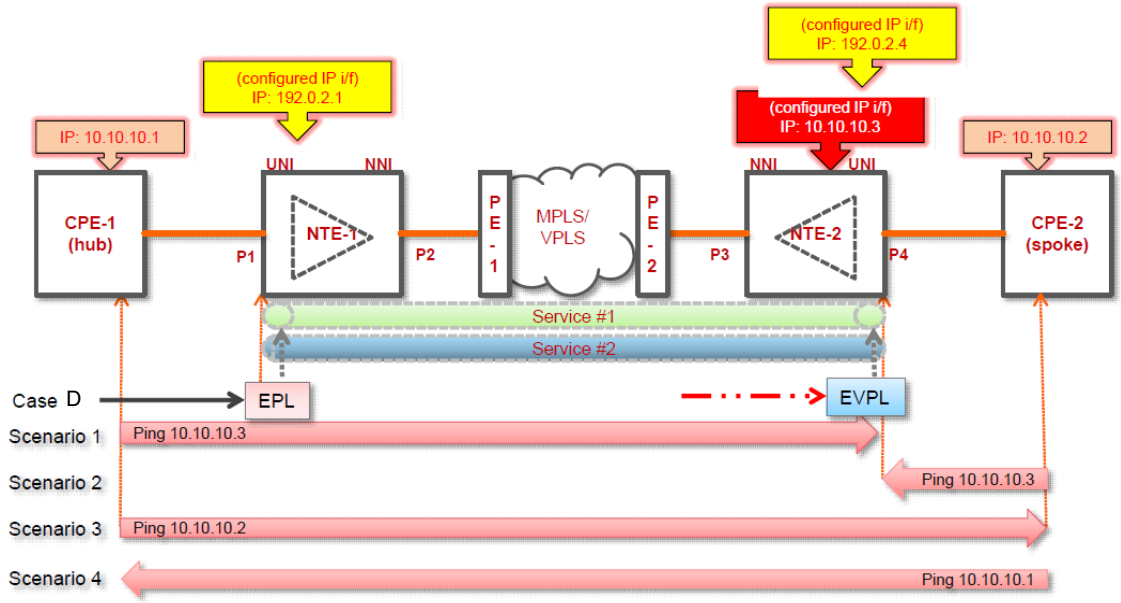
—end—

Copyright© 2022 Ciena® Corporation

Example

Figure 7-16 shows a sample virtual switch with EPL and untagged data virtual switch to IP interface with virtual switch member configuration in an IPv4 and IPv6 network.

Figure 7-16
Use case D IPv4 configuration example



To configure the example shown in Figure 7-16:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1

port set port 1 untagged-data-vs vs8 untagged-data-vid 24

interface create ip-interface ipvs8 ip 192.0.2.1/24 vlan 8
```

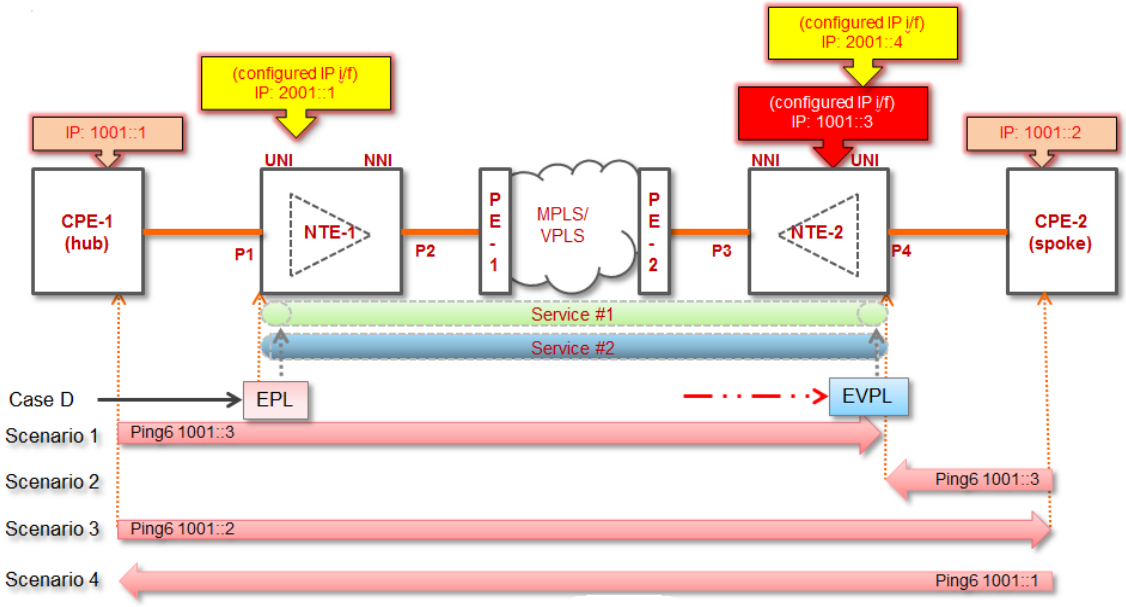
Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4 vlan 24
```


Copyright© 2022 Ciena® Corporation

```
interface create ip-interface ipvs8 ip 20.20.20.4/24 vlan 8
interface create ip-interface ip24 ip 10.10.10.3/24
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan 24
```

Figure 7-17
Use case D IPv6 configuration example



To configure the example shown in Figure 7-17:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1

port set port 1 untagged-data-vs vs8 untagged-data-vid 24

interface create ip-interface ipvs8 ip 2001::1/64 vlan 8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4 vlan 24
```


Copyright© 2022 Ciena® Corporation

```
interface create ip-interface ipvs8 ip 2001::4/64 vlan 8
interface create ip-interface ip24 ip 1001::3/64
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan 24
```


Copyright© 2022 Ciena® Corporation

Procedure 7-36
Configuring EVC ping for use case E

Configure EVC ping for virtual switch with EVPL to IP interface with virtual switch member configuration.

Step	Action

Configure NTE-1

1 Create the VLAN:

```
vlan create vlan <vlan>
```

where

vlan <vlan> is the VLAN ID.

2 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

where

port <port> is the port to add to the VLAN.

3 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

where

vc <vc> is the virtual circuit name.

vlan <vlan> is the VLAN name.

4 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

where

vs <vs> is the virtual switch name.

vc <vc> is the virtual circuit name>

5 Add virtual switch member attributes:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```


Copyright© 2022 Ciena® Corporation

6 Create the ip-interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

where

ip-interface <ip-interface>	is the interface name.
ip <ip address> / <subnet-mask>	is the IP address or subnet-mask.
vlan <vlan>	is the VLAN ID.
priority <NUMBER: 0-7>	The egress priority (pcp) value on packets egressing this interface. The default is 7.

Configure NTE-2

7 Create the VLAN:

```
vlan create vlan <vlan>
```

8 Add a port to the VLAN:

```
vlan add vlan <vlan> port <port>
```

9 Create an Ethernet virtual circuit:

```
virtual-circuit ethernet create vc <vc> vlan <vlan>
```

10 Create an Ethernet virtual switch:

```
virtual-switch ethernet create vs <vs> vc <vc>
```

11 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```

where

vs <vs>	is the virtual switch name.
port <PortList>	is the subscriber port list.
vlan <VLAN>	is the subscriber VLAN id.
ip-interface <interface-name>	is the name of the IP interface.

Copyright© 2022 Ciena® Corporation

where

encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.

12 Create the IP interface for the virtual switch:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> vlan <vlan> [priority <NUMBER: 0-
7>]
```

13 Create the IP interface:

```
interface create ip-interface <ip-interface> ip <ip
address>/<subnet-mask> [priority <NUMBER: 0-7>]
```

14 Add subscriber members to the virtual switch:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>} {encap-cos-
policy <fixed | port-inherit | vs-inherit>} {encap-fixed-
dot1dpri <NUMBER: 0-7>} [statistics <on | off>]
[translate-tag <NUMBER: 0-4094>] [pcp <NUMBER: 0-7>]
```

where

vs <vs>	is the virtual switch name.
port <PortList>	is the subscriber port list.
vlan <VLAN>	is the subscriber VLAN id.
ip-interface <interface-name>	is the name of the IP interface.

Copyright© 2022 Ciena® Corporation

where

encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
encap-fixed-dot1dpri <NUMBER: 0-7>	is the encapsulation fixed dot1dpri.
statistics <on | off>	is the statistics control for the virtual switch member.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp value or range.

The ip-interface is operational.

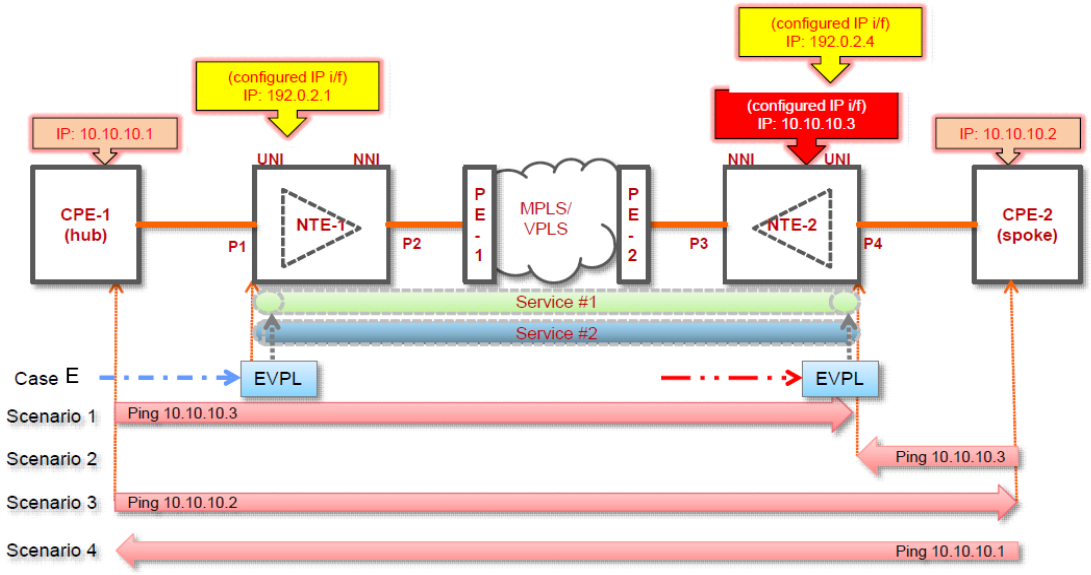
—end—

Example

Figure 7-18 and show a sample virtual switch with EVPL to IP interface with virtual switch member configuration in an IPv4 and IPv6 network.

Copyright© 2022 Ciena® Corporation

Figure 7-18
Use case E IPv4 configuration example



To configure the example shown in Figure 7-18:

Configure NTE-1.

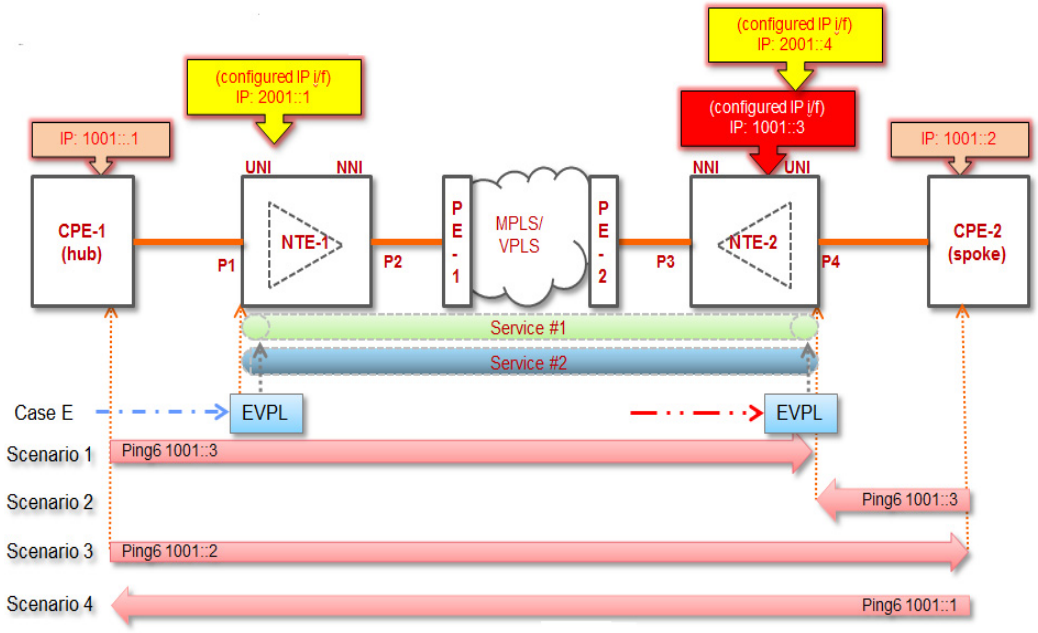
```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1 vlan 24

interface create ip-interface ipvs8 ip 192.0.2.1/24 vlan 8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4 vlan 24

interface create ip-interface ipvs8 ip 20.20.20.4/24 vlan 8
interface create ip-interface ip24 ip 10.10.10.3/24
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan 24
```


Copyright© 2022 Ciena® Corporation

Figure 7-19
Use case E IPv6 configuration example



To configure the example shown in Figure 7-19:

Configure NTE-1.

```
vlan create vlan 8
vlan add vlan 8 port 2
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 1 vlan 24

interface create ip-interface ipvs8 ip 2001::1/64 vlan 8
```

Configure NTE-2.

```
vlan create vlan 8
vlan add vlan 8 port 3
virtual-circuit ethernet create vc vc8 vlan 8
virtual-switch ethernet create vs vs8 vc vc8
virtual-switch ethernet add vs vs8 port 4 vlan 24

interface create ip-interface ipvs8 ip 2001::4/64 vlan 8
interface create ip-interface ip24 ip 1001::3/64
virtual-switch ethernet add vs vs8 ip-interface ip24 vlan 24
```


Copyright© 2022 Ciena® Corporation

Procedure 7-37
Configuring double-tagged management

Configure double-tagged management.

Step	Action
1	Create the VLAN: `vlan create vlan <vlan>` where vlan <vlan> is the VLAN name.
2	Add a port to the VLAN: `vlan add vlan <vlan> port <port>` where vlan <vlan> is the VLAN name. port <port> is the port number.
3	Create an Ethernet virtual circuit: `virtual-circuit ethernet create vc <vc> vlan <vlan>` where vc <vc> is the virtual circuit name. vlan <vlan> is the VLAN name.
4	Create an Ethernet virtual switch: `virtual-switch ethernet create vs <vs> vc <vc>` where vs <vs> is the virtual switch name. vc <vc> is the virtual circuit name.
5	Create the ip-interface for the virtual switch: `interface create ip-interface [interface name <ip-address>] ip-forwarding <on|off> role device-mgmt [priority <NUMBER: 0-7>]` where ip-interface name <ip-address> is the IP interface name and IP address of the IP interface you are creating. ip-forwarding <on|off> turns ip forwarding on or off. [priority <NUMBER: 0-7>] is the egress priority (pcp) value on packets egressing this interface. The default value is 7.

Copyright© 2022 Ciena® Corporation

6 Add the virtual switch member attributes:

```
virtual-switch ethernet add vs <vs> {port <port>} {vlan
<VLAN list>} {ip-interface <interface-name>}{encap-cos-
policy <fixed | port-inherit | vs-inherit>}{encap-
fixeddot1dpri [translate-tag <NUMBER: 0-4094>[pcp
<NUMBER: 0-7>]
```

where

vs <vs>	is the virtual switch name.
port <port>	is the port number you are adding the attributes to.
vlan <VLAN list>	is the subscriber VLAN ID.
ip-interface <interface-name>	is the IP interface name.
encap-cos-policy <fixed | port-inherit | vs-inherit>	is the encapsulation CoS policy. • fixed specifies that the encapsulation PCP value is taken from the encap-fixed-dot1dpri parameter of the virtual switch member. • port-inherit specifies that the encapsulation PCP value is based on the Resolved CoS (R-CoS) policy of the port. • vs-inherit specifies that the encapsulation PCP value is defined by the virtual switch encapsulation CoS policy configuration and all UNI port members inherit this setting. This setting is the default.
translate-tag <NUMBER: 0-4094>	is the subscriber VLAN translate stamp.
[pcp <NUMBER:0-7>]	is the egress C-VID priority value on packets egressing the vs-member IP interface. Default value is 0.

—end—

Example

The following example configures double-tagged management.

```
vlan create vlan 2112
vlan add vlan 2112 port 9
vlan remove vlan 127 port 9
vlan add vlan 2112 port 23

virtual-circuit ethernet create vc vcMgmt vlan 2112
virtual-switch ethernet create vs vsMgmt vc vcMgmt

interface create ip-interface intMgmt ip 47.134.10.182/22 ip-forwarding off
role device-mgmt priority 6
virtual -switch ethernet add vs vsVzMgmt ip-interface inMgmt vlan 127
```


Copyright© 2022 Ciena® Corporation

Procedure 7-38
Displaying double-tagged management

Display double-tagged management.

Step	Action

1 Display double-tagged management:

```
virtual-switch ethernet show vs <vs name>
```

where

vs <vs name> is the virtual switch you wish to display.

—end—

Example

The following example shows the output for the virtual switch vsMgmt.

```
>virtual-switch ethernet show vsMgmt

+-------------------- QinQ/PBT VIRTUAL SWITCH INFO ---------------------+
| Parameter             | Value                                         |
+-----------------------+-----------------------------------------------+
| Name                  | vsMgmt                                        |
| ID                    | 1025                                          |
| Description           |                                               |
| Mode                  | default                                       |
| Active VLAN           | (2112)  VLAN#2112                             |
| CPT Status            | Disabled                                      |
| CPT Method            | l2pt                                          |
| Transparent Validate  | off                                           |
| Mac Learning          | Enabled                                       |
| VC                    | (1025)  vcMgmt                                |
| Subscr Dot1D Policy   | leave                                         |
| Decap CoS Policy      | leave                                         |
| Decap Fixed Dot1DPri  | 2                                             |
| Encap CoS Policy      | fixed                                         |
| Encap Fixed Dot1DPri  | 2                                             |
| PFG State             | Disabled                                      |
|     Fwd-Policies      | A -> AB  B -> A                               |
|-----------------------------------------------------------------------|
+----------------------- Virtual Switch Members -----------------------+
| Port     | Subscriber | Translate | Encap Cos     |Encap Fixed | Fwd     |
|          | VLAN       | Tag       | Policy        | Dot1DPri   | Group   |
|----------+------------+-----------+---------------+------------+---------|
| 9        | 127        | 0         | vs-inherit    | 2          | A       |
|-----------------------------------------------------------------------|
+----------------- Virtual Switch IP-Interface Members -----------------+
| Interface Name                  | VLAN                                |
+---------------------------------+-------------------------------------+
| intMgmt                         | 127                                 |
+-----------------------------------------------------------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-39
Creating an unnumbered IP interface

Create an unnumbered IP interface (IPUI). IPUIs borrow the IP addresses of existing IPv4 numbered interfaces or loopback interfaces to provide network managers with a means to conserve IP addresses.

An IPUI can be created only after its donor IP or loopback interface has been created.

Note 1: Each IPUI interface must be associated with a VLAN.

Note 2: The IPUI operational state (“up” or “down”) is controlled by the operational state of both its donor interface and by the state of the IPUI interface itself - both must be in an “up” state for the IPUI operational state to be “up”. It is recommended that a loopback interface be used as the donor interface as the operational state of loopback interfaces is always “up”.

Step	Action

1 Create an unnumbered IP interface:

```
interface create ip-interface <ip-interface> ip
unnumbered donor-interface <donor-interface> vlan <VLAN>
[mtu <NUMBER: 1500-9216>] [ip-forwarding <on|off>] [mac
<MAC address:XX:XX:XX:XX:XX:XX][priority <NUMBER: 0-7>]
```

where

ip-interface <ip-interface>	is a maximum 15-character string to identify the interface. The following characters cannot be used: • ! • “ • % • , • / • ? • :
donor-interface <donor-interface>	is the name of the donor IP or loopback interface.
vlan <VLAN>	is the VLAN ID for this interface.
[mtu <NUMBER: 1500-9216>]	is the interface MTU size in bytes. The default value is 1500.

Copyright© 2022 Ciena® Corporation

where

[mac <MAC address: XX:XX:XX:XX:XX:XX>]	is the MAC address. If not explicitly assigned the MAC addressed is automatically assigned.
ip-forwarding <on|off>	determines whether IP forwarding is on or off. The default value is off.
i[priority <NUMBER: 0-7>]	is the egress priority (pcp) value on packets egressing this interface. The default value is 7.

Copyright© 2022 Ciena® Corporation

Procedure 7-40
Deleting an unnumbered IP interface

Delete an unnumbered IP interface when it is no longer required.

Note: An unnumbered IP interface cannot be deleted if it is attached to OSPF.

Step	Action
1	Delete an unnumbered IP interface: `interface delete ip-interface <ip-interface>` where ip-interface <ip-interface> is the name of the interface to be deleted.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-41
Modifying an unnumbered IP interface

Modify an unnumbered IP interface to change the current settings. The following settings can be modified:

- IP forwarding - can be enabled or disabled
- MTU size - permitted range is 1500 to 9216 bytes

Step	Action

1 Modify an unnumbered IP interface:

```
interface set ip-interface <Interface> {[ip-forwarding
<on|off>], [mtu <NUMBER: 1500-9216>], [priority <NUMBER:
0-7>]}
```

where

ip-interface <Interface>	is the unnumbered IP interface to be modified.
ip forwarding <on|off>	determines whether IP forwarding is on or off. The default value is off.
mtu <NUMBER: 1500-9216>	is the maximum transmission unit in bytes (maximum frame size). The default value is 1500.
priority <NUMBER: 0-7>	is the egress priority (pcp) value on packets egressing this interface. The default value is 7.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-42
Displaying static ARP entries

Display static ARP entries.

Step	Action
1	Display static ARP entries: `arp static show`

—end—

Example

The following example shows sample output for the arp static show command.

```
> arp static show
+----------------+------------------+--------------------+
| DestinationIp  |    DMAC          | ifName (ifIndex)   |
+----------------+------------------+--------------------+
|1.1.1.2         |00:02:5a:01:b3:c6 |Ref_Test        (5 )|
+----------------+------------------+--------------------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-43
Displaying the AIB table

Display the Adjacency Information Base (AIB) table to view adjacencies for tunnels and AIS when the next hop is reachable.

Step	Action
1	Display the AIB: `ip aib show [summary]|[details]` where summary — displays a summary of AIB information. details — displays detailed AIB information.

Example

The following example shows sample output for the ip aib show command.

```
> ip aib show
+---------------+-------+------------------+--------+
| NexthopIp     |ifIndex|   Dmac           | ObjIdx |
+---------------+-------+------------------+--------+
|1.1.1.2        |5      |00:02:5a:01:b3:c6 |4       |
+---------------+-------+------------------+--------+
```


Copyright© 2022 Ciena® Corporation

Procedure 7-44
Configuring an auxiliary IP interface

To enable support for auxiliary ping on a Ciena device, an IP interface with the role of auxiliary must be configured. Packets addressed to this interface can be accepted on any VLAN, or untagged.

You cannot specify a VLAN parameter for an interface with the role of auxiliary. The auxiliary IP interface is assigned a special reserved MAC (auxiliary MAC). It is not permitted to specify a MAC or service-mac parameter for an interface with the role of auxiliary.

A maximum of one IP interface with the role of auxiliary may be configured on the device.

Note: Only IPv4 is supported, meaning that the IP address must be IPv4.

Step	Action

1 Configure an IP address with the role of auxiliary:

```
interface create ip-interface <interface-name> ip <ip-address/subnet-mask> role <auxiliary>
```

where

ip-interface <ip-interface-name>	is a 15-character string to identify the interface. The following characters cannot be used: • ! • “ • % • , • / • ? • :
ip <IP address/ subnet-mask>	is the IP address with mask. The IP address must be IPv4.
role <auxiliary>	creates the IP interface with the role of auxiliary.
[priority <NUMBER:0-7>]	is the egress priority (or pcp) value on packets egressing this interface. The default value is 7.

—end—

Copyright© 2022 Ciena® Corporation

Procedure 7-45
Generating a ping

The parameters vtag-stack and egress-port are mandatory when initiating an auxiliary ping from the Ciena NTE.

To generate an untagged ping, specify a single *character in the vtag-stack parameter. If you require tagged traffic, the rules for the vtag-stack are as follows:

- The PCP and DEI values with the vtag-stack are optional. The TPID and VID are not optional. If you do not wish to specify a particular TPID, the value * may be used to indicate the default TPID (0x8100). TPIDs must be entered in hexadecimal format. Accepted values are 8100, 88a8 and 9100.
- If the PCP is not supplied, the PCP is populated from the “priority” setting of the auxiliary IP interface.
- If DEI is not populated it is set to 0.

The egress-port parameter must be a physical front panel port, not an aggregate port. If aggregation is being used, the originator of the command should specify a physical port that is one of the primary ports of the aggregate port.

Step	Action
1	Generate a ping: `ping vtag-stack <tpid>.<vid>[.<pcp> [.<dei>]] [:<tpid>.<vid>[.<pcp>[.<dei>]]] egress-port <port-name> [options] <host or ipv4 address>`

Copyright© 2022 Ciena® Corporation

where	
port-name	is the name of the port.
options	The options are as follows: • -s SIZE sends SIZE data bytes in packets. The default is 56. • -t TTL sets the TTL. • -I IFACE/IP uses the interface or IP address as source. If this option is specified, it must be the IP address/name of the auxiliary IP interface on the originating device. If it is not specified, the IP address of the auxiliary IP interface on the originating device is used as the source IP address by default The source and destination IP addresses for the ping command must be the same subnet or the auxiliary IP interface traffic cannot be routed. • -W SEC is the seconds to wait for the first response after all -c CNT packets are sent. The default is 10. • -q is the quiet option and only displays the output at the start and when finished.
host or ipv4 address	is the host name or IPv4 address of the auxiliary IP interface.

—end—

Examples

The following example generates an untagged ping.

```
> ping vtag-stack * egress-port 1 10.19.19.1
```

The following example generates a single ping.

```
> ping vtag-stack * .100 egress-port 1 10.19.19.1
```

The following example generates an untagged ping.

```
> ping vtag-stack 88a8.200.4.1:*.100 egress-port 1 10.10.19.1
```

The following example generates a double tag ping.

```
> ping vtag-stack 88a8.200.4.1:8100.100.7.0 egress-port 1 10.10.10.1
```


Copyright© 2022 Ciena® Corporation

Copyright© 2022 Ciena® Corporation

39XX/51XX Switches and Platforms

Advanced OAM Configuration

Copyright© 2022 Ciena® Corporation. All rights reserved.

SAOS 6.21.2
Publication: 009-3458-044
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**