



---

Junos<sup>®</sup> OS

# Ethernet Interfaces Configuration Guide

Release  
11.2



---

Published: 2011-05-20

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

#### *Junos® OS Ethernet Interfaces Configuration Guide*

Release 11.2

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

#### Revision History

May 2011—R1 Junos® OS 11.2

The information in this document is current as of the date listed in the revision history.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Abbreviated Table of Contents

	About This Guide .....	xxix
Part 1	Ethernet Interfaces Configuration Statements Overview	
Chapter 1	Ethernet Interfaces Configuration Statements and Hierarchy .....	3
Part 2	Configuring Ethernet Interfaces	
Chapter 2	Configuring Ethernet Interfaces .....	31
Chapter 3	Configuring 802.1Q VLANs .....	47
Chapter 4	Configuring Aggregated Ethernet Interfaces .....	75
Chapter 5	Stacking and Rewriting Gigabit Ethernet VLAN Tags .....	119
Chapter 6	Configuring Layer 2 Bridging Interfaces .....	141
Chapter 7	Configuring TCC and Layer 2.5 Switching .....	143
Chapter 8	Configuring Static ARP Table Entries .....	147
Chapter 9	Configuring Unrestricted Proxy ARP .....	149
Chapter 10	Configuring MAC Address Validation on Static Ethernet Interfaces .....	153
Chapter 11	Enabling Passive Monitoring on Ethernet Interfaces .....	155
Chapter 12	Configuring IEEE 802.1ag OAM Connectivity-Fault Management .....	159
Chapter 13	Configuring ITU-T Y.1731 Ethernet Service OAM .....	201
Chapter 14	Configuring IEEE 802.1x Port-Based Network Access Control .....	249
Chapter 15	Configuring IEEE 802.3ah OAM Link-Fault Management .....	253
Chapter 16	Configuring VRRP and VRRP for IPv6 .....	261
Chapter 17	Configuring Gigabit Ethernet Accounting and Policing .....	263
Chapter 18	Configuring Gigabit Ethernet Autonegotiation .....	277
Chapter 19	Configuring Gigabit Ethernet OTN Options .....	283
Chapter 20	Configuring the Management Ethernet Interface .....	285
Chapter 21	Configuring 10-Gigabit Ethernet LAN/WAN PICs .....	289
Chapter 22	Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength .....	297
Chapter 23	Configuring 10-Gigabit Ethernet Framing .....	299
Chapter 24	Configuring 10-Gigabit Ethernet Notification of Link Down Alarm .....	301
Chapter 25	Configuring 10-Gigabit Ethernet Notification of Link Down for Optics Alarms .....	303
Chapter 26	Configuring Point-to-Point Protocol over Ethernet .....	305
Chapter 27	Configuring Ethernet Ring Protection Switching .....	339

Chapter 28	Example Ethernet Configurations . . . . .	353
Part 3	Ethernet Interface Configuration Statements	
Chapter 29	Summary of Ethernet Interfaces Configuration Statements . . . . .	359
Part 4	Index	
	Index . . . . .	461
	Index of Statements and Commands . . . . .	471



# Table of Contents

	<b>About This Guide</b> . . . . .	<b>xxix</b>
	JUNOS Documentation and Release Notes . . . . .	xxix
	Objectives . . . . .	xxx
	Audience . . . . .	xxx
	Supported Routing Platforms . . . . .	xxx
	Using the Indexes . . . . .	xxx
	Using the Examples in This Manual . . . . .	xxx
	Merging a Full Example . . . . .	xxx
	Merging a Snippet . . . . .	xxx
	Documentation Conventions . . . . .	xxx
	Documentation Feedback . . . . .	xxx
	Requesting Technical Support . . . . .	xxx
	Self-Help Online Tools and Resources . . . . .	xxx
	Opening a Case with JTAC . . . . .	xxx
<b>Part 1</b>	<b>Ethernet Interfaces Configuration Statements Overview</b>	
<b>Chapter 1</b>	<b>Ethernet Interfaces Configuration Statements and Hierarchy</b> . . . . .	<b>3</b>
	[edit interfaces] Hierarchy Level . . . . .	3
	[edit logical-systems] Hierarchy Level . . . . .	19
	[edit protocols connections] Hierarchy Level . . . . .	23
	[edit protocols dot1x] Hierarchy Level . . . . .	24
	[edit protocols iccp] Hierarchy Level . . . . .	24
	[edit protocols lacp] Hierarchy Level . . . . .	24
	[edit protocols oam] Hierarchy Level . . . . .	24
	[edit protocols ppp] Hierarchy Level . . . . .	26
	[edit protocols pppoe] Hierarchy Level . . . . .	26
	[edit protocols protection-group] Hierarchy Level . . . . .	27
	[edit protocols vrrp] Hierarchy Level . . . . .	27
<b>Part 2</b>	<b>Configuring Ethernet Interfaces</b>	
<b>Chapter 2</b>	<b>Configuring Ethernet Interfaces</b> . . . . .	<b>31</b>
	Ethernet Interfaces Overview . . . . .	31
	Configuring Ethernet Physical Interface Properties . . . . .	32
	Configuring J Series Services Router Switching Interfaces . . . . .	36
	Example: Configuring J Series Services Router Switching Interfaces . . . . .	37
	MX Series Router Interface Identifiers . . . . .	37
	Enabling Ethernet MAC Address Filtering . . . . .	38
	Filtering Specific MAC Addresses . . . . .	39
	Configuring Ethernet Loopback Capability . . . . .	40

**Chapter 3**

Configuring Flow Control .....	41
Ignoring Layer 3 Incomplete Errors .....	41
Configuring the Link Characteristics on Ethernet Interfaces .....	41
Configuring Gratuitous ARP .....	42
Adjusting the ARP Aging Timer .....	43
Configuring the Interface Speed on Ethernet Interfaces .....	44
Configuring the Ingress Rate Limit .....	44
Configuring Multicast Statistics Collection on Ethernet Interfaces .....	45
Configuring Weighted Random Early Detection .....	45
<b>Configuring 802.1Q VLANs .....</b>	<b>47</b>
802.1Q VLANs Overview .....	47
Configuring Dynamic 802.1Q VLANs .....	48
802.1Q VLAN IDs and Ethernet Interface Types .....	49
Enabling VLAN Tagging .....	50
Configuring Single-Tag Framing .....	50
Configuring Dual Tagging .....	50
Configuring Mixed Tagging .....	51
Configuring Mixed Tagging Support for Untagged Packets .....	52
Example: Configuring Mixed Tagging .....	52
Example: Configuring Mixed Tagging to Support Untagged Packets .....	52
Binding VLAN IDs to Logical Interfaces .....	53
Binding VLAN IDs to Logical Interfaces Overview .....	53
Binding a VLAN ID to a Logical Interface .....	54
Binding a VLAN ID to a Single-Tag Logical Interface .....	54
Binding a VLAN ID to a Dual-Tag Logical Interface .....	54
Binding a Range of VLAN IDs to a Logical Interface .....	54
Binding a Range of VLAN IDs to a Single-Tag Logical Interface .....	54
Binding a Range of VLAN IDs to a Dual-Tag Logical Interface .....	55
Example: Binding Ranges VLAN IDs to Logical Interfaces .....	55
Binding a List of VLAN IDs to a Logical Interface .....	56
Binding a List of VLAN IDs to a Single-Tag Logical Interface .....	56
Binding a List of VLAN IDs to a Dual-Tag Logical Interface .....	56
Example: Binding Lists of VLAN IDs to Logical Interfaces .....	57
Associating VLAN IDs to VLAN Demux Interfaces .....	58
Associating VLAN IDs to VLAN Demux Interfaces Overview .....	58
Associating a VLAN ID to a VLAN Demux Interface .....	58
Associating a VLAN ID to a Single-Tag VLAN Demux Interface .....	58
Associating a VLAN ID to a Dual-Tag VLAN Demux Interface .....	58
Configuring VLAN Encapsulation .....	59
Example: Configuring VLAN Encapsulation on a Gigabit Ethernet Interface .....	60
Example: Configuring VLAN Encapsulation on an Aggregated Ethernet Interface .....	60

Configuring Extended VLAN Encapsulation . . . . .	60
Example: Configuring Extended VLAN Encapsulation on a Gigabit Ethernet Interface . . . . .	61
Example: Configuring Extended VLAN Encapsulation on an Aggregated Ethernet Interface . . . . .	61
Guidelines for Configuring VLAN ID List-Bundled Logical Interfaces That Connect CCCs . . . . .	62
Guidelines for Configuring Physical Link-Layer Encapsulation to Support CCCs . . . . .	62
Guidelines for Configuring Logical Link-Layer Encapsulation to Support CCCs . . . . .	62
Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface . . . . .	63
Configuring a VLAN-Bundled Logical Interface . . . . .	64
Specifying the Interface Over Which VPN Traffic Travels to the CE Router . . . . .	64
Specifying the Interface to Handle Traffic for a CCC . . . . .	64
Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface . . . . .	65
Configuring a VLAN-Bundled Logical Interface . . . . .	65
Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit . . . . .	66
Example: Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface . . . . .	66
Example: Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface . . . . .	68
Configuring a Logical Interface for Access Mode . . . . .	69
Example: Configuring a Logical Interface for Access Mode . . . . .	69
Configuring a Logical Interface for Trunk Mode . . . . .	70
Configuring the VLAN ID List for a Trunk Interface . . . . .	70
Configuring a Trunk Interface on a Bridge Network . . . . .	71
<b>Chapter 4 Configuring Aggregated Ethernet Interfaces . . . . .</b>	<b>75</b>
Aggregated Ethernet Interfaces Overview . . . . .	75
Platform Support for Aggregated Ethernet Interfaces . . . . .	76
Configuration Guidelines for Aggregated Ethernet Interfaces . . . . .	76
Configuring an Aggregated Ethernet Interface . . . . .	77
Deleting an Aggregated Ethernet Interface . . . . .	78
Configuring Multichassis Link Aggregation . . . . .	78
Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers	
Overview . . . . .	80
Data Traffic Forwarding Rules . . . . .	83
MAC Address Management . . . . .	85
MAC Aging . . . . .	85
Layer 3 Routing . . . . .	85
Address Resolution Protocol Active-Active MC-LAG Support	
Methodology . . . . .	86
IGMP Snooping on Active-Active MC-LAG . . . . .	86
Up and Down Event Handling . . . . .	87
Interchassis Control Protocol . . . . .	88

Interchassis Control Protocol Message . . . . .	88
Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link	
Aggregation on MX Series Routers . . . . .	88
Configuring MC-LAG . . . . .	89
Configuring Interchassis Link Label . . . . .	89
Configuring Multiple Chassis . . . . .	90
Configuring Service ID . . . . .	90
Configuring IGMP Snooping for Active-Active MC-LAG . . . . .	92
IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview . . . . .	93
IGMP snooping in MC-LAG active-active on MX Series Routers	
functionality . . . . .	93
Typically supported network topology for IGMP snooping with MC-LAG	
active-active bridging . . . . .	95
Control plane state updates triggered by packets received on remote	
chassis . . . . .	95
Data forwarding . . . . .	96
Pure Layer 2 topology without integrated routing and bridging . . . . .	97
Qualified learning . . . . .	97
Data forwarding with qualified learning . . . . .	98
Static groups on single homed interfaces . . . . .	98
Router facing interfaces as multichassis links . . . . .	98
Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers . . . . .	99
Configuring Aggregated Ethernet Link Protection . . . . .	100
Configuring Link Protection for Aggregated Ethernet Interfaces . . . . .	100
Configuring Primary and Backup Links for Link Aggregated Ethernet	
Interfaces . . . . .	101
Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup	
Link . . . . .	101
Disabling Link Protection for Aggregated Ethernet Interfaces . . . . .	101
Configuring the Number of Aggregated Ethernet Interfaces on the Device . . . . .	101
Configuring Aggregated Ethernet LACP . . . . .	102
Configuring the LACP Interval . . . . .	103
Configuring LACP Link Protection . . . . .	104
Enabling LACP Link Protection . . . . .	104
Configuring LACP System Priority . . . . .	105
Configuring LACP Port Priority . . . . .	106
Tracing LACP Operations . . . . .	106
Example: Configuring Aggregated Ethernet LACP . . . . .	107
Configuring Untagged Aggregated Ethernet Interfaces . . . . .	108
Example: Configuring Untagged Aggregated Ethernet Interfaces . . . . .	109
Configuring Aggregated Ethernet Link Speed . . . . .	109
Configuring Aggregated Ethernet Minimum Links . . . . .	110
Configuring Multicast Statistics Collection on Aggregated Ethernet	
Interfaces . . . . .	111
Configuring Hierarchical Scheduler on Aggregated Ethernet Interfaces Without	
Link Protection . . . . .	111

	Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers . . . . .	112
	Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview . . . . .	112
	Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers . . . . .	113
	Example Configurations . . . . .	116
	Example Configurations of Chassis Wide Settings . . . . .	116
	Example Configurations of Per-Packet-Forwarding-Engine Settings . . . . .	116
<b>Chapter 5</b>	<b>Stacking and Rewriting Gigabit Ethernet VLAN Tags . . . . .</b>	<b>119</b>
	Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview . . . . .	119
	Stacking and Rewriting Gigabit Ethernet VLAN Tags . . . . .	120
	Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames . . . . .	123
	Configuring Stacked VLAN Tagging . . . . .	124
	Configuring Dual VLAN Tags . . . . .	124
	Configuring Inner and Outer TPIDs and VLAN IDs . . . . .	124
	Stacking a VLAN Tag . . . . .	127
	Removing a VLAN Tag . . . . .	128
	Removing the Outer and Inner VLAN Tags . . . . .	128
	Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag . . . . .	129
	Stacking Two VLAN Tags . . . . .	129
	Rewriting the VLAN Tag on Tagged Frames . . . . .	130
	Rewriting a VLAN Tag on Untagged Frames . . . . .	131
	Rewriting a VLAN Tag and Adding a New Tag . . . . .	133
	Rewriting the Inner and Outer VLAN Tags . . . . .	134
	Examples: Stacking and Rewriting Gigabit Ethernet IQ VLAN Tags . . . . .	134
<b>Chapter 6</b>	<b>Configuring Layer 2 Bridging Interfaces . . . . .</b>	<b>141</b>
	Layer 2 Bridging Interfaces Overview . . . . .	141
	Configuring Layer 2 Bridging Interfaces . . . . .	141
	Example: Configuring Layer 2 Bridging Interfaces . . . . .	142
<b>Chapter 7</b>	<b>Configuring TCC and Layer 2.5 Switching . . . . .</b>	<b>143</b>
	TCC and Layer 2.5 Switching Overview . . . . .	143
	Configuring VLAN TCC Encapsulation . . . . .	143
	Configuring Ethernet TCC . . . . .	144
	Example: Configuring an Ethernet TCC or Extended VLAN TCC . . . . .	145
<b>Chapter 8</b>	<b>Configuring Static ARP Table Entries . . . . .</b>	<b>147</b>
	Static ARP Table Entries Overview . . . . .	147
	Configuring Static ARP Table Entries . . . . .	147
	Example: Configuring Static ARP Table Entries . . . . .	148
<b>Chapter 9</b>	<b>Configuring Unrestricted Proxy ARP . . . . .</b>	<b>149</b>
	Unrestricted Proxy ARP Overview . . . . .	149
	Configuring Unrestricted Proxy ARP . . . . .	150

<b>Chapter 10</b>	<b>Configuring MAC Address Validation on Static Ethernet Interfaces . . . . .</b>	<b>153</b>
	MAC Address Validation on Static Ethernet Interfaces Overview . . . . .	153
	Configuring MAC Address Validation on Static Ethernet Interfaces . . . . .	153
	Example of Strict MAC Validation on a Static Ethernet Interface . . . . .	154
	Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors . . . . .	154
<b>Chapter 11</b>	<b>Enabling Passive Monitoring on Ethernet Interfaces . . . . .</b>	<b>155</b>
	Passive Monitoring on Ethernet Interfaces Overview . . . . .	155
	Enabling Passive Monitoring on Ethernet Interfaces . . . . .	156
<b>Chapter 12</b>	<b>Configuring IEEE 802.1ag OAM Connectivity-Fault Management . . . . .</b>	<b>159</b>
	IEEE 802.1ag OAM Connectivity Fault Management Overview . . . . .	159
	Connectivity Fault Management Key Elements . . . . .	160
	Creating the Maintenance Domain . . . . .	161
	Configuring the Maintenance Domain Name Format . . . . .	161
	Configuring the Maintenance Domain Level . . . . .	161
	Configuring Maintenance Intermediate Points . . . . .	162
	Configuring MIP for Bridge Domains of a Virtual Switch . . . . .	162
	Configuring the Maintenance Domain Bridge Domain . . . . .	163
	Configuring the Maintenance Domain Instance . . . . .	163
	Configuring the Maintenance Domain MIP Half Function . . . . .	163
	Creating a Maintenance Association . . . . .	163
	Continuity Check Protocol . . . . .	164
	Configuring the Continuity Check . . . . .	164
	Configuring the Continuity Check Hold Interval . . . . .	164
	Configuring the Continuity Check Interval . . . . .	165
	Configuring the Continuity Check Loss Threshold . . . . .	165
	Continuity Measurement . . . . .	165
	Configuring a Maintenance Endpoint . . . . .	166
	Enabling Maintenance Endpoint Automatic Discovery . . . . .	166
	Configuring the Maintenance Endpoint Direction . . . . .	166
	Configuring the Maintenance Endpoint Interface . . . . .	167
	Configuring the Maintenance Endpoint Priority . . . . .	167
	Configuring the Maintenance Endpoint Lowest Priority Defect . . . . .	167
	Configuring a Remote Maintenance Endpoint . . . . .	168
	Configuring a Remote Maintenance Endpoint Action Profile . . . . .	168
	Configuring Maintenance Endpoint Service Protection . . . . .	169
	Configuring a Connectivity Fault Management Action Profile . . . . .	170
	Configuring the Action of a CFM Action Profile . . . . .	170
	Configuring the Default Actions of a CFM Action Profile . . . . .	171
	Configuring a CFM Action Profile Event . . . . .	172
	Configuring Linktrace Protocol in CFM . . . . .	173
	Configuring the Linktrace Path Age Timer . . . . .	173
	Configuring the Linktrace Database Size . . . . .	173

Configuring Ethernet Local Management Interface . . . . .	173
Ethernet Local Management Interface Overview . . . . .	173
Configuring the Ethernet Local Management Interface . . . . .	175
Configuring an OAM Protocol (CFM) . . . . .	175
Assigning the OAM Protocol to an EVC . . . . .	175
Enabling E-LMI on an Interface and Mapping CE VLAN IDs to an EVC . . . . .	176
Example E-LMI Configuration . . . . .	177
Configuring PE1 . . . . .	177
Configuring PE2 . . . . .	178
Configuring Two UNIs Sharing the Same EVC . . . . .	180
Configuring Port Status TLV and Interface Status TLV . . . . .	180
TLVs Overview . . . . .	181
Various TLVs for CFM PDUs . . . . .	181
Support for Additional Optional TLVs . . . . .	183
Port Status TLV . . . . .	183
Interface Status TLV . . . . .	186
MAC Status Defects . . . . .	189
Configuring Remote MEP Action Profile Support . . . . .	190
Monitoring a Remote MEP Action Profile . . . . .	191
Configuring MAC Flush Message Processing in CET Mode . . . . .	192
Configuring a Connection Protection TLV Action Profile . . . . .	194
Configuring M120 and MX Series Routers for CCC Encapsulated Packets . . . . .	195
IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview . . . . .	195
CFM Features Supported on Layer 2 VPN Circuits . . . . .	195
Configuring CFM for CCC Encapsulated Packets . . . . .	196
Configuring Rate Limiting of Ethernet OAM Messages . . . . .	196
Configuring 802.1ag Ethernet OAM for VPLS . . . . .	198
<b>Chapter 13</b>	
<b>Configuring ITU-T Y.1731 Ethernet Service OAM . . . . .</b>	<b>201</b>
Service-Level Agreement Measurement . . . . .	202
Ethernet Frame Delay Measurements Overview . . . . .	202
ITU-T Y.1731 Frame Delay Measurement Feature . . . . .	203
Ethernet CFM . . . . .	203
Ethernet Frame Delay Measurement . . . . .	204
One-Way Ethernet Frame Delay Measurement . . . . .	204
1DM Transmission . . . . .	204
1DM Reception . . . . .	204
One-Way ETH-DM Statistics . . . . .	205
One-Way ETH-DM Frame Counts . . . . .	205
Synchronization of System Clocks . . . . .	205
Two-Way Ethernet Frame Delay Measurement . . . . .	205
DMM Transmission . . . . .	205
DMR Transmission . . . . .	206
DMR Reception . . . . .	206
Two-Way ETH-DM Statistics . . . . .	206
Two-Way ETH-DM Frame Counts . . . . .	206
Choosing Between One-Way and Two-Way ETH-DM . . . . .	207

Restrictions for Ethernet Frame Delay Measurement . . . . .	207
Ethernet Frame Loss Measurement Overview . . . . .	208
On-Demand Mode . . . . .	209
Proactive Mode . . . . .	210
Ethernet Delay Measurements and Loss Measurement by Proactive Mode . . . . .	211
Configuring an Iterator Profile . . . . .	211
Configuring a Remote MEP with an Iterator Profile . . . . .	213
Configuring Statistical Frame Loss Measurement for VPLS Connections . . . . .	214
Guidelines for Configuring Routers to Support an ETH-DM Session . . . . .	215
Configuration Requirements for ETH-DM . . . . .	215
Configuration Options for ETH-DM . . . . .	216
Guidelines for Starting an ETH-DM Session . . . . .	216
ETH-DM Session Prerequisites . . . . .	216
ETH-DM Session Parameters . . . . .	217
Restrictions for an ETH-DM Session . . . . .	218
Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts . . . . .	218
ETH-DM Statistics . . . . .	219
ETH-DM Statistics Retrieval . . . . .	220
ETH-DM Frame Counts . . . . .	221
ETH-DM Frame Count Retrieval . . . . .	221
Frame Counts Stored in CFM Databases . . . . .	221
One-Way ETH-DM Frame Counts . . . . .	222
Two-Way ETH-DM Frame Counts . . . . .	222
Configuring Routers to Support an ETH-DM Session . . . . .	223
Configuring MEP Interfaces . . . . .	223
Ensuring that Distributed ppm Is Not Disabled . . . . .	224
Enabling the Hardware-Assisted Timestamping Option . . . . .	225
Configuring the Server-Side Processing Option . . . . .	226
Starting an ETH-DM Session . . . . .	226
Using the monitor ethernet delay-measurement Command . . . . .	226
Starting a One-Way ETH-DM Session . . . . .	227
Starting a Two-Way ETH-DM Session . . . . .	228
Managing ETH-DM Statistics and ETH-DM Frame Counts . . . . .	228
Displaying ETH-DM Statistics Only . . . . .	228
Displaying ETH-DM Statistics and Frame Counts . . . . .	229
Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity . . . . .	229
Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level . . . . .	230
Clearing ETH-DM Statistics and Frame Counts . . . . .	231
Managing ETH-LM Statistics . . . . .	231
Displaying ETH-LM Statistics . . . . .	231
Clearing ETH-LM Statistics . . . . .	232
Managing Iterator Statistics . . . . .	233
Displaying Iterator Statistics . . . . .	233
Clearing Iterator Statistics . . . . .	237



	Managing Continuity Measurement Statistics . . . . .	238
	Displaying Continuity Measurement Statistics . . . . .	238
	Clearing Continuity Measurement Statistics . . . . .	238
	Example: One-Way Ethernet Frame Delay Measurement . . . . .	238
	Description of the One-Way Frame Delay Measurement Example . . . . .	238
	Routers Used in This Example . . . . .	239
	ETH-DM Frame Counts for this Example . . . . .	239
	ETH-DM Statistics for this Example . . . . .	239
	Steps for the One-Way Frame Delay Measurement Example . . . . .	240
	Example: Configuring an Iterator . . . . .	246
	Example: Configuring an Iterator Profile for Two-way Delay Measurement . . . . .	246
	Example: Configuring an Iterator Profile for Loss Measurement . . . . .	246
	Example: Configuring a Remote MEP with an Iterator Profile . . . . .	246
	Example: Disabling an Iterator Profile with the disable Statement . . . . .	247
	Example: Disabling an Iterator Profile by Deactivating the Profile . . . . .	247
<b>Chapter 14</b>	<b>Configuring IEEE 802.1x Port-Based Network Access Control . . . . .</b>	<b>249</b>
	IEEE 802.1x Port-Based Network Access Control Overview . . . . .	249
	Understanding the Administrative State of the Authenticator Port . . . . .	250
	Understanding the Administrative Mode of the Authenticator Port . . . . .	250
	Configuring the Authenticator . . . . .	250
	Viewing the dot1x Configuration . . . . .	251
<b>Chapter 15</b>	<b>Configuring IEEE 802.3ah OAM Link-Fault Management . . . . .</b>	<b>253</b>
	IEEE 802.3ah OAM Link-Fault Management Overview . . . . .	253
	Configuring IEEE 802.3ah OAM Link-Fault Management . . . . .	254
	Enabling IEEE 802.3ah OAM Support . . . . .	254
	Configuring Link Discovery . . . . .	255
	Configuring the OAM PDU Interval . . . . .	255
	Configuring the OAM PDU Threshold . . . . .	255
	Configuring Threshold Values for Local Fault Events on an Interface . . . . .	255
	Disabling the Sending of Link Event TLVs . . . . .	256
	Detecting Remote Faults . . . . .	256
	Configuring an OAM Action Profile . . . . .	256
	Specifying the Actions to Be Taken for Link-Fault Management Events . . . . .	257
	Monitoring the Loss of Link Adjacency . . . . .	258
	Monitoring Protocol Status . . . . .	258
	Configuring Threshold Values for Fault Events in an Action Profile . . . . .	258
	Applying an Action Profile . . . . .	259
	Setting a Remote Interface into Loopback Mode . . . . .	259
	Enabling Remote Loopback Support on the Local Interface . . . . .	259
	Example: Configuring IEEE 802.3ah OAM Support on an Interface . . . . .	260
<b>Chapter 16</b>	<b>Configuring VRRP and VRRP for IPv6 . . . . .</b>	<b>261</b>
	VRRP and VRRP for IPv6 Overview . . . . .	261
	Configuring VRRP and VRRP for IPv6 . . . . .	261

<b>Chapter 17</b>	<b>Configuring Gigabit Ethernet Accounting and Policing . . . . .</b>	<b>263</b>
	Gigabit Ethernet Accounting and Policing Overview . . . . .	263
	Configuring Gigabit Ethernet Policers . . . . .	265
	Configuring a Policer . . . . .	266
	Specifying an Input Priority Map . . . . .	266
	Specifying an Output Priority Map . . . . .	267
	Applying a Policer . . . . .	268
	Configuring MAC Address Filtering . . . . .	269
	Example: Configuring Gigabit Ethernet Policers . . . . .	270
	Configuring Gigabit Ethernet Two-Color and Tricolor Policers . . . . .	271
	Configuring a Policer . . . . .	272
	Applying a Policer . . . . .	273
	Example: Configuring and Applying a Policer . . . . .	273
	Configuring MAC Address Accounting . . . . .	274
<b>Chapter 18</b>	<b>Configuring Gigabit Ethernet Autonegotiation . . . . .</b>	<b>277</b>
	Gigabit Ethernet Autonegotiation Overview . . . . .	277
	Configuring Gigabit Ethernet Autonegotiation . . . . .	277
	Configuring Gigabit Ethernet Autonegotiation with Remote Fault . . . . .	278
	Configuring Flow Control . . . . .	278
	Configuring Autonegotiation Speed on MX Series Routers . . . . .	278
	Displaying Autonegotiation Status . . . . .	278
<b>Chapter 19</b>	<b>Configuring Gigabit Ethernet OTN Options . . . . .</b>	<b>283</b>
	Gigabit Ethernet OTN Options Configuration Overview . . . . .	283
	Gigabit Ethernet OTN Options . . . . .	283
<b>Chapter 20</b>	<b>Configuring the Management Ethernet Interface . . . . .</b>	<b>285</b>
	Management Ethernet Interface Overview . . . . .	285
	Configuring a Consistent Management IP Address . . . . .	285
	Configuring the MAC Address on the Management Ethernet Interface . . . . .	286
<b>Chapter 21</b>	<b>Configuring 10-Gigabit Ethernet LAN/WAN PICs . . . . .</b>	<b>289</b>
	10-Gigabit Ethernet LAN/WAN PIC Overview . . . . .	289
	Configuring Line-Rate Mode on 10-Gigabit Ethernet LAN/WAN PIC . . . . .	292
	Configuring Control Queue Disable on a 10-Gigabit Ethernet LAN/WAN PIC . . . . .	292
	Example: Handling Oversubscription on a 10-Gigabit Ethernet LAN/WAN PIC . . . . .	295
<b>Chapter 22</b>	<b>Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength . . . . .</b>	<b>297</b>
	10-Gigabit Ethernet DWDM Interface Wavelength Overview . . . . .	297
	Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength . . . . .	297
<b>Chapter 23</b>	<b>Configuring 10-Gigabit Ethernet Framing . . . . .</b>	<b>299</b>
	10-Gigabit Ethernet Framing Overview . . . . .	299
	Configuring 10-Gigabit Ethernet Framing . . . . .	299
	Understanding WAN Framing for 10-Gigabit Ethernet Trio Interfaces . . . . .	300
<b>Chapter 24</b>	<b>Configuring 10-Gigabit Ethernet Notification of Link Down Alarm . . . . .</b>	<b>301</b>
	10-Gigabit Ethernet Notification of Link Down Alarm Overview . . . . .	301
	Configuring 10-Gigabit Ethernet Notification of Link Down Alarm . . . . .	301

<b>Chapter 25</b>	<b>Configuring 10-Gigabit Ethernet Notification of Link Down for Optics Alarms</b>	<b>303</b>
	10-Gigabit Ethernet Notification of Link Down for Optics Options Overview . . .	303
	Configuring 10-Gigabit Ethernet Link Down Notification for Optics Options Alarm or Warning . . . . .	303
<b>Chapter 26</b>	<b>Configuring Point-to-Point Protocol over Ethernet</b>	<b>305</b>
	PPPoE Overview . . . . .	306
	PPPoE Interfaces . . . . .	306
	Ethernet Interface . . . . .	307
	PPPoE Stages . . . . .	307
	PPPoE Discovery Stage . . . . .	307
	PPPoE Session Stage . . . . .	308
	Optional CHAP Authentication . . . . .	308
	Understanding PPPoE Service Name Tables . . . . .	309
	Interaction Among PPPoE Clients and Routers During the Discovery Stage . . . . .	309
	Service Entries and Actions in PPPoE Service Name Tables . . . . .	310
	ACI/ARI Pairs in PPPoE Service Name Tables . . . . .	311
	Dynamic Profiles and Routing Instances in PPPoE Service Name Tables . . .	312
	Maximum Sessions Limit in PPPoE Service Name Tables . . . . .	312
	Static PPPoE Interfaces in PPPoE Service Name Tables . . . . .	313
	PADO Advertisement of Named Services in PPPoE Service Name Tables . . . . .	313
	Evaluation Order for Matching Client Information in PPPoE Service Name Tables . . . . .	314
	Benefits of Configuring PPPoE Service Name Tables . . . . .	314
	Configuring PPPoE . . . . .	315
	Setting the Appropriate Encapsulation on the PPPoE Interface . . . . .	316
	Configuring PPPoE Encapsulation on an Ethernet Interface . . . . .	317
	Configuring PPPoE Encapsulation on an ATM-over-ADSL Interface . . .	317
	Configuring a PPPoE Interface . . . . .	317
	Configuring the PPPoE Underlying Interface . . . . .	318
	Identifying the Access Concentrator . . . . .	318
	Configuring the PPPoE Automatic Reconnect Wait Timer . . . . .	319
	Configuring the PPPoE Service Name . . . . .	319
	Configuring the PPPoE Server Mode . . . . .	319
	Configuring the PPPoE Client Mode . . . . .	319
	Configuring the PPPoE Source and Destination Addresses . . . . .	320
	Deriving the PPPoE Source Address From a Specified Interface . . . . .	320
	Configuring the PPPoE IP Address by Negotiation . . . . .	320
	Configuring the Protocol MTU PPPoE . . . . .	320
	Example: Configuring a PPPoE Client Interface on a J Series Services Router . . . . .	321
	Example: Configuring a PPPoE Server Interface on an M120 or M320 Router . . . . .	322
	Disabling the Sending of PPPoE Keepalive Messages . . . . .	322
	Configuring PPPoE Service Name Tables . . . . .	323
	Creating a Service Name Table . . . . .	324

	Configuring the Action Taken When the Client Request Includes an Empty Service Name Tag . . . . .	324
	Configuring the Action Taken for the Any Service . . . . .	325
	Assigning a Service to a Service Name Table and Configuring the Action Taken When the Client Request Includes a Non-zero Service Name Tag . . . . .	326
	Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information . . . . .	328
	Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name . . . . .	329
	Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client . . . . .	330
	Enabling Advertisement of Named Services in PADO Control Packets . . . . .	331
	Assigning a Service Name Table to a PPPoE Underlying Interface . . . . .	331
	Example: Configuring a PPPoE Service Name Table . . . . .	331
	Tracing PPPoE Operations . . . . .	334
	Configuring the PPPoE Trace Log Filename . . . . .	335
	Configuring the Number and Size of PPPoE Log Files . . . . .	335
	Configuring Access to the PPPoE Log File . . . . .	335
	Configuring a Regular Expression for PPPoE Lines to Be Logged . . . . .	335
	Configuring the PPPoE Tracing Flags . . . . .	336
	Troubleshooting PPPoE Service Name Tables . . . . .	336
	Verifying a PPPoE Configuration . . . . .	338
<b>Chapter 27</b>	<b>Configuring Ethernet Ring Protection Switching . . . . .</b>	<b>339</b>
	Ethernet Ring Protection Switching Overview . . . . .	339
	Understanding Ethernet Ring Protection Switching Functionality . . . . .	340
	Acronyms . . . . .	340
	Ring Nodes . . . . .	340
	Ring Node States . . . . .	341
	Failure Detection . . . . .	341
	Logical Ring . . . . .	341
	FDB Flush . . . . .	341
	Traffic Blocking and Forwarding . . . . .	341
	RAPS Message Blocking and Forwarding . . . . .	341
	Dedicated Signaling Control Channel . . . . .	343
	RAPS Message Termination . . . . .	343
	Manual Switch . . . . .	343
	Nonrevertive Switch . . . . .	343
	Multiple Rings . . . . .	343
	Node ID . . . . .	343
	Bridge Domains with the Ring Port . . . . .	343
	Configuring Ethernet Ring Protection Switching . . . . .	344
	Example: Ethernet Ring Protection Switching Configuration . . . . .	345
<b>Chapter 28</b>	<b>Example Ethernet Configurations . . . . .</b>	<b>353</b>
	Example: Configuring Fast Ethernet Interfaces . . . . .	353
	Example: Configuring Gigabit Ethernet Interfaces . . . . .	353
	Example: Configuring Aggregated Ethernet Interfaces . . . . .	354
	Example: Configuring Aggregated Ethernet Link Protection . . . . .	355

## Part 3

## Ethernet Interface Configuration Statements

## Chapter 29

<b>Summary of Ethernet Interfaces Configuration Statements . . . . .</b>	<b>359</b>
802.3ad . . . . .	359
aggregate (Gigabit Ethernet CoS Policer) . . . . .	360
aggregated-ether-options . . . . .	361
auto-negotiation . . . . .	363
bandwidth-limit (Policer for Gigabit Ethernet Interfaces) . . . . .	364
burst-size-limit (Policer for Gigabit Ethernet Interfaces) . . . . .	364
classifier . . . . .	365
ethernet (Protocols OAM) . . . . .	366
ethernet-policer-profile . . . . .	369
ethernet-ring . . . . .	370
ethernet-switch-profile . . . . .	371
fastether-options . . . . .	372
flow-control . . . . .	373
flow-control-options . . . . .	374
forwarding-class (Gigabit Ethernet IQ Classifier) . . . . .	374
forwarding-mode (100-Gigabit Ethernet) . . . . .	375
framing (10-Gigabit Ethernet Interfaces) . . . . .	376
gether-options . . . . .	377
gratuitous-arp-reply . . . . .	378
ieee802.1p . . . . .	379
ignore-l3-incompletes . . . . .	379
ingress-rate-limit . . . . .	380
inner-tag-protocol-id . . . . .	380
inner-vlan-id . . . . .	381
inner-vlan-id-range . . . . .	382
input-priority-map . . . . .	382
input-vlan-map . . . . .	383
input-vlan-map (Aggregated Ethernet) . . . . .	383
input-vlan-map (Gigabit Ethernet IQ and 10-Gigabit Ethernet SFPP) . . . . .	384
interfaces . . . . .	384
lACP . . . . .	385
lACP (802.3ad) . . . . .	385
lACP (Aggregated Ethernet) . . . . .	386
link-discovery . . . . .	387
link-fault-management . . . . .	388
link-mode . . . . .	389
link-protection . . . . .	390
link-speed (Aggregated Ethernet) . . . . .	391
loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet) . . . . .	392
loss-priority . . . . .	392
mac-learn-enable . . . . .	393
mep . . . . .	394
minimum-links . . . . .	395
mip-half-function . . . . .	396
mpls . . . . .	397
no-auto-mdix . . . . .	397

no-gratuitous-arp-request	398
oam	399
optics-options	401
output-priority-map	402
pdu-interval	402
pdu-threshold	403
periodic	404
policer	405
policer (CFM Firewall)	405
policer (CFM Global)	406
policer (CFM Session)	407
policer (CoS)	408
policer (MAC)	409
pop	410
pop-pop	410
pop-swap	411
port-status-tlv	411
ppp-options	412
pppoe-options	413
pppoe-underlying-options (Static and Dynamic Subscribers)	414
premium	415
premium (Hierarchical Policer)	415
premium (Output Priority Map)	416
premium (Policer)	416
protection-group	417
protocol-down	418
push	418
push-push	419
remote-mep	420
request	420
ring-protection-link-end	421
ring-protection-link-owner	421
sa-multicast (100-Gigabit Ethernet)	422
source-address-filter	423
source-filtering	424
speed	425
speed (Ethernet)	425
speed (MX Series DPC)	426
swap	427
swap-push	427
swap-swap	428
switch-options	428
switch-port	429
tag-protocol-id	430
tag-protocol-id (TPIDs Expected to Be Sent or Received)	430
tag-protocol-id (TPID to Rewrite)	431
unit	432

vlan-id	438
vlan-id (Logical Port in Bridge Domain)	438
vlan-id (Outer VLAN ID)	439
vlan-id (VLAN ID to Be Bound to a Logical Interface)	439
vlan-id (VLAN ID to Rewrite)	440
vlan-id-list	441
vlan-id-list (Ethernet VLAN Circuit)	442
vlan-id-list (Interface in Bridge Domain)	443
vlan-id-range	444
vlan-ranges	445
vlan-rewrite	446
vlan-rule (100-Gigabit Ethernet)	446
vlan-steering (100-Gigabit Ethernet)	447
vlan-tagging	448
vlan-tags	449
vlan-tags (Dual-Tagged Logical Interface)	450
vlan-tags (Stacked VLAN Tags)	452
vlan-tags-outer	453
vlan-vci-tagging	453
wavelength	454
west-interface	457
working-circuit	458

## Part 4

## Index

Index	461
Index of Statements and Commands	471





# List of Figures

<b>Part 2</b>	<b>Configuring Ethernet Interfaces</b>	
<b>Chapter 4</b>	<b>Configuring Aggregated Ethernet Interfaces</b>	<b>75</b>
	Figure 1: Single Multichassis Link	80
	Figure 2: Dual Multichassis Link	80
	Figure 3: Interchassis Data Link Between Active-Active Nodes	81
	Figure 4: Active-Active MC-LAG with Single MC-LAG	81
	Figure 5: Active-Active MC-LAG with Multiple Nodes on a Single Multichassis Link	82
	Figure 6: MC-LAG Device and Single-Homed Client	83
	Figure 7: Loop Caused by the ICL Links	84
	Figure 8: Multicast topology with source connected via Layer 3	86
	Figure 9: Multicast topology with source connected via MC-Link	87
	Figure 10: N1 and N2 for the same service with same service ID	91
	Figure 11: Bridge Domain with Logical Interfaces from Two MC-AE Interfaces	92
	Figure 12: Typical network over which active-active is supported	95
	Figure 13: Layer 2 configuration without integrated routing and bridging	97
	Figure 14: Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers	113
<b>Chapter 7</b>	<b>Configuring TCC and Layer 2.5 Switching</b>	<b>143</b>
	Figure 15: Topology of Layer 2.5 Translational Cross-Connect	145
<b>Chapter 9</b>	<b>Configuring Unrestricted Proxy ARP</b>	<b>149</b>
	Figure 16: Edge Device Case for Unrestricted Proxy ARP	150
	Figure 17: Core Device Case for Unrestricted Proxy ARP	150
<b>Chapter 12</b>	<b>Configuring IEEE 802.1ag OAM Connectivity-Fault Management</b>	<b>159</b>
	Figure 18: Relationship Among MEPs, MIPs, and Maintenance Domain Levels	160
	Figure 19: Relationship Among Bridges, Maintenance Domains, Maintenance Associations, and MEPs	161
	Figure 20: Scope of the E-LMI Protocol	174
	Figure 21: E-LMI Configuration for a Point-to-Point EVC (SVLAN) Monitored by CFM	177
	Figure 22: CET inter-op dual homed topology	193
	Figure 23: CET inter-op dual attached topology	194
	Figure 24: Layer 2 VPN Topology	195
<b>Chapter 13</b>	<b>Configuring ITU-T Y.1731 Ethernet Service OAM</b>	<b>201</b>
	Figure 25: Relationship of MEPs, MIPs, and Maintenance Domain Levels	204
<b>Chapter 21</b>	<b>Configuring 10-Gigabit Ethernet LAN/WAN PICs</b>	<b>289</b>
	Figure 26: Control Queue Rate Limiter Scenario	293

<b>Chapter 26</b>	<b>Configuring Point-to-Point Protocol over Ethernet . . . . .</b>	<b>305</b>
	Figure 27: PPPoE Session on an Ethernet Loop . . . . .	307
<b>Chapter 27</b>	<b>Configuring Ethernet Ring Protection Switching . . . . .</b>	<b>339</b>
	Figure 28: Protocol Packets from the Network to the Router . . . . .	342
	Figure 29: Protocol Packets from the Router to the Network . . . . .	342
	Figure 30: Example of a Three-Node Ring Topology . . . . .	345

# List of Tables

	<b>About This Guide</b> .....	<b>xxix</b>
	Table 1: Notice Icons .....	xxxiii
	Table 2: Text and Syntax Conventions .....	xxxiii
<b>Part 2</b>	<b>Configuring Ethernet Interfaces</b>	
<b>Chapter 3</b>	<b>Configuring 802.1Q VLANs</b> .....	<b>47</b>
	Table 3: VLAN ID Range by Interface Type .....	49
	Table 4: Configuration Statements Used to Bind VLAN IDs to Logical Interfaces .....	53
	Table 5: Configuration Statements Used to Associate VLAN IDs to VLAN Demux Interfaces .....	58
	Table 6: Encapsulation Inside Circuits CCC-Connected by VLAN-Bundled Logical Interfaces .....	63
<b>Chapter 4</b>	<b>Configuring Aggregated Ethernet Interfaces</b> .....	<b>75</b>
	Table 7: Untagged Aggregated Ethernet and LACP Support by PIC and Platform .....	108
<b>Chapter 5</b>	<b>Stacking and Rewriting Gigabit Ethernet VLAN Tags</b> .....	<b>119</b>
	Table 8: Rewrite Operations on Untagged, Single-Tagged, and Dual-Tagged Frames .....	121
	Table 9: Applying Rewrite Operations to VLAN Maps .....	122
	Table 10: Rewrite Operations and Statement Usage for Input VLAN Maps .....	126
	Table 11: Rewrite Operations and Statement Usage for Output VLAN Maps .....	126
	Table 12: Input VLAN Map Statements Allowed for ethernet-ccc and ethernet-vpls Encapsulations .....	132
	Table 13: Output VLAN Map Statements Allowed for ethernet-ccc and ethernet-vpls Encapsulations .....	132
	Table 14: Rules for Applying Rewrite Operations to VLAN Maps .....	132
<b>Chapter 12</b>	<b>Configuring IEEE 802.1ag OAM Connectivity-Fault Management</b> .....	<b>159</b>
	Table 15: Lowest Priority Defect Options .....	168
	Table 16: Service Protection Options .....	169
	Table 17: Format of TLVs .....	181
	Table 18: Type Field Values for Various TLVs for CFM PDUs .....	181
	Table 19: Port Status TLV Format .....	184
	Table 20: Port Status TLV Values .....	184
	Table 21: Interface Status TLV Format .....	186
	Table 22: Interface Status TLV Values .....	186
<b>Chapter 13</b>	<b>Configuring ITU-T Y.1731 Ethernet Service OAM</b> .....	<b>201</b>

	Table 23: ETH-DM Statistics . . . . .	219
	Table 24: ETH-DM Frame Counts . . . . .	221
	Table 25: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields . . . . .	234
	Table 26: Displaying Iterator Statistics for Ethernet Loss Measurement Output Fields . . . . .	236
<b>Chapter 17</b>	<b>Configuring Gigabit Ethernet Accounting and Policing . . . . .</b>	<b>263</b>
	Table 27: Capabilities of Gigabit Ethernet IQ and Gigabit Ethernet with SFPs . .	264
	Table 28: Default Forwarding Classes . . . . .	267
<b>Chapter 18</b>	<b>Configuring Gigabit Ethernet Autonegotiation . . . . .</b>	<b>277</b>
	Table 29: Mode and Autonegotiation Status (Local) . . . . .	279
	Table 30: Mode and Autonegotiation Status (Remote) . . . . .	281
<b>Chapter 21</b>	<b>Configuring 10-Gigabit Ethernet LAN/WAN PICs . . . . .</b>	<b>289</b>
	Table 31: Capabilities of 10-Gigabit Ethernet LAN/WAN PICs . . . . .	291
	Table 32: Handling Oversubscription on 10-Gigabit Ethernet LAN/WAN PICs . .	295
<b>Chapter 22</b>	<b>Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength . . . . .</b>	<b>297</b>
	Table 33: Wavelength-to-Frequency Conversion Matrix . . . . .	298
<b>Chapter 26</b>	<b>Configuring Point-to-Point Protocol over Ethernet . . . . .</b>	<b>305</b>
	Table 34: PPPoE Trace Operation Flags . . . . .	336

# About This Guide

This preface provides the following guidelines for using the *Junos<sup>®</sup> OS Ethernet Interfaces Configuration Guide*:

- JUNOS Documentation and Release Notes on page xxix
- Objectives on page xxx
- Audience on page xxx
- Supported Routing Platforms on page xxx
- Using the Indexes on page xxxi
- Using the Examples in This Manual on page xxxi
- Documentation Conventions on page xxxii
- Documentation Feedback on page xxxiv
- Requesting Technical Support on page xxxiv

## JUNOS Documentation and Release Notes

---

For a list of related JUNOS documentation, see  
<http://www.juniper.net/techpubs/software/junos/>.

If the information in the latest release notes differs from the information in the documentation, follow the *JUNOS Release Notes*.

To obtain the most current version of all Juniper Networks<sup>®</sup> technical documentation, see the product documentation page on the Juniper Networks website at  
<http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

## Objectives

---

This guide provides an overview of the network interfaces features of the JUNOS Software and describes how to configure these properties on the routing platform.



**NOTE:** For additional information about the Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at <http://www.juniper.net/>.

---

## Audience

---

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M Series, MX Series, T Series, EX Series, or J Series router or switch.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

## Supported Routing Platforms

---

For the features described in this manual, the JUNOS Software currently supports the following routing platforms:

- J Series
- M Series

- MX Series
- T Series

## Using the Indexes

---

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines*, refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
```

```
        address 10.0.0.1/24;
    }
}
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the [Junos OS CLI User Guide](#).

---

## Documentation Conventions

Table 1 on page xxxiii defines notice icons used in this guide.



Table 1: Notice Icons




Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xxxiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  <code>user@host&gt; configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host&gt; show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols <b>ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub &lt;default-metric metric&gt;;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <i>(string1   string2   string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identify a level in the configuration hierarchy.	<b>[edit]</b> <b>routing-options {</b> <b>static {</b> <b>route default {</b> <b>nexthop address;</b> <b>retain;</b> <b>}</b> <b>}</b> <b>}</b>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>J-Web GUI Conventions</b>		
<b>Bold text like this</b>	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>



## PART 1

# Ethernet Interfaces Configuration Statements Overview

- Ethernet Interfaces Configuration Statements and Hierarchy on page 3



## CHAPTER 1

# Ethernet Interfaces Configuration Statements and Hierarchy

The following interfaces hierarchy listings show the complete configuration statement hierarchy for the indicated hierarchy levels, listing all possible configuration statements within the indicated hierarchy levels, and showing their level in the configuration hierarchy. When you are configuring the Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

This section contains the following topics:

- [edit interfaces] Hierarchy Level on page 3
- [edit logical-systems] Hierarchy Level on page 19
- [edit protocols connections] Hierarchy Level on page 23
- [edit protocols dot1x] Hierarchy Level on page 24
- [edit protocols iccp] Hierarchy Level on page 24
- [edit protocols lacp] Hierarchy Level on page 24
- [edit protocols oam] Hierarchy Level on page 24
- [edit protocols ppp] Hierarchy Level on page 26
- [edit protocols pppoe] Hierarchy Level on page 26
- [edit protocols protection-group] Hierarchy Level on page 27
- [edit protocols vrrp] Hierarchy Level on page 27

## [edit interfaces] Hierarchy Level

---

The statements at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level can also be configured at the **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.



**NOTE:** The accounting-profile statement is an exception to this rule. The accounting-profile statement can be configured at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level, but it cannot be configured at the **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

```
interfaces {
  traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable |
      no-world-readable> ;
    flag flag <disable>;
  }
  interface-name {
    accounting-profile name;
    aggregated-ether-options {
      (flow-control | no-flow-control);
      lacp {
        (active | passive);
        link-protection {
          disable;
          (revertive | non-revertive);
          periodic interval;
          system-priority priority;
        }
        link-protection;
        link-speed speed;
        (loopback | no-loopback);
        mc-ae {
          chassis-id chassis-id;
          mc-ae-id mc-ae-id;
          mode (active-active | active-standby);
          redundancy-group group-id;
          status-control (active | standby);
        }
        minimum-links number;
        source-address-filter {
          mac-address;
        }
        (source-filtering | no-source-filtering);
      }
    }
    aggregated-sonet-options {
      link-speed speed | mixed;
      minimum-links number;
    }
    atm-options {
      cell-bundle-size cells;
      ilmi;
      linear-red-profiles profile-name {
        high-plp-max-threshold percent;
        low-plp-max-threshold percent;
        queue-depth cells high-plp-threshold percent low-plp-threshold percent;
      }
      mpls {
        pop-all-labels {
          required-depth number;
        }
      }
      pic-type (atm1 | atm2);
      plp-to-clp;
      promiscuous-mode {
        vpi vpi-identifier;
      }
    }
  }
}
```



```

scheduler-maps map-name {
    forwarding-class class-name {
        epd-threshold cells plp1 cells;
        linear-red-profile profile-name;
        priority (high | low);
        transmit-weight (cells number | percent number);
    }
    vc-cos-mode (alternate | strict);
}
use-null-cw;
vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
        down-count cells;
        up-count cells;
    }
    oam-period (seconds | disable);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
        burst length);
        queue-length number;
    }
}
}
clocking clock-source;
data-input (system | interface interface-name);
dce;
serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    dsr-polarity (negative | positive);
    dte-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
}

```

```
dtr-circuit (balanced | unbalanced);
dtr-polarity (negative | positive);
encoding (nrz | nrzi);
indication-polarity (negative | positive);
line-protocol protocol;
loopback mode;
rts-polarity (negative | positive);
tm-polarity (negative | positive);
transmit-clock invert;
}
description text;
dialer-options {
    pool pool-name <priority priority>;
}
disable;
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback payload;
    start-end-flag (filler | shared);
}
e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
e3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag (filler | shared);
    invert-data;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
    (unframed | no-unframed);
}
encapsulation type;
es-options {
    backup-interface es-fpc/pic/port;
```

```

}
fastether-options {
  802.3ad aex;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  ingress-rate-limit rate;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
flexible-vlan-tagging;
gigether-options {
  802.3ad aex;
  (asynchronous-notification | no-asynchronous-notification);
  (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
    local-interface-offline>;
  auto-reconnect seconds;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  no-auto-mdix;
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ];
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [ values ];
      }
      output-priority-map {
        classifier {
          premium {
            forwarding-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
    }
  }
  policer cos-policer-name {
    aggregate {
      bandwidth-limit bps;

```

```

    burst-size-limit bytes;
}
premium {
    bandwidth-limit bps;
    burst-size-limit bytes;
}
}
}
}
}
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
ima-group-options {
    differential-delay number;
    frame-length (32 | 64 | 128 | 256);
    frame-synchronization {
        alpha number;
        beta number;
        gamma number;
    }
    minimum-links number;
    symmetry (symmetrical-config-and-operation |
        symmetrical-config-asymmetrical-operation);
    test-procedure {
        ima-test-start;
        ima-test-stop;
        interface name;
        pattern number;
        period number;
    }
    transmit-clock (common | independent);
    version (1.0 | 1.1);
}
ima-link-options group-id group-id;
interface-set interface-set-name {
    interface ethernet-interface-name {
        (unit unit-number | vlan-tags-outer vlan-tag);
    }
    interface interface-name {
        (unit unit-number);
    }
}
}
isdn-options {
    bchannel-allocation (ascending | descending);
    calling-number number;
    pool pool-name <priority priority>;
    spid1 spid-string;
    spid2 spid-string;
    static-tei-val value;
    switch-type (att5e | etsi | nil | ntdms100 | ntt);
    t310 seconds;
    tei-option (first-call | power-up);
}
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
lmi {
```

```

lmi-type (ansi | itu);
n391dte number;
n392dce number;
n392dte number;
n393dce number;
n393dte number;
t391dte seconds;
t392dce seconds;
}
lsq-failure-options {
  no-termination-request;
  [ trigger-link-failure interface-name ];
}
mac mac-address;
mlfr-uni-nni-bundle-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  cisco-interoperability send-lip-remove-link-for-link-reject;
  hello-timer milliseconds;
  link-layer-overhead percent;
  lmi-type (ansi | itu);
  minimum-links number;
  mrru bytes;
  n391 number;
  n392 number;
  n393 number;
  red-differential-delay milliseconds;
  t391 seconds;
  t392 seconds;
  yellow-differential-delay milliseconds;
}
modem-options {
  dialin (console | routable);
  init-command-string initialization-command-string;
}
mtu bytes;
multiservice-options {
  (core-dump | no-core-dump);
  (syslog | no-syslog);
}
native-vlan-id number;
no-gratuitous-arp-request;
no-keepalives;
no-partition {
  interface-type type;
}
otn-options {
  fec (efec | gfec | none);
  (laser-enable | no-laser-enable);
  (line-loopback | no-line-loopback);
  pass-thru;
  rate (fixed-stuff-bytes | no-fixed-stuff-bytes | pass-thru);
  transmit-payload-type number;

```

```
trigger (oc-lof | oc-lom | oc-los | oc-wavelength-lock | odu-ais | odu-bbe-th | odu-bdi
| odu-es-th | odu-lck | odu-oci | odu-sd | odu-ses-th | odu-ttim | odu-uas-th |
opu-ptm | otu-ais | otu-bbe-th | otu-bdi | otu-es-th | otu-fec-deg | otu-fec-exe |
otu-iae | otu-sd | otu-ses-th | otu-ttim | otu-uas-th);
tti;
}
optics-options {
wavelength nm;
alarm alarm-name {
(syslog | link-down);
}
warning warning-name {
(syslog | link-down);
}
}
partition partition-number oc-slice oc-slice-range interface-type type;
timeslots time-slot-range;
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
chap {
access-profile name;
default-chap-secret name;
local-name name;
passive;
}
compression {
acfc;
pfc;
}
dynamic-profile profile-name;
no-termination-request;
pap {
access-profile name;
local-name name;
local-password password;
compression;
}
}
receive-bucket {
overflow (discard | tag);
rate percentage;
threshold bytes;
}
redundancy-options {
priority sp-fpc/pic/port;
secondary sp-fpc/pic/port;
hot-standby;
}
satop-options {
payload-size n;
}
schedulers number;
serial-options {
clock-rate rate;
clocking-mode (dce | internal | loop);
```

```

control-polarity (negative | positive);
cts-polarity (negative | positive);
dcd-polarity (negative | positive);
dce-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
dsr-polarity (negative | positive);
dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
dtr-circuit (balanced | unbalanced);
dtr-polarity (negative | positive);
encoding (nrz | nrzi);
indication-polarity (negative | positive);
line-protocol protocol;
loopback mode;
rts-polarity (negative | positive);
tm-polarity (negative | positive);
transmit-clock invert;
}
services-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    session-limit {
        maximum number;
        rate new-sessions-per-second;
    }
    syslog {
        host hostname {
            facility-override facility-name;
            log-prefix prefix-number;
            services priority-level;
        }
    }
}
shdsl-options {
    annex (annex-a | annex-b);
    line-rate line-rate;
    loopback (local | remote);
    snr-margin {

```

```
        current margin;
        snext margin;
    }
}
sonet-options {
    aggregate asx;
    aps {
        advertise-interval milliseconds;
        annex-b;
        authentication-key key;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        preserve-interface;
        protect-circuit group-name;
        request;
        revert-time seconds;
        switching-mode (bidirectional | unidirectional);
        working-circuit group-name;
    }
    bytes {
        c2 value;
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (16 | 32);
    loopback (local | remote);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
    rfc-2615;
    trigger {
        defect ignore;
        hold-time up milliseconds down milliseconds;
    }
    vtmapping (itu-t | klm);
    (z0-increment | no-z0-increment);
}
speed (10m | 100m | 1g | oc3 | oc12 | oc48);
stacked-vlan-tagging;
switch-options {
    switch-port port-number {
        (auto-negotiation | no-auto-negotiation);
        speed (10m | 100m | 1g);
        link-mode (full-duplex | half-duplex);
    }
}
```



```

}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout value;
    byte-encoding (nx56 | nx64);
    crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
    crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
t3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate
        value>;
    fcs (16 | 32);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    (loop-timing | no-loop-timing);
    loopback (local | payload | remote);
    (mac | no-mac);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
unidirectional;
vlan-tagging;
vlan-vci-tagging;
unit logical-unit-number {
    accept-source-mac {
        mac-address mac-address {
            policer {
                input cos-policer-name;
                output cos-policer-name;
            }
        }
    }
}

```

```
    }
  }
}
accounting-profile name;
allow-any-vci;
atm-scheduler-map (map-name | default);
backup-options {
  interface interface-name;
}
bandwidth rate;
cell-bundle-size cells;
clear-dont-fragment-bit;
compression {
  rtp {
    f-max-period number;
    maximum-contexts number <force>;
    queues [ queue-numbers ];
    port {
      minimum port-number;
      maximum port-number;
    }
  }
}
}
compression-device interface-name;
copy-tos-to-outer-ip-header;
demux-destination family;
demux-source family;
demux-options {
  underlying-interface interface-name;
}
description text;
dial-options {
  l2tp-interface-id name;
  (dedicated | shared);
}
dialer-options {
  activation-delay seconds;
  callback;
  callback-wait-period time;
  deactivation-delay seconds;
  dial-string [ dial-string-numbers ];
  idle-timeout seconds;
  incoming-map {
    caller (caller-id | accept-all);
    initial-route-check seconds;
    load-interval seconds;
    load-threshold percent;
    pool pool-name;
    redial-delay time;
    watch-list {
      [ routes ];
    }
  }
}
}
disable;
disable-mlppp-inner-ppp-pfc;
```

```

dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold cells plp1 cells;
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
interleave-fragments;
inverse-arp;
layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
}
link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
    down-count cells;
    up-count cells;
}
oam-period (seconds | disable);
output-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
    chap {
        access-profile name;
        default-chap-secret name;
        local-name name;
        passive;
    }
    compression {

```

```
    acfc;
    pfc;
    pap;
    default-pap-password password;
    local-name name;
    local-password password;
    passive;
  }
  dynamic-profile profile-name;
  lcp-max-conf-req number;
  lcp-restart-timer milliseconds;
  loopback-clear-timer seconds;
  ncp-max-conf-req number;
  ncp-restart-timer milliseconds;
}
pppoe-options {
  access-concentrator name;
  auto-reconnect seconds;
  (client | server);
  service-name name;
  underlying-interface interface-name;
}
proxy-arp;
service-domain (inside | outside);
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
    burst length);
  queue-length number;
}
short-sequence;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
  backup-destination address;
  destination address;
  key number;
  routing-instance {
    destination routing-instance-name;
  }
  source source-address;
  ttl number;
}
vci vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-list [vlan-id vlan-id-vlan-id];
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
vlan-tags-outer tpid.vlan-id inner-list [vlan-id vlan-id-vlan-id];
family family {
  accounting {
    destination-class-usage;
    source-class-usage {
```

```

        direction;
    }
}
access-concentrator name;
address address {
    destination address;
}
bundle ml-fpc/pic/port | ls-fpc/pic/port);
duplicate-protection;
dynamic-profile profile-name;
filter {
    group filter-group-number;
    input filter-name;
    input-list {
        [ filter-names ];
        output filter-name;
    }
    output-list {
        [ filter-names ];
    }
}
}
ipsec-sa sa-name;
keep-address-and-control;
max-sessions number;
mtu bytes;
multicast-only;
negotiate-address;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name;
    mode loose;
}
sampling {
    direction;
}
}
service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
    output {
        service-set service-set-names <service-filter filter-name>;
    }
}
}
service-name-table table-name
targeted-broadcast {

```

```

    forward-and-send-to-re;
    forward-only;
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
unnumbered-address interface-name <destination address destination-profile
    profile-name | preferred-source-address address>;
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    multipoint-destination address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination address {
        epd-threshold cells plp1 cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (seconds | disable);
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained
                rate burst length);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    (vrrp-group | vrrp-inet6-group) group-number {
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-type authentication;
        authentication-key key;
        fast-interval milliseconds;
        (preempt | no-preempt) {
            hold-time seconds;
        }
        priority-number number;
        track {
            priority-cost seconds;
            priority-hold-time interface-name {
                bandwidth-threshold bits-per-second {
                    priority;
                }
                interface priority;
            }
            route ip-address/mask routing-instance instance-name priority-cost cost;
        }
        virtual-address [ addresses ];
    }
}
}
}

```

```

    }
  }

```

## [edit logical-systems] Hierarchy Level

The following lists the statements that can be configured at the **[edit logical-systems]** hierarchy level that are also documented in this manual. For more information about logical systems, see the [Junos OS Routing Protocols Configuration Guide](#).

```

logical-systems logical-system-name {
  interfaces interface-name {
    unit logical-unit-number {
      accept-source-mac {
        mac-address mac-address {
          policer {
            input cos-policer-name;
            output cos-policer-name;
          }
        }
      }
    }
    allow-any-vci;
    atm-scheduler-map (map-name | default);
    bandwidth rate;
    backup-options {
      interface interface-name;
    }
    cell-bundle-size cells;
    clear-dont-fragment-bit;
    compression {
      rtp {
        f-max-period number;
        port {
          minimum port-number;
          maximum port-number;
        }
        queues [ queue-numbers ];
      }
    }
    compression-device interface-name;
    description text;
    dial-options {
      l2tp-interface-id name;
      (dedicated | shared);
    }
    dialer-options {
      activation-delay seconds;
      deactivation-delay seconds;
      dial-string [ dial-string-numbers ];
      idle-timeout seconds;
      initial-route-check seconds;
      load-threshold number;
      pool pool;
      remote-name remote-callers;
      watch-list {
        [ routes ];
      }
    }
  }
}

```

```
    }
  }
  disable;
  dlci dlci-identifier;
  drop-timeout milliseconds;
  dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
  }
  encapsulation type;
  epd-threshold cells plp1 cells;
  fragment-threshold bytes;
  input-vlan-map {
    inner-tag-protocol-id;
    inner-vlan-id;
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  interleave-fragments;
  inverse-arp;
  layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
  }
  link-layer-overhead percent;
  minimum-links number;
  mrru bytes;
  multicast-dlci dlci-identifier;
  multicast-vci vpi-identifier.vci-identifier;
  multilink-max-classes number;
  multipoint;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period (seconds | disable);
  output-vlan-map {
    inner-tag-protocol-id;
    inner-vlan-id;
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  passive-monitor-mode;
  peer-unit unit-number;
  plp-to-clp;
  point-to-point;
  ppp-options {
    chap {
      access-profile name;
      default-chap-secret name;
      local-name name;
      passive;
```



```

}
compression {
    acfc;
    pfc;
}
}
dynamic-profile profile-name;
pap {
    default-pap-password password;
    local-name name;
    local-password password;
    passive;
}
}
proxy-arp;
service-domain (inside | outside);
shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
    burst length);
    queue-length number;
}
short-sequence;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
}
vci vpi-identifier.vci-identifier;
vlan-id number;
vlan-id-list [vlan-id vlan-id-vlan-id]
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
vlan-tags outer tpid.vlan-id inner-list [vlan-id vlan-id-vlan-id]
vpi vpi-identifier;
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            direction;
        }
    }
}
bundle interface-name;
filter {
    group filter-group-number;
    input filter-name;
    input-list {
        [ filter-names ];
    }
}

```

```
    output filter-name;
    output-list {
        [ filter-names ];
    }
}
ipsec-sa sa-name;
keep-address-and-control;
mtu bytes;
multicast-only;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check <fail-filter filter-name> {
    <mode loose>;
}
sampling {
    direction;
}
service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
unnumbered-address interface-name destination address destination-profile
    profile-name;
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    multipoint-destination address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination address {
        epd-threshold cells plp1 cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (seconds | disable);
        shaping {
```

```

        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained
          rate burst length);
        queue-length number;
      }
      vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    (vrrp-group | vrrp-inet6-group) group-number {
      (accept-data | no-accept-data);
      advertise-interval seconds;
      authentication-type authentication;
      authentication-key key;
      fast-interval milliseconds;
      (preempt | no-preempt) {
        hold-time seconds;
      }
      priority-number number;
      track {
        priority-cost seconds;
        priority-hold-time interface-name {
          interface priority;
          bandwidth-threshold bits-per-second {
            priority;
          }
        }
      }
      route ip-address/mask routing-instance instance-name priority-cost cost;
    }
  }
  virtual-address [ addresses ];
}
}
}
}
}

```

## [\[edit protocols connections\] Hierarchy Level](#)

The following statements can also be configured at the **[edit logical-systems *logical-system-name* protocols connections]** hierarchy level.

```

interface-switch connection-name {
  interface interface-name.unit-number;
  interface interface-name.unit-number;
}

```

## [edit protocols dot1x] Hierarchy Level

---

```
dot1x {
  authenticator
    authentication-profile-name access-profile-name;
    interface interface-ids {
      maximum-requests integer;
      retries integer;
      quiet-period seconds;
      transmit-period seconds;
      reauthentication (disable | interval seconds);
      server-timeout seconds;
      supplicant (single);
      supplicant-timeout seconds;
    }
  }
}
```

## [edit protocols iccp] Hierarchy Level

---

```
iccp {
  traceoptions;
  local-ip-address ip address;
  session-establishment-hold-time value;
  authentication-key string;
  peer ip-address {
    local-ip-address ip address;
    session-establishment-hold-time value;
    authentication-key string;
    redundancy-group-id-list redundancy-group-id-list;
    liveness-detection;
  }
}
```

## [edit protocols laccp] Hierarchy Level

---

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <disable>;
}
```

## [edit protocols oam] Hierarchy Level

---

```
ethernet {
  connectivity-fault-management {
    action-profile profile-name {
      default-action {
        interface-down;
      }
    }
  }
  linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
  }
}
```

```

}
maintenance-domain domain-name {
    bridge-domain name;
    routing-instance r1 {
        bridge-domain name;
        instance vpls-instance;
        interface (ge | xe) fpc/pic/port.domain;
        level number;
        maintenance-association name{
            mep identifier {
                direction (up | down)
                interface (ge | xe) fpc/pic/port.domain (working | protect );
                auto-discovery;
                lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
                    rem-err-xcon | xcon);
                priority number;
            }
        }
        mip-half-function (none | default | explicit);
        name-format (character-string | none | dns | mac+2oct);
        short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
        continuity-check {
            hold-interval minutes;
            interval (10m | 10s | 1m | 1s | 100ms);
            loss-threshold number;
        }
        maintenance-association ma-name {
            mip-half-function (none | default | explicit);
            mep mep-id {
                auto-discovery;
                direction (up | down);
                interface interface-name (working | protect);
                priority number;
                remote-mep mep-id {
                    action-profile profile-name;
                    sla-iterator-profile profile-name {
                        data-tlv-size bytes;
                        iteration-count frames;
                        priority priority-value;
                    }
                }
            }
        }
    }
}
performance-monitoring {
    hardware-assisted-timestamping;
    sla-iterator-profiles {
        profile-name {
            disable;
            calculation-weight {
                delay delay-weight;
                delay-variation delay-variation-weight;
            }
            cycle-time milliseconds;
            iteration-period connections;
            measurement-type (loss | statistical-frame-loss | two-way-delay);
        }
    }
}

```

```
    }
  }
}
link-fault-management {
  action-profile profile-name {
    action {
      syslog;
      link-down;
      send-critical-event;
    }
    event {
      link-adjacency-loss;
      link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
      }
      protocol-down;
    }
  }
}
interface interface-name {
  apply-action-profile profile-name;
  event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
  }
  link-discovery (active | passive);
  negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
  }
  pdu-interval interval;
  pdu-threshold threshold-value;
  remote-loopback;
}
}
```

---

### [\[edit protocols ppp\] Hierarchy Level](#)

```
monitor-session (interface-name | all);
traceoptions {
  file filename <files number> <match regular-expression> <size size> <world-readable |
  no-world-readable> ;
  flag flag <disable>;
}
```

---

### [\[edit protocols pppoe\] Hierarchy Level](#)

```
protocols {
  pppoe {
```

```

pado-advertise;
service-name-tables table-name {
  service service-name {
    agent-specifier {
      aci circuit-id-string ari remote-id-string {
        (delay seconds | drop | terminate);
        dynamic-profile profile-name;
        routing-instance routing-instance-name;
        static-interface interface-name;
      }
    }
    (delay seconds | drop | terminate);
    dynamic-profile profile-name;
    max-sessions number;
    routing-instance routing-instance-name;
  }
}
traceoptions {
  file <filename> <files number> <match regular-expression> <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}

```

#### Related Documentation

- Notational Conventions Used in Junos OS Configuration Hierarchies
- [edit protocols] Hierarchy Level

### [edit protocols protection-group] Hierarchy Level

```

ethernet-ring ring-name {
  east-interface {
    control-channel channel-name {
      vlan number;
    }
  }
  guard-interval number;
  node-id mac-address;
  restore-interval number;
  ring-protection-link-owner;
  west-interface {
    control-channel channel-name {
      vlan number;
    }
  }
}

```

### [edit protocols vrrp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  vrrp {  
    failover-delay milliseconds;  
    startup-silent-period seconds;  
    traceoptions {  
      file <filename> <files number> <match regular-expression> <microsecond-stamp>  
        <size maximum-file-size> <world-readable | no-world-readable>;  
      flag flag;  
      no-remote-trace;  
    }  
  }  
}
```

- Related Documentation**
- Notational Conventions Used in Junos OS Configuration Hierarchies
  - [edit protocols] Hierarchy Level



## PART 2

# Configuring Ethernet Interfaces

- Configuring Ethernet Interfaces on page 31
- Configuring 802.1Q VLANs on page 47
- Configuring Aggregated Ethernet Interfaces on page 75
- Stacking and Rewriting Gigabit Ethernet VLAN Tags on page 119
- Configuring Layer 2 Bridging Interfaces on page 141
- Configuring TCC and Layer 2.5 Switching on page 143
- Configuring Static ARP Table Entries on page 147
- Configuring Unrestricted Proxy ARP on page 149
- Configuring MAC Address Validation on Static Ethernet Interfaces on page 153
- Enabling Passive Monitoring on Ethernet Interfaces on page 155
- Configuring IEEE 802.1ag OAM Connectivity-Fault Management on page 159
- Configuring ITU-T Y.1731 Ethernet Service OAM on page 201
- Configuring IEEE 802.1x Port-Based Network Access Control on page 249
- Configuring IEEE 802.3ah OAM Link-Fault Management on page 253
- Configuring VRRP and VRRP for IPv6 on page 261
- Configuring Gigabit Ethernet Accounting and Policing on page 263
- Configuring Gigabit Ethernet Autonegotiation on page 277
- Configuring Gigabit Ethernet OTN Options on page 283
- Configuring the Management Ethernet Interface on page 285
- Configuring 10-Gigabit Ethernet LAN/WAN PICs on page 289
- Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength on page 297
- Configuring 10-Gigabit Ethernet Framing on page 299
- Configuring 10-Gigabit Ethernet Notification of Link Down Alarm on page 301
- Configuring 10-Gigabit Ethernet Notification of Link Down for Optics Alarms on page 303
- Configuring Point-to-Point Protocol over Ethernet on page 305
- Configuring Ethernet Ring Protection Switching on page 339
- Example Ethernet Configurations on page 353



## CHAPTER 2

# Configuring Ethernet Interfaces

You can configure the following properties specific to aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces:

- Ethernet Interfaces Overview on page 31
- Configuring Ethernet Physical Interface Properties on page 32
- Configuring J Series Services Router Switching Interfaces on page 36
- MX Series Router Interface Identifiers on page 37
- Enabling Ethernet MAC Address Filtering on page 38
- Configuring Ethernet Loopback Capability on page 40
- Configuring Flow Control on page 41
- Ignoring Layer 3 Incomplete Errors on page 41
- Configuring the Link Characteristics on Ethernet Interfaces on page 41
- Configuring Gratuitous ARP on page 42
- Adjusting the ARP Aging Timer on page 43
- Configuring the Interface Speed on Ethernet Interfaces on page 44
- Configuring the Ingress Rate Limit on page 44
- Configuring Multicast Statistics Collection on Ethernet Interfaces on page 45
- Configuring Weighted Random Early Detection on page 45

## Ethernet Interfaces Overview

---

Ethernet was developed in the early 1970s at the Xerox Palo Alto Research Center (PARC) as a data-link control layer protocol for interconnecting computers. It was first widely used at 10 megabits per second (Mbps) over coaxial cables and later over unshielded twisted pairs using 10Base-T. More recently, 100Base-TX (Fast Ethernet, 100 Mbps), Gigabit Ethernet (1 gigabit per second [Gbps]), 10-Gigabit Ethernet (10 Gbps), and 100-Gigabit Ethernet (100 Gbps) have become available.

Juniper Networks routers support the following types of Ethernet interfaces:

- Fast Ethernet
- Tri-Rate Ethernet copper

- Gigabit Ethernet
- Gigabit Ethernet intelligent queuing (IQ)
- Gigabit Ethernet IQ2 and IQ2-E
- 10-Gigabit Ethernet IQ2 and IQ2-E
- 10-Gigabit Ethernet
- 10-Gigabit Ethernet dense wavelength-division multiplexing (DWDM)
- 100-Gigabit Ethernet
- Management Ethernet interface, which is an out-of-band management interface within the router
- Internal Ethernet interface, which connects the Routing Engine to the packet forwarding components
- Aggregated Ethernet interface, a logical linkage of Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet physical connections

---

## Configuring Ethernet Physical Interface Properties

To configure Fast Ethernet-specific physical interface properties, include the **fastether-options** statement at the **[edit interfaces fe-*fpc/pic/port*]** hierarchy level:

```
[edit interfaces fe-fpc/pic/port]  
link-mode (full-duplex | half-duplex);  
speed (10m | 100m);  
vlan-tagging;  
fastether-options {  
    802.3ad aex (primary | backup);  
    (flow-control | no-flow-control);  
    ignore-l3-incompletes;  
    ingress-rate-limit rate;  
    (loopback | no-loopback);  
    source-address-filter {  
        mac-address;  
    }  
    (source-filtering | no-source-filtering);  
}
```



**NOTE:** The speed statement applies to the management Ethernet interface (fxp0 or em0), the Fast Ethernet 12-port and 48-port Physical Interface Card (PIC) interfaces, the J Series Gigabit Ethernet uPIM interfaces and the MX Series Tri-Rate Ethernet copper interfaces. The Fast Ethernet, fxp0, and em0 interfaces can be configured for 10 Mbps or 100 Mbps (10m | 100m). The J Series Gigabit Ethernet uPIM interfaces and the MX Series Tri-Rate Ethernet copper interfaces can be configured for 10 Mbps, 100 Mbps, or 1 Gbps (10m | 100m | 1g). The 4-port and 8-port Fast Ethernet PICs support a speed of 100 Mbps only.

MX Series routers support Gigabit Ethernet automatic line sensing of MDI (Media Dependent Interface) and MDIX (Media Dependent Interface with Crossover) port connections. MDI is the Ethernet port connection typically used on network interface cards (NIC). MDIX is the standard Ethernet port wiring for hubs and switches. This feature allows MX Series routers to automatically detect MDI and MDIX connections and configure the router port accordingly. You can disable this feature by using the `no-auto-mdix` statement at the `[edit interfaces ge-fpc/pic/port]` hierarchy level.



**NOTE:** Junos OS supports Ethernet host addresses with no subnets. This enables you to configure an Ethernet interface as a host address (that is, with a network mask of /32), without requiring a subnet. Such interfaces can serve as OSPF point-to-point interfaces, and MPLS is also supported.

To configure physical interface properties specific to Gigabit Ethernet and 10-Gigabit Ethernet, include the `gigether-options` statement at the `[edit interfaces ge-fpc/pic/port]` or `[edit interfaces xe-fpc/pic/port]` hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
gigether-options {
  802.3ad aex (primary | backup);
  auto-negotiation | no-auto-negotiation remote-fault <local-interface-online |
    local-interface-offline>;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  no-auto-mdix;
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```

Additionally, for 10-Gigabit Ethernet DWDM-specific physical interface properties, include the `optics-options` statement at the `[edit interfaces ge-fpc/pic/port]` hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
optics-options {
  wavelength nm;
```

```
}
```

To configure Gigabit Ethernet IQ-specific physical interface properties, include the **gigether-options** statement at the **[edit interfaces ge-fpc/pic/port]** hierarchy level. These statements are supported on 10-Gigabit Ethernet IQ2 and IQ2-E PIC. Some of these statements are also supported on Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router). For more information, see “Example: Configuring Gigabit Ethernet Interfaces” on page 353.

```
[edit interfaces ge-fpc/pic/port]
flexible-vlan-tagging;
gigether-options {
  802.3ad aex (primary | backup);
  auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
    local-interface-offline>;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [tpids];
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [values];
      }
      output-priority-map {
        classifier {
          premium {
            forwarding-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
    }
    policer cos-policer-name {
      aggregate {
        bandwidth-limit bps;
        burst-size-limit bytes;
      }
      premium {
        bandwidth-limit bps;
        burst-size-limit bytes;
      }
    }
  }
  native-vlan-id number;
}
```

To configure 10-Gigabit Ethernet physical interface properties, include the **lan-phy** or **wan-phy** statement at the **[edit interfaces xe-fpc/pic/port framing]** hierarchy level. For more information, see “10-Gigabit Ethernet Framing Overview” on page 299.

```
[edit interfaces]
xe-0/0/0 {
  framing {
    (lan-phy | wan-phy);
  }
}
```

To configure OAM 802.3ah support for Ethernet interfaces, include the **oam** statement at the **[edit protocols]** hierarchy level.

```
oam {
  ethernet {
    link-fault-management {
      interfaces {
        interface-name {
          pdu-interval interval;
          link-discovery (active | passive);
          pdu-threshold count;
        }
      }
    }
  }
}
```

To configure Gigabit Ethernet IQ-specific logical interface properties, include the **input-vlan-map**, **output-vlan-map**, **layer2-policer**, and **vlan-tags** statements:

```
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
output-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
layer2-policer {
  input-policer policer-name;
  input-three-color policer-name;
  output-policer policer-name;
  output-three-color policer-name;
}
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
```

You can include these statements at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

To configure aggregated Ethernet-specific physical interface properties, include the **aggregated-ether-options** statement at the **[edit interfaces aex]** hierarchy level:

```
[edit interfaces aex]
aggregated-ether-options {
  ethernet-switch-profile {
    tag-protocol-id tpid;
  }
  (flow-control | no-flow-control);
  lacp mode {
    periodic interval;
  }
  link-protection;
  link-speed speed;
  (loopback | no-loopback);
  minimum-links number;
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```

---

## Configuring J Series Services Router Switching Interfaces

The J Series routers with multiport Gigabit Ethernet uPIMs supports Ethernet access switching. This functionality provides the ability to switch traffic at Layer 2 in addition to routing traffic at Layer 3.

J Series routers with multiport Gigabit Ethernet uPIMs can be deployed in branch offices as an access or desktop switch with integrated routing capability. The multiport Gigabit Ethernet uPIM provides Ethernet switching, while the Routing Engine provides routing functionality.

Routed traffic is forwarded from any port of the multiport Gigabit Ethernet uPIM to the WAN interface. Switched traffic is forwarded from one port of the multiport Gigabit Ethernet uPIM to another port on the same the multiport Gigabit Ethernet uPIM. Switched traffic is not forwarded from a port on one multiport Gigabit Ethernet uPIM to a port on a different multiport Gigabit Ethernet uPIM. For more information about configuring the multiport Gigabit Ethernet uPIM switching mode, see the [Junos OS System Basics Configuration Guide](#).

In access switching mode, only one physical interface is configured for the entire multiport Gigabit Ethernet uPIM. The single physical interface serves as a Virtual Router Interface (VRI). Configuration of the physical port characteristics is done under the single physical interface.

To configure multiport Gigabit Ethernet uPIM Ethernet port properties, include the **switch-port** statement at the **[edit interfaces ge-pim/0/0]** hierarchy level:

```
[edit interfaces ge-pim/0/0]
switch-options {
  switch-port port-number {
    (auto-negotiation | no-auto-negotiation);
  }
}
```



```

    speed 1g;
    link-mode (full-duplex | half-duplex);
  }
}

```

Access switching mode is supported on the 6-port, 8-port, and 16-port Gigabit Ethernet uPIMs.

The multiport Gigabit Ethernet uPIMs are supported on the J2320, J2350, J4350, and J6350 Services Routers.

The 6-port and 8-port multiport Gigabit Ethernet uPIM occupies a single slot and can be installed in any slot. Because the 16-port Gigabit Ethernet uPIM is two slots high, you cannot install a 16-port uPIM in the top slots (slots 1 and 4). Ports are numbered 0 through 5 on the 6-port Gigabit Ethernet uPIM, 0 through 7 on the 8-port Gigabit Ethernet uPIM, and 0 through 15 on the 16-port Gigabit Ethernet uPIM.

### Example: Configuring J Series Services Router Switching Interfaces

Configure a single physical interface for the uPIM and set the port parameters for port 0 and port 1:

```

[edit interfaces]
ge-2/0/0 {
  switch-options {
    switch-port 0 {
      no-auto-negotiation;
      speed 1g;
      link-mode full-duplex;
    }
    switch-port 1 {
      no-auto-negotiation;
      speed 10m;
      link-mode half-duplex;
    }
  }
}

```

### MX Series Router Interface Identifiers

Juniper Networks MX Series 3D Universal Edge Routers support several types of line cards, including Dense Port Concentrators (DPCs), Flexible Port Concentrators (FPCs) with associated Physical Interface Cards (PICs), Trio Modular Port Concentrators (MPCs) with associated Modular Interface Cards (MICs), or MICs. FPCs are populated with PICs for various interface types. DPCs and MPCs with associated MICs, and MICs support a variety of port configurations and combine the functions of FPCs and the PICs. The configuration syntax for each type of line card is the same: *type-fpc/pic/port*.

Ports are numbered from 0 through 9 for Gigabit Ethernet and Tri-Rate Ethernet copper interfaces. Port numbers are always 0 for 10-Gigabit Ethernet interfaces.



**NOTE:** In certain displays, the MX Series routers identify the Packet Forwarding Engine (PFE) rather than the PIC number. PFE 0 corresponds to PIC 0, PFE 1 corresponds to PIC 2, PFE 2 corresponds to PIC 1, and PFE 3 corresponds to PIC 3.

---

## Enabling Ethernet MAC Address Filtering

---

By default, source address filtering is disabled. On aggregated Ethernet interfaces, Fast Ethernet, Gigabit Ethernet, Gigabit Ethernet IQ, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can enable source address filtering, which blocks all incoming packets to an interface.

---



**NOTE:** Source address filtering is not supported on J Series Services Routers.

---

To enable the filtering, include the **source-filtering** statement:

**source-filtering;**

To explicitly disable filtering, include the **no-source-filtering** statement:

**no-source-filtering;**

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* aggregated-ether-options]
  - [edit interfaces *interface-name* fastether-options]
  - [edit interfaces *interface-name* gigether-options]
- 



**NOTE:** When you integrate a standalone T640 router into a routing matrix, the PIC media access control (MAC) addresses for the integrated T640 router are derived from a pool of MAC addresses maintained by the TX Matrix router. For each MAC address you specify in the configuration of a formerly standalone T640 router, you must specify the same MAC address in the configuration of the TX Matrix router.

Similarly, when you integrate a standalone T1600 router into a routing matrix, the PIC MAC addresses for the integrated T1600 router are derived from a pool of MAC addresses maintained by the TX Matrix Plus router. For each MAC address you specify in the configuration of a formerly standalone T1600 router, you must specify the same MAC address in the configuration of the TX Matrix Plus router.

---

## Filtering Specific MAC Addresses

When source address filtering is enabled, you can configure the interface to receive packets from specific MAC addresses. To do this, specify the MAC addresses in the **source-address-filter** statement:

```
source-address-filter {
  mac-address;
  <additional-mac-address>;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* aggregated-ether-options]
- [edit interfaces *interface-name* fastether-options]
- [edit interfaces *interface-name* gigether-options]

You can specify the MAC address as *nn:nn:nn:nn:nn:nn* or *nnnn.nnnn.nnnn*, where *n* is a hexadecimal number. You can configure up to 64 source addresses. To specify more than one address, include the **source-address-filter** statement multiple times.



**NOTE:** The **source-address-filter** statement is not supported on Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router); instead, include the **accept-source-mac** statement. For more information, see “Configuring MAC Address Filtering” on page 269.

If the remote Ethernet card is changed, the interface cannot receive packets from the new card because it has a different MAC address.

Source address filtering does not work when Link Aggregation Control Protocol (LACP) is enabled. For more information about LACP, see “Configuring Aggregated Ethernet LACP” on page 102.



**NOTE:** On untagged Gigabit Ethernet interfaces, you should not configure the `source-address-filter` statement at the `[edit interfaces ge-fpc/pic/port gigether-options]` hierarchy level and the `accept-source-mac` statement at the `[edit interfaces ge-fpc/pic/port gigether-options unit logical-unit-number]` hierarchy level simultaneously. If these statements are configured for the same interfaces at the same time, an error message is displayed.

On tagged Gigabit Ethernet interfaces, you should not configure the `source-address-filter` statement at the `[edit interfaces [edit interfaces ge-fpc/pic/port gigether-options]` hierarchy level and the `accept-source-mac` statement at the `[edit interfaces ge-fpc/pic/port gigether-options unit logical-unit-number]` hierarchy level with an identical MAC address specified in both filters. If these statements are configured for the same interfaces with an identical MAC address specified, an error message is displayed.

---

## Configuring Ethernet Loopback Capability

---

By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system. To place an interface in loopback mode, include the **loopback** statement:

```
loopback;
```



**NOTE:** If you configure a local loopback on a 1-port 10-Gigabit IQ2 and IQ2-E PIC using the `loopback` statement at the `[edit interfaces interface-name gigether-options]` hierarchy level, the transmit-path stops working, causing the remote end to detect a link down.

To return to the default—that is, to disable loopback mode—delete the **loopback** statement from the configuration:

```
[edit]
user@host# delete interfaces fe-fpc/pic/port fastether-options loopback
```

To explicitly disable loopback mode, include the **no-loopback** statement:

```
no-loopback;
```

You can include the **loopback** and **no-loopback** statements at the following hierarchy levels:

- `[edit interfaces interface-name aggregated-ether-options]`
- `[edit interfaces interface-name ether-options]`
- `[edit interfaces interface-name fastether-options]`
- `[edit interfaces interface-name gigether-options]`

## Configuring Flow Control

---

By default, the router or switch imposes flow control to regulate the amount of traffic sent out on a Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interface. Flow control is not supported on the 4-port Fast Ethernet PIC. This is useful if the remote side of the connection is a Fast Ethernet or Gigabit Ethernet switch.

You can disable flow control if you want the router or switch to permit unrestricted traffic. To disable flow control, include the **no-flow-control** statement:

```
no-flow-control;
```

To explicitly reinstate flow control, include the **flow-control** statement:

```
flow-control;
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* aggregated-ether-options]
- [edit interfaces *interface-name* ether-options]
- [edit interfaces *interface-name* fastether-options]
- [edit interfaces *interface-name* gigether-options]

## Ignoring Layer 3 Incomplete Errors

---

By default, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces count Layer 3 incomplete errors. You can configure the interface to ignore Layer 3 incomplete errors.

To ignore Layer 3 incomplete errors, include the **ignore-l3-incompletes** statement:

```
ignore-l3-incompletes;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* fastether-options]
- [edit interfaces *interface-name* gigether-options]

## Configuring the Link Characteristics on Ethernet Interfaces

---

*Full-duplex* communication means that both ends of the communication can send and receive signals at the same time. *Half-duplex* is also bidirectional communication, but signals can flow in only one direction at a time.

By default, the router's management Ethernet interface, **fxp0** or **em0**, autonegotiates whether to operate in full-duplex or half-duplex mode. J Series Gigabit Ethernet interfaces and Fast Ethernet interfaces, except the J Series ePIM Fast Ethernet interfaces, can operate in either full-duplex or half-duplex mode, and all other interfaces can operate

only in full-duplex mode. For Gigabit Ethernet and 10-Gigabit Ethernet, the link partner must also be set to full duplex.



**NOTE:** For M Series, MX Series, and most T Series routers, the management Ethernet interface is `fxp0`. For TX Matrix Plus routers and T1600 routers configured in a routing matrix, the management Ethernet interface is `em0`.



**NOTE:** Automated scripts that you have developed for standalone T1600 routers (T1600 routers that are not in a routing matrix) might contain references to the `fxp0` management Ethernet interface. Before reusing the scripts on T1600 routers in a routing matrix, edit the command lines that reference the `fxp0` management Ethernet interface so that the commands reference the `em0` management Ethernet interface instead.



**NOTE:** When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled.



**NOTE:** On a J Series ePIM Fast Ethernet interface, if you specify half-duplex (or if full-duplex mode is not autonegotiated), the following message is written to the system log: "Half-duplex mode not supported on this PIC, forcing full-duplex mode."



**NOTE:** When you manually configure Fast Ethernet interfaces on the M Series and T Series routers, link mode and speed must both be configured. If both these values are not configured, the router uses autonegotiation for the link and ignores the user-configured settings.

To explicitly configure an Ethernet interface to operate in either full-duplex or half-duplex mode, include the `link-mode` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]  
link-mode (full-duplex | half-duplex);
```

---

## Configuring Gratuitous ARP

Gratuitous Address Resolution Protocol (ARP) requests provide duplicate IP address detection. A gratuitous ARP request is a broadcast request for a router's own IP address. If a router or switch sends an ARP request for its own IP address and no ARP replies are received, the router- or switch-assigned IP address is not being used by other nodes. If a router or switch sends an ARP request for its own IP address and an ARP reply is received, the router- or switch-assigned IP address is already being used by another node.

By default, the router or switch responds to gratuitous ARP requests. On Ethernet interfaces, you can disable responses to gratuitous ARP requests. To disable responses to gratuitous ARP requests, include the **no-gratuitous-arp-request** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
no-gratuitous-arp-request;
```

To return to the default—that is, to respond to gratuitous ARP requests—delete the **no-gratuitous-arp-request** statement from the configuration:

```
[edit]  
user@host# delete interfaces interface-name no-gratuitous-arp-request
```

Gratuitous ARP replies are reply packets sent to the broadcast MAC address with the target IP address set to be the same as the sender's IP address. When the router or switch receives a gratuitous ARP reply, the router or switch can insert an entry for that reply in the ARP cache.

By default, updating the ARP cache on gratuitous ARP replies is disabled on the router or switch. On Ethernet interfaces, you can enable handling of gratuitous ARP replies on a specific interface by including the **gratuitous-arp-reply** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
gratuitous-arp-reply;
```

To restore the default behavior, include the **no-gratuitous-arp-reply** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
no-gratuitous-arp-reply;
```

---

## Adjusting the ARP Aging Timer

By default, the ARP aging timer is set at 20 minutes. In most network environments, this default value does not cause a problem. However, in environments with many directly attached hosts, such as metro Ethernet, the number of ARP entries to update can be high. In such environments, you might want to increase the amount of time between ARP updates by configuring the ARP aging timer.

To configure the ARP aging timer, include the **aging-timer** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]  
aging-timer minutes;
```

The aging timer range is from 20 through 240 minutes. The timer value you configure takes effect as ARP entries expire. In other words, each subsequent refreshed ARP entry receives the new timer value. The new timer value does not apply to ARP entries that exist at the time you commit the configuration.

For more information about statements you can configure at the **[edit system]** hierarchy level, see the [Junos OS System Basics Configuration Guide](#).

## Configuring the Interface Speed on Ethernet Interfaces

---

For M Series and T Series Fast Ethernet 12-port and 48-port PIC interfaces, the management Ethernet interface (**fxp0** or **em0**), the J Series Gigabit Ethernet uPIM interfaces, and the MX Series Tri-Rate Ethernet copper interfaces, you can explicitly set the interface speed. The Fast Ethernet, **fxp0**, and **em0** interfaces can be configured for 10 Mbps or 100 Mbps (**10m** | **100m**). The J Series Gigabit Ethernet uPIM interfaces and the MX Series Tri-Rate Ethernet copper interfaces can be configured for 10 Mbps, 100 Mbps, or 1 Gbps (**10m** | **100m** | **1g**). MX Series routers, with MX-DPC and Tri-Rate Copper SFPs, support 20x1 Copper to provide backwards compatibility with 100/10BASE-T and 1000BASE-T operation through an Serial Gigabit Media Independent Interface (SGMII) interface.



**NOTE:** On MX Series routers with tri-rate copper SFP interfaces, if the port speed is negotiated to the configured value and the negotiated speed and interface speed do not match, the link will not be brought up.



**NOTE:** When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled.



**NOTE:** Half-duplex mode is not supported on Tri-Rate Ethernet copper interfaces. When you include the **speed** statement, you must include the **link-mode full-duplex** statement at the same hierarchy level.

To explicitly configure the speed, include the **speed** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
speed (10m | 100m | 1g);
```

## Configuring the Ingress Rate Limit

---

On Fast Ethernet 8-port, 12-port, and 48-port PIC interfaces only, you can apply port-based rate limiting to the ingress traffic that arrives at the PIC.

To configure an ingress rate limit on a Fast Ethernet 8-port, 12-port, or 48-port PIC interface, include the **ingress-rate-limit** statement at the **[edit interfaces *interface-name* fastether-options]** hierarchy level:

```
[edit interfaces interface-name fastether-options]  
ingress-rate-limit rate;
```

**rate** can range in value from 1 through 100 Mbps.



## Configuring Multicast Statistics Collection on Ethernet Interfaces

---

T Series and TX Matrix routers support multicast statistics collection on Ethernet interfaces in both ingress and egress directions. The multicast statistics functionality can be configured on a physical interface thus enabling multicast accounting for all the logical interfaces below the physical interface.

The multicast statistics information is displayed only when the interface is configured with the **multicast-statistics** statement, which is not enabled by default.

Multicast statistics collection requires at least one logical interface is configured with family inet and/or inet6; otherwise, the commit for **multicast-statistics** will fail.

The multicast in/out statistics can be obtained via interfaces statistics query through CLI and via MIB objects through SNMP query.

To configure multicast statistics:

1. Include the **multicast-statistics** statement at the **[edit interfaces interface-name]** hierarchy level.

An example of a multicast statistics configuration for a Ethernet interface follows:

```
[edit interfaces]
  ge-fpc/pic/port {
    multicast-statistics;
  }
```

To display multicast statistics, use the **show interfaces *interface-name* statistics detail** command.

- Related Documentation**
- [multicast-statistics](#)
  - [Configuring Multicast Statistics Collection on Aggregated Ethernet Interfaces](#) on page 111

## Configuring Weighted Random Early Detection

---

On M7i, M10i, M40e, M320, M120, and T Series routers, the Ethernet IQ2 and IQ2-E PIC families extend CoS functionality by supporting network congestion avoidance with weighted random early detection (WRED).

- Related Documentation**
- For information on configuring WRED, see the [Junos OS Class of Service Configuration Guide](#).



## CHAPTER 3

# Configuring 802.1Q VLANs

- 802.1Q VLANs Overview on page 47
- Configuring Dynamic 802.1Q VLANs on page 48
- 802.1Q VLAN IDs and Ethernet Interface Types on page 49
- Enabling VLAN Tagging on page 50
- Binding VLAN IDs to Logical Interfaces on page 53
- Associating VLAN IDs to VLAN Demux Interfaces on page 58
- Configuring VLAN Encapsulation on page 59
- Configuring Extended VLAN Encapsulation on page 60
- Guidelines for Configuring VLAN ID List-Bundled Logical Interfaces That Connect CCCs on page 62
- Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface on page 63
- Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface on page 65
- Example: Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface on page 66
- Example: Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface on page 68
- Configuring a Logical Interface for Access Mode on page 69
- Configuring a Logical Interface for Trunk Mode on page 70
- Configuring the VLAN ID List for a Trunk Interface on page 70
- Configuring a Trunk Interface on a Bridge Network on page 71

## 802.1Q VLANs Overview

---

For Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet interfaces supporting VPLS, the Junos OS supports a subset of the IEEE 802.1Q standard for channelizing an Ethernet interface into multiple logical interfaces, allowing many hosts to be connected to the same Gigabit Ethernet switch, but preventing them from being in the same routing or bridging domain.

### Related Documentation

- Configuring Dynamic 802.1Q VLANs on page 48
- 802.1Q VLAN IDs and Ethernet Interface Types on page 49

- Enabling VLAN Tagging on page 50
- Binding VLAN IDs to Logical Interfaces on page 53
- Configuring VLAN Encapsulation on page 59
- Configuring Extended VLAN Encapsulation on page 60
- Guidelines for Configuring VLAN ID List-Bundled Logical Interfaces That Connect CCCs on page 62
- Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface on page 63
- Configuring a VLAN-Bundled Logical Interface on page 64
- Specifying the Interface Over Which VPN Traffic Travels to the CE Router on page 64
- Specifying the Interface to Handle Traffic for a CCC on page 64
- Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface on page 65
- Configuring a VLAN-Bundled Logical Interface on page 65
- Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit on page 66
- Example: Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface on page 66
- Example: Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface on page 68
- Configuring a Logical Interface for Access Mode on page 69
- Configuring a Logical Interface for Trunk Mode on page 70
- Configuring the VLAN ID List for a Trunk Interface on page 70
- Configuring a Trunk Interface on a Bridge Network on page 71

---

## Configuring Dynamic 802.1Q VLANs

---

You can configure the router to dynamically create VLANs when a client accesses an interface and requests a VLAN ID that does not yet exist. When a client accesses a VLAN interface, the router instantiates a VLAN dynamic profile that you have associated with the interface. Using the settings in the dynamic profile, the router extracts information about the client from the incoming packet (for example, the interface and unit values), saves this information in the routing table, and creates a VLAN or stacked VLAN ID for the client from a range of VLAN IDs that you configure for the interface.

Dynamically configuring VLANs or stacked VLANs requires the following general steps:

1. Configure a dynamic profile for dynamic VLAN or dynamic stacked VLAN creation.
2. Associate the VLAN or stacked VLAN dynamic profile with the interface.
3. Specify the Ethernet packet type that the VLAN dynamic profile accepts.
4. Define VLAN ranges for use by the dynamic profile when creating VLAN IDs.

For procedures on how to configure dynamic VLANs and dynamic stacked VLANs for client access, see the [Junos OS Subscriber Access Configuration Guide](#).

**Related Documentation**

- 802.1Q VLANs Overview on page 47

## 802.1Q VLAN IDs and Ethernet Interface Types

You can partition the router into up to 4095 different VLANs—depending on the router model and the physical interface types—by associating logical interfaces with specific VLAN IDs.

VLAN ID 0 is reserved for tagging the priority of frames. VLAN IDs 1 through 511 are reserved for normal VLANs. VLAN IDs 512 and above are reserved for VLAN circuit cross-connect (CCCs).

For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can configure flexible Ethernet services encapsulation on the physical interface. With flexible Ethernet services encapsulation, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

The maximum number of user-configurable VLANs is 15 on each port of the Dense-FE PIC (8-port/12-port/48-port).

Table 3 on page 49 lists VLAN ID range by interface type.

**Table 3: VLAN ID Range by Interface Type**

Interface Type	VLAN ID Range
Aggregated Ethernet for Fast Ethernet	1 through 1023
Aggregate Ethernet for Gigabit Ethernet	1 through 4094
4-port, 8-port, and 12-port Fast Ethernet	1 through 1023
48-port Fast Ethernet	1 through 4094
Tri-Rate Ethernet copper	1 through 4094
Gigabit Ethernet	1 through 4094
Gigabit Ethernet IQ	1 through 4094
10-Gigabit Ethernet	1 through 4094
Management and internal Ethernet interfaces	1 through 1023



**NOTE:** For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the built-in Gigabit Ethernet port on the M7i router), VLAN IDs on a single interface can differ from each other.

Because IS-IS has an 8-bit limit for broadcast multiaccess media, you cannot set up more than 255 adjacencies over Gigabit Ethernet using VLAN tagging. For more information, see the [Junos OS Routing Protocols Configuration Guide](#).

**Related Documentation**

- 802.1Q VLANs Overview on page 47

---

## Enabling VLAN Tagging

You can configure the router to receive and forward single-tag frames, dual-tag frames, or a mixture of single-tag and dual-tag frames. For more information, see the following sections:

- Configuring Single-Tag Framing on page 50
- Configuring Dual Tagging on page 50
- Configuring Mixed Tagging on page 51
- Configuring Mixed Tagging Support for Untagged Packets on page 52
- Example: Configuring Mixed Tagging on page 52
- Example: Configuring Mixed Tagging to Support Untagged Packets on page 52



**NOTE:** If you configure VLAN tagging on Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces on M320, M120, and T Series routers, the Junos OS creates an internal logical interface that reserves 50 Kbps of bandwidth from Gigabit Ethernet IQ interfaces and 2 Mbps of bandwidth from Gigabit Ethernet IQ2 and IQ2-E interfaces. As a result, the effective available bandwidth for these interface types is now 999.5 Mbps and 998 Mbps, respectively.

---

## Configuring Single-Tag Framing

To configure the router to receive and forward single-tag frames with 802.1Q VLAN tags, include the **vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
vlan-tagging;
```

## Configuring Dual Tagging

To configure the routing platform to receive and forward dual-tag frames with 802.1Q VLAN tags, include the **stacked-vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
stacked-vlan-tagging;
```

## Configuring Mixed Tagging

Mixed tagging is supported for Gigabit Ethernet interfaces on Gigabit Ethernet IQ2 and IQ2-E, and IQ or IQE PICs on M Series and T Series routers, for all MX Series router Gigabit and 10-Gigabit Ethernet interfaces, and for aggregated Ethernet interfaces with member links in IQ2 and IQ2-E PICs or in MX Series DPCs. Mixed tagging lets you configure two logical interfaces on the same Ethernet port, one with single-tag framing and one with dual-tag framing.



**NOTE:** Mixed tagging is not supported on Fast Ethernet interfaces or on J Series Services Routers.

To configure mixed tagging, include the **flexible-vlan-tagging** statement at the **[edit interfaces ge-fpc/pic/port]** hierarchy level. You must also include the **vlan-tags** statement with **inner** and **outer** options or the **vlan-id** statement at the **[edit interfaces ge-fpc/pic/port unit logical-unit-number]** hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
flexible-vlan-tagging;
unit logical-unit-number {
    vlan-id number;
    family family {
        address address;
    }
}
unit logical-unit-number {
    vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
    family family {
        address address;
    }
}
```



**NOTE:** When you configure the physical interface MTU for mixed tagging, you must increase the MTU to 4 bytes more than the MTU value you would configure for a standard VLAN-tagged interface.

For example, if the MTU value is configured to be 1018 on a VLAN-tagged interface, then the MTU value on a flexible VLAN tagged interface must be 1022—4 bytes more. The additional 4 bytes accommodates the future addition of a stacked VLAN tag configuration on the same physical interface.

If the same physical interface MTU value is configured on both the VLAN and flexible VLAN-tag routers, the L2 circuit configuration does not come up and a MTU mismatch is logged. However, normal traffic flow is unaffected.

For encapsulation type **flexible-ethernet-services**, all VLAN IDs are valid. See “Configuring VLAN Encapsulation” on page 59.

## Configuring Mixed Tagging Support for Untagged Packets

For 1-, 4-, and 8-port Gigabit Ethernet IQ2 and IQ2-E PICs, for 1-port 10-Gigabit Ethernet IQ2 and IQ2-E PICs, for all MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces configured for 802.1Q flexible VLAN tagging, and for aggregated Ethernet interfaces on IQ2 and IQ2-E PICs or MX Series DPCs, you can configure mixed tagging support for untagged packets on a port. Untagged packets are accepted on the same mixed VLAN-tagged port. To accept untagged packets, include the **native-vlan-id** statement and the **flexible-vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
flexible-vlan-tagging;
native-vlan-id number;
```

The logical interface on which untagged packets are to be received must be configured with the same native VLAN ID as that configured on the physical interface. To configure the logical interface, include the **vlan-id** statement (matching the **native-vlan-id** statement on the physical interface) at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

### Example: Configuring Mixed Tagging

The following example configures mixed tagging. Dual-tag and single-tag logical interfaces are under the same physical interface:

```
[edit interfaces ge-3/0/1]
flexible-vlan-tagging;
unit 0 {
  vlan-id 232;
  family inet {
    address 10.66.1.2/30;
  }
}
unit 1 {
  vlan-tags outer 0x8100.222 inner 0x8100.221;
  family inet {
    address 10.66.1.2/30;
  }
}
```

For information about binding VLAN IDs to logical interfaces, see “Binding VLAN IDs to Logical Interfaces” on page 53. For information about configuring dual VLAN tags using the **vlan-tag** statement, see “Stacking a VLAN Tag” on page 127.

### Example: Configuring Mixed Tagging to Support Untagged Packets

The following example configures untagged packets to be mapped to logical unit number 0:

```
[edit interfaces ge-0/2/0]
flexible-vlan-tagging;
native-vlan-id 232;
unit 0 {
```



```

    vlan-id 232;
    family inet {
        address 10.66.1.2/30;
    }
}
unit 1 {
    vlan-tags outer 0x8100.222 inner 0x8100.221;
    family inet {
        address 10.66.1.2/30;
    }
}
```

**Related Documentation**

- 802.1Q VLANs Overview on page 47

### Binding VLAN IDs to Logical Interfaces

The following sections describe how to configure logical interfaces to receive and forward VLAN-tagged frames:

- Binding VLAN IDs to Logical Interfaces Overview on page 53
- Binding a VLAN ID to a Logical Interface on page 54
- Binding a Range of VLAN IDs to a Logical Interface on page 54
- Binding a List of VLAN IDs to a Logical Interface on page 56

### Binding VLAN IDs to Logical Interfaces Overview

To configure a logical interface to receive and forward VLAN-tagged frames, you must bind a VLAN ID, a range of VLAN IDs, or a list of VLAN IDs to the logical interface. Table 4 on page 53 lists the configuration statements you use to bind VLAN IDs to logical interfaces, organized by scope of the VLAN IDs used to match incoming packets:

Table 4: Configuration Statements Used to Bind VLAN IDs to Logical Interfaces

Scope of VLAN ID Matching	Type of VLAN Framing Supported on the Logical Interface	
	Single-Tag Framing	Dual-Tag Framing
VLAN ID	<code>vlan-id <i>vlan-id</i>;</code>	<code>vlan-tags outer <i>tpid</i>.&lt;<i>vlan-id</i>&gt; inner <i>tpid</i><i>vlan-id</i>;</code>
VLAN ID Range	<code>vlan-id-range <i>vlan-id-vlan-id</i>;</code>	<code>vlan-tags outer <i>tpid.vlan-id</i> inner-range <i>tpid.vlan-id-vlan-id</i>;</code>
VLAN ID List	<code>vlan-id-list [<i>vlan-id</i> <i>vlan-id-vlan-id</i>];</code>	<code>vlan-tags outer &lt;<i>tpid</i>.&gt;<i>vlan-id</i> inner-list [<i>vlan-id</i> <i>vlan-id-vlan-id</i>];</code>

You can include all of the statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]



**NOTE:** The inner-list option of the `vlan-tags` statement does not support Tag Protocol ID (TPID) values.

---

## Binding a VLAN ID to a Logical Interface

A logical interface that you have associated (bound) to a particular VLAN ID will receive and forward incoming frames that contain a matching VLAN ID.

### Binding a VLAN ID to a Single-Tag Logical Interface

---

To bind a VLAN ID to a single-tag logical interface, include the `vlan-id` statement:

```
vlan-id vlan-id;
```

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support single-tag logical interfaces, include the `vlan-tagging` statement at the [edit interfaces *ethernet-interface-name*] hierarchy level. To support mixed tagging, include the `flexible-vlan-tagging` statement instead.

### Binding a VLAN ID to a Dual-Tag Logical Interface

---

To bind a VLAN ID to a dual-tag logical interface, include the `vlan-tags` statement:

```
vlan-tags inner <tpid.>vlan-id outer <tpid.>vlan-id;
```

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support dual-tag logical interfaces, include the `stacked-vlan-tagging` statement at the [edit interfaces *ethernet-interface-name*] hierarchy level. To support mixed tagging, include the `flexible-vlan-tagging` statement instead.

## Binding a Range of VLAN IDs to a Logical Interface

A VLAN range can be used by service providers to interconnect multiple VLANs belonging to a particular customer over multiple sites. Using a VLAN ID range conserves switch resources and simplifies configuration.

### Binding a Range of VLAN IDs to a Single-Tag Logical Interface

---

To bind a range of VLAN IDs to a single-tag logical interface, include the `vlan-id-range` statement:

```
vlan-id-range vlan-id-vlan-id;
```

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support single-tag logical interfaces, include the **vlan-tagging** statement at the [edit interfaces *ethernet-interface-name*] hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

### Binding a Range of VLAN IDs to a Dual-Tag Logical Interface

To bind a range of VLAN IDs to a dual-tag logical interface, include the **vlan-tags** statement. Use the **inner-list** option to specify the VLAN IDs as an inclusive range by separating the starting VLAN ID and ending VLAN ID with a hyphen.

```
vlan-tags inner-list [ vlan-id vlan-id-vlan-id ] outer <tpid.>vlan-id;
```

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support dual-tag logical interfaces, include the **stacked-vlan-tagging** statement at the [edit interfaces *ethernet-interface-name*] hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

### Example: Binding Ranges VLAN IDs to Logical Interfaces

The following example configures two different ranges of VLAN IDs on two different logical ports:

```
[edit interfaces]
ge-3/0/0 {
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 500-600;
  }
}
ge-3/0/1 {
  flexible-vlan-tagging;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 200-300;
  }
  unit 1 {
    encapsulation vlan-bridge;
    vlan-tags outer 1000 inner-range 100-200;
  }
}
```

## Binding a List of VLAN IDs to a Logical Interface

In Junos OS Release 9.5 and later, on MX Series routers you can bind a list of VLAN IDs to a single logical interface, eliminating the need to configure a separate logical interface for every VLAN or VLAN range. A logical interface that accepts packets tagged with any VLAN ID specified in a VLAN ID list is called a *VLAN-bundled* logical interface.

You can use VLAN-bundled logical interfaces to configure circuit cross-connects between Layer 2 VPN routing instances or Layer 2 circuits. Using VLAN-bundled logical interfaces simplifies configuration and reduces use of system resources such as logical interfaces, next hops, and circuits.

As an alternative to configuring multiple logical interfaces (one for each VLAN ID and one for each range of VLAN IDs), you can configure a single VLAN-bundled logical interface based on a list of VLAN IDs.

---

### Binding a List of VLAN IDs to a Single-Tag Logical Interface

To bind a list of VLAN IDs to a single-tag logical interface, include the **vlan-id-list** statement. Specify the VLAN IDs in the list individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both.

```
vlan-id-list [ vlan-id vlan-id-vlan-id ];
```

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support single-tag logical interfaces, include the **vlan-tagging** statement at the [edit interfaces *ethernet-interface-name*] hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

---

### Binding a List of VLAN IDs to a Dual-Tag Logical Interface

To bind a list of VLAN IDs to a dual-tag logical interface, include the **vlan-tags** statement. Use the **inner-list** option to specify the VLAN IDs individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both:

```
vlan-tags inner-list [ vlan-id vlan-id-vlan-id ] outer <tpid>vlan-id;
```



**NOTE:** The inner-list option of the **vlan-tags** statement does not support Tag Protocol ID (TPID) values.

---

You can include the statement at the following hierarchy levels:

- [edit interfaces *ethernet-interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *ethernet-interface-name* unit *logical-unit-number*]

To configure an Ethernet interface to support dual-tag logical interfaces, include the **stacked-vlan-tagging** statement at the **[edit interfaces *ethernet-interface-name*]** hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

### Example: Binding Lists of VLAN IDs to Logical Interfaces

The following example configures two different lists of VLAN IDs on two different logical ports:

```
[edit interfaces]
ge-1/1/0 {
  vlan-tagging; # Only for single-tagging
  encapsulation flexible-ethernet-services;
  unit 10 {
    encapsulation vlan-ccc;
    vlan-id-list [20 30–40 45];
  }
}
ge-1/1/1 {
  flexible-vlan-tagging; # Only for mixed tagging
  encapsulation flexible-ethernet-services;
  unit 10 {
    encapsulation vlan-ccc;
    vlan-id-list [1 10 20 30–40];
  }
  unit 20 {
    encapsulation vlan-ccc;
    vlan-tags outer 200 inner-list [50–60 80 90–100];
  }
}
```

In the example configuration above, **ge-1/1/0** supports single-tag logical interfaces, and **ge-1/1/1** supports mixed tagging. The single-tag logical interfaces **ge-1/1/0.10** and **ge-1/1/1.20** each bundle lists of VLAN IDs. The dual-tag logical interface **ge-1/1/1.20** bundles lists of inner VLAN IDs.



**TIP:** You can group a range of identical interfaces into an interface range and then apply a common configuration to that interface range. For example, in the above example configuration, both interfaces **ge-1/1/0** and **ge-1/1/1** have the same physical encapsulation type of **flexible-ethernet-services**. Thus you can define an interface range with the interfaces **ge-1/1/0** and **ge-1/1/1** as its members and apply the encapsulation type **flexible-ethernet-services** to that defined interface range. For more information about interface ranges, see [Configuring Interface Ranges](#).

#### Related Documentation

- 802.1Q VLANs Overview on page 47
- Configuring Interface Ranges

## Associating VLAN IDs to VLAN Demux Interfaces

The following sections describe how to configure VLAN demux interfaces to receive and forward VLAN-tagged frames:

- Associating VLAN IDs to VLAN Demux Interfaces Overview on page 58
- Associating a VLAN ID to a VLAN Demux Interface on page 58

### Associating VLAN IDs to VLAN Demux Interfaces Overview

To configure a VLAN demux interface to receive and forward VLAN-tagged frames, you must associate a VLAN ID or dual tagged (stacked) VLAN ID to the interface. Table 5 on page 58 shows the configuration statements you use to associate VLAN IDs to VLAN demux interfaces, depending on the VLAN tag framing you use:

**Table 5: Configuration Statements Used to Associate VLAN IDs to VLAN Demux Interfaces**

	Single-Tag Framing	Dual-Tag Framing
Statement Format	<code>vlan-id <i>vlan-id</i>;</code>	<code>vlan-tags outer <i>tpid</i>.&lt;<i>vlan-id</i>&gt; inner <i>tpid</i><i>vlan-id</i>;</code>

You can include all of the statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]
- [edit interfaces *demux0* unit *logical-unit-number*]

### Associating a VLAN ID to a VLAN Demux Interface

A VLAN demux interface that you have associated to a particular VLAN ID receives and forwards incoming frames that contain a matching VLAN ID. You can associate a VLAN ID to a single-tag logical interface or to a dual-tagged (stacked) logical interface.

1. Associating a VLAN ID to a Single-Tag VLAN Demux Interface on page 58
2. Associating a VLAN ID to a Dual-Tag VLAN Demux Interface on page 58

#### Associating a VLAN ID to a Single-Tag VLAN Demux Interface

To associate a VLAN ID to a single-tag VLAN demux interface, include the **vlan-id** statement at the [edit interfaces *demux0* unit *logical-unit-number*] hierarchy level:

```
vlan-id vlan-id;
```

To configure an interface to support single-tag logical interfaces, you must also include the **vlan-tagging** statement at the [edit interfaces *interface-name*] hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

#### Associating a VLAN ID to a Dual-Tag VLAN Demux Interface

To associate a VLAN ID to a dual-tag VLAN demux interface, include the **vlan-tags** statement at the [edit interfaces *demux0* unit *logical-unit-number*] hierarchy level:

```
vlan-tags inner <tpid.>vlan-id outer <tpid.>vlan-id;
```

To configure an interface to support dual-tag logical interfaces, include the **stacked-vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level. To support mixed tagging, include the **flexible-vlan-tagging** statement instead.

## Configuring VLAN Encapsulation

Gigabit Ethernet IQ, Gigabit Ethernet PICs with small form-factor pluggable optics (SFPs), and MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces with VLAN tagging enabled can use flexible Ethernet services, VLAN CCC, or VLAN virtual private LAN service (VPLS) encapsulation.

Aggregated Ethernet interfaces configured for VPLS can use Ethernet VPLS or VLAN VPLS.

To configure the encapsulation on a Gigabit Ethernet IQ or Gigabit Ethernet physical interface, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level, specifying **flexible-ethernet-services**, **vlan-ccc**, or **vlan-vpls**:

```
[edit interfaces interface-name]  
encapsulation (flexible-ethernet-services | vlan-ccc | vlan-vpls);
```

To configure the encapsulation on an aggregated Ethernet interface, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level, specifying **flexible-ethernet-services**, **ethernet-vpls**, or **vlan-vpls**:

```
[edit interfaces interface-name]  
encapsulation (flexible-ethernet-services | ethernet-vpls | vlan-vpls);
```

Ethernet interfaces in VLAN mode can have multiple logical interfaces. In CCC and VPLS modes, VLAN IDs from 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 4094 are reserved for CCC or VPLS VLANs. For 4-port Fast Ethernet interfaces, you can use VLAN IDs 512 through 1024 for CCC or VPLS VLANs.

For encapsulation type **flexible-ethernet-services**, all VLAN IDs are valid.

In general, you configure an interface's encapsulation at the **[edit interfaces *interface-name*]** hierarchy level. However, for some encapsulation types, including flexible Ethernet services, Ethernet VLAN CCC and VLAN VPLS, you can also configure the encapsulation type that is used inside the VLAN circuit itself. To do this, include the **encapsulation** statement:

```
encapsulation (vlan-ccc | vlan-tcc | vlan-vpls);
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

You cannot configure a logical interface with VLAN CCC or VLAN VPLS encapsulation unless you also configure the physical device with the same encapsulation or with flexible Ethernet services encapsulation. In general, the logical interface must have a VLAN ID of

512 or higher; if the VLAN ID is 511 or lower, it will be subject to the normal destination filter lookups in addition to source address filtering. However if you configure flexible Ethernet services encapsulation, this VLAN ID restriction is removed.

### Example: Configuring VLAN Encapsulation on a Gigabit Ethernet Interface

Configure VLAN CCC encapsulation on a Gigabit Ethernet interface:

```
interfaces ge-2/1/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 600;
  }
}
```

### Example: Configuring VLAN Encapsulation on an Aggregated Ethernet Interface

Configure VLAN CCC encapsulation on an aggregated Gigabit Ethernet interface:

```
interfaces ae0 {
  vlan-tagging;
  encapsulation vlan-vpls;
  unit 0 {
    vlan-id 100;
  }
}
```

**Related Documentation**

- 802.1Q VLANs Overview on page 47

---

## Configuring Extended VLAN Encapsulation

Gigabit Ethernet, 4-port Fast Ethernet, MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, 10-Gigabit Ethernet, and aggregated Ethernet interfaces with VLAN tagging enabled can use extended VLAN CCC or VLAN VPLS, which allow 802.1Q tagging. To configure the encapsulation on a physical interface, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level, specifying **extended-vlan-ccc** or **extended-vlan-vpls**:

```
[edit interfaces interface-name]
encapsulation (extended-vlan-ccc | extended-vlan-vpls);
```

For extended VLAN CCC and extended VLAN VPLS encapsulation, all VLAN IDs 1 and higher are valid. VLAN ID 0 is reserved for tagging the priority of frames.



**NOTE:** For extended VLAN CCC, the VLAN IDs on ingress and egress interfaces must be the same. For back-to-back connections, all VLAN IDs must be the same.

---



### Example: Configuring Extended VLAN Encapsulation on a Gigabit Ethernet Interface

Configure extended VLAN CCC encapsulation on Gigabit Ethernet ingress and egress interfaces:

```
interfaces ge-0/0/0 {
  vlan-tagging;
  encapsulation extended-vlan-ccc;
  unit 0 {
    vlan-id 2;
    family ccc;
  }
}
interfaces ge-1/0/0 {
  vlan-tagging;
  encapsulation extended-vlan-ccc;
  unit 0 {
    vlan-id 2;
    family ccc;
  }
}
```

### Example: Configuring Extended VLAN Encapsulation on an Aggregated Ethernet Interface

Configure extended VLAN VPLS encapsulation on an aggregated Ethernet interface:

```
interfaces ae0 {
  vlan-tagging;
  encapsulation extended-vlan-vpls;
  unit 0 {
    vlan-id 100;
  }
}
```

**Related Documentation**

- [802.1Q VLANs Overview on page 47](#)

## Guidelines for Configuring VLAN ID List-Bundled Logical Interfaces That Connect CCCs

For MX Series routers, you can bind a list of VLAN IDs to a logical interface, configure a Layer 2 VPN routing instance or Layer 2 circuit on the logical interface, and then use the logical interface to configure a circuit cross-connect (CCC) to another Layer 2 VPN routing instance or Layer 2 circuit.

A CCC allows you to configure transparent connections between two circuits so that packets from the source circuit are delivered to the destination circuit with, at most, the Layer 2 address being changed. You configure a CCC by connecting circuit interfaces of the same type. For more information, see [Circuit and Translational Cross-Connects Overview](#).



**NOTE:** The Junos OS supports binding of Ethernet logical interfaces to lists of VLAN IDs on MX Series routers only. For all other routers, you can bind an Ethernet logical interface to only a single VLAN ID or to a single range of VLAN IDs.

The following configuration guidelines apply to bundling lists of VLAN IDs to Ethernet logical interfaces used to configure CCCs:

- Guidelines for Configuring Physical Link-Layer Encapsulation to Support CCCs on page 62
- Guidelines for Configuring Logical Link-Layer Encapsulation to Support CCCs on page 62

## Guidelines for Configuring Physical Link-Layer Encapsulation to Support CCCs

To enable a physical interface to support VLAN-bundled logical interfaces that you will use to configure a CCC, you must specify one of the following physical link-layer encapsulation types as the value of the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
encapsulation (extended-vlan-ccc | flexible-ethernet-services);
```

- **extended-vlan-ccc**—For Ethernet interfaces with standard TPID tagging.
- **flexible-ethernet-services**—For supported Gigabit Ethernet interfaces for which you want to configure multiple per-unit Ethernet encapsulations.

For more information about configuring the encapsulation on a physical interface, see [Configuring Interface Encapsulation on Physical Interfaces](#).

## Guidelines for Configuring Logical Link-Layer Encapsulation to Support CCCs

For VLAN-bundled logical interfaces that you use to configure a CCC, specific logical link-layer encapsulation types are used inside the circuits themselves.

Table 6 on page 63 describes the logical link-layer encapsulation types used within circuits connected using VLAN-bundled logical interfaces of the same type.

Table 6: Encapsulation Inside Circuits CCC-Connected by VLAN-Bundled Logical Interfaces

Encapsulation Inside the Circuit	Layer 2 Circuit Joined by Configuring an Interface-to-Interface CCC Connection	
	Layer 2 VPN Routing Instance	Layer 2 Circuit
Syntax	encapsulation-type (ethernet   ethernet-vlan);	encapsulation vlan-ccc;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols l2vpn], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn]	[edit interfaces <i>ethernet-interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>ethernet-interface-name</i> unit <i>logical-unit-number</i> ]
Usage Guidelines	See the <a href="#">Junos OS VPNs Configuration Guide</a> .	See Configuring Interface Encapsulation on Logical Interfaces, Circuit and Translational Cross-Connects Overview, and Defining the Encapsulation for Switching Cross-Connects.
For a Single-Tag Logical Interface	The MX Series router automatically uses <b>ethernet</b> as the Layer 2 protocol used to encapsulate incoming traffic. Although the connection spans multiple VLANs, the VLANs are bundled and therefore can be encapsulated as a single VLAN.  <b>NOTE:</b> With <b>ethernet</b> encapsulation, the circuit signal processing does not check that the VLAN ID list is the same at both ends of the CCC connection.	Configure the MX Series router to use <b>vlan-ccc</b> as the logical link-layer encapsulation type.
For a Dual-Tag Logical Interface	Configure the MX Series router to use <b>ethernet-vlan</b> as the Layer 2 protocol to encapsulate incoming traffic.  With <b>ethernet-vlan</b> encapsulation, circuit signal processing checks that the VLAN ID list is the same at both ends of the CCC connection. If a VLAN ID list mismatch is detected, you can view the error condition in the <b>show interfaces</b> command output.	The MX Series router automatically uses <b>vlan-ccc</b> as the logical link-layer encapsulation type, regardless of the value configured.

- Related Documentation**
- 802.1Q VLANs Overview on page 47
  - Binding VLAN IDs to Logical Interfaces on page 53
  - Defining the Encapsulation for Switching Cross-Connects

## Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface

This topic describes how to configure a Layer 2 VPN routing instance on a logical interface bound to a list of VLAN IDs.

- Configuring a VLAN-Bundled Logical Interface on page 64
- Specifying the Interface Over Which VPN Traffic Travels to the CE Router on page 64
- Specifying the Interface to Handle Traffic for a CCC on page 64

## Configuring a VLAN-Bundled Logical Interface

To configure a VLAN-bundled logical interface, specify the list of VLAN IDs by including the **vlan-id-list** statement or the **vlan-tags** statement on a provider edge (PE) router:

```
interfaces {
  ethernet-interface-name {
    vlan-tagging; # Support single- or dual-tag logical interfaces
    flexible-vlan-tagging; # Support mixed tagging
    encapsulation (extended-vlan-ccc | flexible-ethernet-services);
    unit logical-unit-number {
      vlan-id-list [vlan-id vlan-id-vlan-id]; # For single-tag
      vlan-tags outer <tpid.>vlan-id inner-list [vlan-id vlan-id-vlan-id]; # For dual-tag
    }
    ...
  }
}
```

You can include the statements at the following hierarchy levels:

- [edit]
- [edit logical-systems *logical-system-name*]

## Specifying the Interface Over Which VPN Traffic Travels to the CE Router

To configure a Layer 2 VPN routing instance on a PE router, include the **instance-type** statement and specify the value **l2vpn**. To specify an interface connected to the router, include the **interface** statement and specify the VLAN-bundled logical interface:

```
instance-type l2vpn;
interface logical-interface-name;
```

You can include the statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]

## Specifying the Interface to Handle Traffic for a CCC

To configure the VLAN-bundled logical interface as the interface to handle traffic for a circuit connected to the Layer 2 VPN routing instance, include the following statements:

```
protocols {
  l2vpn {
    (control-word | no-control-word);
    encapsulation-type (ethernet | ethernet-vlan);
    site site-name {
      site-identifier identifier;
      interface logical-interface-name { # VLAN-bundled logical interface
        ... interface-options ...
      }
    }
  }
}
```

You can include the statements at the same hierarchy level at which you include the **instance-type l2vpn** and **interface logical-interface-name** statements:

- [edit routing-instances *routing-instance-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]

To enable a Layer 2 VPN routing instance on a PE router, include the **l2vpn** statement. For more information, see the *Junos OS VPNs Configuration Guide*.

The **encapsulation-type** statement specifies the Layer 2 protocol used for traffic from the customer edge (CE) router. If the Layer 2 VPN routing instance is being connected to a single-tag Layer 2 circuit, specify **ethernet** as the encapsulation type. If the Layer 2 VPN routing instance is being connected to a dual-tag Layer 2 circuit, specify **ethernet-vlan** as the encapsulation type.

To specify the interface to handle traffic for a circuit connected to the Layer 2 VPN routing instance, include the **interface** statement and specify the VLAN-bundled logical interface.

## Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface

This topic describes how to configure a Layer 2 circuit on a logical interface bound to a list of VLAN IDs.

- Configuring a VLAN-Bundled Logical Interface on page 65
- Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit on page 66

## Configuring a VLAN-Bundled Logical Interface

To configure a VLAN-bundled logical interface, specify the list of VLAN IDs by including the **vlan-id-list** statement or the **vlan-tags** statement:

```
interfaces {
  ethernet-interface-name {
    vlan-tagging; # Support single- or dual-tag logical interfaces
    flexible-vlan-tagging; # Support mixed tagging
    encapsulation (extended-vlan-ccc | flexible-ethernet-services);
    unit logical-unit-number {
      encapsulation vlan-ccc; # Required for single-tag
      vlan-id-list [vlan-id vlan-id-vlan-id]; # For single-tag
      vlan-tags outer tpid.vlan-id inner-list [vlan-id vlan-id-vlan-id]; # For dual-tag
    }
    ...
  }
}
```

You can include the statements at the following hierarchy levels:

- [edit]
- [edit logical-systems *logical-system-name*]

For a single-tag logical interface, include the **encapsulation** statement and specify **vlan-ccc** so that CCC circuit encapsulation is used inside the Layer 2 circuit.



**NOTE:** In the case of a dual-tag logical interface, the Junos OS automatically uses the `vlan-ccc` encapsulation type.

---

## Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit

To configure the VLAN-bundled logical interface as the interface to handle traffic for a circuit connected to the Layer 2 circuit, include the following statements:

```
l2circuit {  
  neighbor address {  
    interface logical-interface-name {  
      virtual-circuit-id number;  
      no-control-word;  
    }  
  }  
}
```

You can include the statements at the following hierarchy levels:

- `[edit protocols]`
- `[edit logical-systems logical-system-name protocols]`

To enable a Layer 2 circuit, include the `l2circuit` statement.

To configure the router as a neighbor for a Layer 2 circuit, specify the neighbor address using the `neighbor` statement.

To specify the interface to handle traffic for a circuit connected to the Layer 2 circuit, include the `interface` statement and specify the VLAN-bundled logical interface.

---

## Example: Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface

The following configuration shows that the single-tag logical interface `ge-1/0/5.0` bundles a list of VLAN IDs, and the logical interface `ge-1/1/1.0` supports IPv4 traffic using IP address 10.30.1.130 and can participate in an MPLS path.

```
[edit interfaces]  
ge-1/0/5 {  
  vlan-tagging;  
  encapsulation extended-vlan-ccc;  
  unit 0 { # VLAN-bundled logical interface  
    vlan-id-list [513 516 520-525];  
  }  
}  
ge-1/1/1 {  
  unit 0 {  
    family inet {  
      address 10.30.1.1/30;  
    }  
    family mpls;  
  }  
}
```

The following configuration shows the type of traffic supported on the Layer 2 VPN routing instance:

```
[edit protocols]
rsvp {
  interface all;
  interface lo0.0;
}
mpls {
  label-switched-path lsp {
    to 10.255.69.128;
  }
  interface all;
}
bgp {
  group g1 {
    type internal;
    local-address 10.255.69.96;
    family l2vpn {
      signaling;
    }
    neighbor 10.255.69.128;
  }
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface lo0.0;
    interface ge-1/1/1.0;
  }
}
```

The following configuration shows that the VLAN-bundled logical interface is the interface over which VPN traffic travels to the CE router and handles traffic for a CCC to which the VPN connects.

```
[edit routing-instances]
red {
  instance-type l2vpn;
  interface ge-1/0/5.0; # VLAN-bundled logical interface
  route-distinguisher 10.255.69.96:100;
  vrf-target target:1:1;
  protocols {
    l2vpn {
      encapsulation-type ethernet; # For single-tag VLAN logical interface
      site CE_ultima {
        site-identifier 1;
        interface ge-1/0/5.0;
      }
    }
  }
}
```



**NOTE:** Because the VLAN-bundled logical interface supports single-tag frames, Ethernet is the Layer 2 protocol used to encapsulate incoming traffic. Although the connection spans multiple VLANs, the VLANs are bundled and therefore can be encapsulated as a single VLAN.

However, with Ethernet encapsulation, the circuit signal processing does not check that the VLAN ID list is the same at both ends of the CCC connection.

**Related Documentation**

- 802.1Q VLANs Overview on page 47

---

## Example: Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface

---

The following configuration shows that the single-tag logical interface **ge-1/0/5.0** bundles a list of VLAN IDs, and the logical interface **ge-1/1/1.0** supports IPv4 traffic using IP address 10.30.1.1/30 and can participate in an MPLS path.

```
[edit interfaces]
ge-1/0/5 {
  vlan-tagging;
  encapsulation extended-vlan-ccc;
  unit 0 { # VLAN-bundled logical interface
    vlan-id-list [513 516 520-525];
  }
}
ge-1/1/1 {
  unit 0 {
    family inet {
      address 10.30.1.1/30;
    }
    family mpls;
  }
}
```

The following configuration shows the type of traffic supported on the Layer 2 VPN routing instance, and shows that the VLAN-bundled logical interface handles traffic for a CCC to which the Layer 2 circuit connects:

```
[edit protocols]
rsvp {
  interface all;
  interface lo0.0;
}
mpls {
  label-switched-path lsp {
    to 10.255.69.128;
  }
  interface all;
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface lo0.0;
  }
}
```



```

        interface ge-1/1/1.0;
    }
}
ldp {
    interface ge-1/1/1.0;
    interface ge-1/0/5.0; # VLAN-bundled logical interface
    interface lo0.0;
}
l2circuit {
    neighbor 10.255.69.128 {
        interface ge-1/0/5.0 { # VLAN-bundled logical interface
            virtual-circuit-id 3;
            no-control-word;
        }
    }
}
}

```

**Related Documentation**

- 802.1Q VLANs Overview on page 47

## Configuring a Logical Interface for Access Mode

Enterprise network administrators can configure a single logical interface to accept untagged packets and forward the packets within a specified bridge domain. A logical interface configured to accept untagged packets is called an *access interface* or *access port*. Access interface configuration is supported on MX Series routers only.

```
interface-mode access;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family bridge]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family bridge]

When an untagged or tagged packet is received on an access interface, the packet is accepted, the VLAN ID is added to the packet, and the packet is forwarded within the bridge domain that is configured with the matching VLAN ID.

### Example: Configuring a Logical Interface for Access Mode

The following example configures a logical interface as an access port with a VLAN ID of 20:

```

[edit interfaces ge-1/2/0]
unit 1 {
    family bridge {
        interface-mode access;
        vlan-id 20;
    }
}

```

**Related Documentation**

- 802.1Q VLANs Overview on page 47

## Configuring a Logical Interface for Trunk Mode

---

As an alternative to configuring a logical interface for each VLAN, enterprise network administrators can configure a single logical interface to accept untagged packets or packets tagged with any VLAN ID specified in a list of VLAN IDs. Using a VLAN ID list conserves switch resources and simplifies configuration. A logical interface configured to accept packets tagged with any VLAN ID specified in a list is called a *trunk interface* or *trunk port*. Trunk interface configuration is supported on MX Series routers only. Trunk interfaces support integrated routing and bridging (IRB).

To configure a logical interface to accept any packet tagged with a VLAN ID that matches the list of VLAN IDs, include the **interface-mode** statement and specify the **trunk** option:

```
interface-mode trunk;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family bridge]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family bridge]

### Related Documentation

- 802.1Q VLANs Overview on page 47

## Configuring the VLAN ID List for a Trunk Interface

---

To configure the list of VLAN IDs to be accepted by the trunk port, include the **vlan-id-list** statement and specify the list of VLAN IDs. You can specify individual VLAN IDs with a space separating the ID numbers, specify a range of VLAN IDs with a dash separating the ID numbers, or specify a combination of individual VLAN IDs and a range of VLAN IDs.

```
vlan-id-list [number number-number];
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family bridge interface-mode trunk]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family bridge interface-mode trunk]

When a packet is received that is tagged with a VLAN ID specified in the trunk interface list of VLAN IDs, the packet is accepted and forwarded within the bridge domain that is configured with the matching VLAN ID.

When a packet is received that is tagged with a VLAN ID not specified in the trunk interface list of VLAN IDs, the native VLAN ID is pushed in front of the existing VLAN tag or tags and the packet is forwarded within the bridge domain that is configured with the matching VLAN ID.

When an untagged packet is received on a trunk interface, the native VLAN ID is added to the packet and the packet is forwarded within the bridge domain that is configured with the matching VLAN ID.

A bridge domain configured with a matching VLAN ID must be configured before the trunk interface is configured. To learn more about configuring bridge domains, see the *Junos Routing Protocols Configuration Guide*.

**Related Documentation**

- 802.1Q VLANs Overview on page 47

## Configuring a Trunk Interface on a Bridge Network

On MX Series routers, you can configure a trunk interface on a bridge network.

The following output sample shows trunk port configuration on a bridge network:

```
user@host# run show interfaces
ge-0/0/0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id 1;
  }
}
ge-2/0/0 {
  unit 0 {
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-200;
    }
  }
}
ge-2/0/1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id 1;
  }
}
```

If you want **igmp-snooping** to be functional for a bridge domain, then you should not configure **interface-mode** and **irb** for that bridge domain. Such a configuration commit succeeds, but IGMP snooping is not functional, and a message informing the same is displayed as shown after the sample configuration below:

```
user@host# run show configuration
interfaces {
  ge-5/1/1 {
    flexible-vlan-tagging;
    native-vlan-id 1;
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list 401;
      }
    }
  }
}
```

```
    }
  }
  irb {
    unit 401 {
      family inet {
        address 192.168.2.2/27;
      }
    }
  }
}
protocols {
  igmp {
    interface all;
  }
}
bridge-domains {
  VLAN-401 {
    vlan-id 401;
    routing-interface irb.401;
    protocols {
      igmp-snooping;
    }
  }
}

user@host# commit
[edit bridge-domains]
'VLAN-401'
IGMP Snooping not supported with IRB and trunk mode interface ge-5/1/1.0
commit complete
```

To achieve IGMP snooping for a bridge domain, you should use such a configuration as shown in the following example:

```
user@host# run show configuration
interfaces {
  ge-0/0/1 {
    flexible-vlan-tagging;
    native-vlan-id 1;
    encapsulation flexible-ethernet-services;
    unit 0 {
      encapsulation vlan-bridge;
      vlan-id 401;
    }
  }
  irb {
    unit 401 {
      family inet {
        address 192.168.2.2/27;
      }
    }
  }
}
protocols {
  igmp {
    interface all;
  }
}
bridge-domains {
  VLAN-401 {
    vlan-id 401;
    interface ge-0/0/1.0;
  }
}
```

```
        routing-interface irb.401;
        protocols {
            igmp-snooping;
        }
    }

user@host# commit
commit complete
```

- Related Documentation**
- 802.1Q VLANs Overview on page 47
  - interface-mode



## CHAPTER 4

# Configuring Aggregated Ethernet Interfaces

- Aggregated Ethernet Interfaces Overview on page 75
- Configuring an Aggregated Ethernet Interface on page 77
- Deleting an Aggregated Ethernet Interface on page 78
- Configuring Multichassis Link Aggregation on page 78
- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 80
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 88
- IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview on page 93
- Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers on page 99
- Configuring Aggregated Ethernet Link Protection on page 100
- Configuring the Number of Aggregated Ethernet Interfaces on the Device on page 101
- Configuring Aggregated Ethernet LACP on page 102
- Configuring Untagged Aggregated Ethernet Interfaces on page 108
- Configuring Aggregated Ethernet Link Speed on page 109
- Configuring Aggregated Ethernet Minimum Links on page 110
- Configuring Multicast Statistics Collection on Aggregated Ethernet Interfaces on page 111
- Configuring Hierarchical Scheduler on Aggregated Ethernet Interfaces Without Link Protection on page 111
- Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers on page 112

## Aggregated Ethernet Interfaces Overview

---

Link aggregation of Ethernet interfaces is defined in the IEEE 802.3ad standard. The Junos implementation of 802.3ad balances traffic across the member links within an aggregated Ethernet bundle based on the Layer 3 information carried in the packet. This implementation uses the same load-balancing algorithm used for per-packet load balancing. For information about per-packet load balancing, see the [Junos OS Routing Protocols Configuration Guide](#).



**NOTE:** For information about configuring circuit cross-connects over aggregated Ethernet, see [Circuit and Translational Cross-Connects Overview](#).

## Platform Support for Aggregated Ethernet Interfaces

You configure an aggregated Ethernet virtual link by specifying the link number as a physical device and then associating a set of ports that have the same speed and are in full-duplex mode. The physical interfaces can be Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ, Gigabit Ethernet IQ2 and IQ2-E, or 10-Gigabit Ethernet IQ2 and IQ2-E. Generally, you cannot use a combination of these interfaces within the same aggregated link; however, you can combine Gigabit Ethernet and Gigabit Ethernet IQ interfaces in a single aggregated Ethernet bundle.

The following routers support a maximum of 16 physical interfaces per single aggregated Ethernet bundle:

- M120
- M320
- All MX Series 3D Universal Edge Routers
- All T Series routers

All other routers support a maximum of 8 physical interfaces per aggregated Ethernet bundle.

Aggregated Ethernet interfaces can use interfaces from different FPCs, DPCs, PICs, or Trio MPCs.

## Configuration Guidelines for Aggregated Ethernet Interfaces

Simple filters are not supported for interfaces in aggregated Ethernet bundles:

- in M Series routers, simple filters are supported in Gigabit Ethernet Enhanced Intelligent Queuing interfaces only, except when the interface is part of an aggregated Ethernet bundle.
- in MX Series routers, simple filters are supported in Enhanced Queuing Dense Port Concentrator (EQ DPC) interfaces only, except when the interface is part of an aggregated Ethernet bundle.

For more information about simple filters, see the [Junos OS Class of Service Configuration Guide](#).

On the aggregated bundle, no IQ-specific capabilities such as MAC accounting, VLAN rewrites, and VLAN queuing are available. For more information about IQ-specific capabilities, see “Gigabit Ethernet Accounting and Policing Overview” on page 263.

Use the **show interfaces aggregate-interface extensive** and **show interfaces aggregate.logical-interface** commands to show the bandwidth of the aggregate. Also, the



SNMP object identifier `ifSpeed`/`ifHighSpeed` shows the corresponding bandwidth on the aggregate logical interface if it is configured properly.

Aggregated Ethernet interfaces can be either tagged or untagged, with LACP enabled or disabled. Aggregated Ethernet interfaces on MX Series routers support the configuration of **flexible-vlan-tagging**, **native-vlan-id**, and on dual-tagged frames, which consist of the following configuration statements:

- **inner-tag-protocol-id**
- **inner-vlan-id**
- **pop-pop**
- **pop-swap**
- **push-push**
- **swap-push**
- **swap-swap**

In all cases, you must set the number of aggregated Ethernet interfaces on the chassis. You can also set the link speed and the minimum links in a bundle.

---

## Configuring an Aggregated Ethernet Interface

On Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces on M Series and T Series routers, you can associate a physical interface with an aggregated Ethernet interface.

To configure an aggregated Ethernet interface:

1. Specify that you want to configure the link aggregation group interface.

```
user@host# edit interfaces interface-name
```

2. Configure the aggregated Ethernet interface.

```
[edit interfaces interface-name]  
user@host# set (fastether-options | gether-options) 802.3ad aex
```

You specify the interface instance number *x* to complete the link association; *x* can be from 1 through 480, for a total of 480 aggregated interfaces. You must also include a statement defining **aex** at the **[edit interfaces]** hierarchy level. You can optionally specify other physical properties that apply specifically to the aggregated Ethernet interfaces; for details, see “Ethernet Interfaces Overview” on page 31, and for a sample configuration, see “Example: Configuring Aggregated Ethernet Interfaces” on page 354.



**NOTE:** In general, aggregated Ethernet bundles support the features available on all supported interfaces that can become a member link within the bundle. As an exception, Gigabit Ethernet IQ features and some newer Gigabit Ethernet features are not supported in aggregated Ethernet bundles.

Gigabit Ethernet IQ and SFP interfaces can be member links, but IQ- and SFP-specific features are not supported on the aggregated Ethernet bundle even if all the member links individually support those features.

**Related Documentation**

- Configuring the Number of Aggregated Ethernet Interfaces on the Device on page 101
- Deleting an Aggregated Ethernet Interface on page 78
- Aggregated Ethernet Interfaces Overview on page 75

---

## Deleting an Aggregated Ethernet Interface

---

There are two approaches to deleting an aggregated Ethernet interface:

- You can delete an aggregated Ethernet interface from the interface configuration. The Junos OS removes the configuration statements related to **aex** and sets this interface to down state.
- You can also permanently remove the aggregated Ethernet interface from the device configuration by deleting it from the device-count on the routing device.

To delete an aggregated Ethernet interface:

1. Delete the aggregated Ethernet configuration.

This step changes the interface state to down and removing the configuration statements related to **aex**.

```
[edit]  
user@host# delete interfaces aex
```

2. Delete the interface from the device count.

```
[edit]  
user@host# delete chassis aggregated-devices ethernet device-count
```

**Related Documentation**

- Configuring an Aggregated Ethernet Interface on page 77
- Configuring the Number of Aggregated Ethernet Interfaces on the Device on page 101
- Aggregated Ethernet Interfaces Overview on page 75

---

## Configuring Multichassis Link Aggregation

---

On MX Series routers, multichassis link aggregation (MC-LAG) enables a device to form a logical LAG interface with two or more other devices. MC-LAG provides additional

benefits over traditional LAG in terms of node level redundancy, multi-homing support, and loop-free Layer 2 network without running Spanning Tree Protocol (STP). MC-LAG can be configured for VPLS routing instance, CCC application, and Layer 2 circuit encapsulation types.

The MC-LAG devices use Inter-Chassis Control Protocol (ICCP) to exchange the control information between two MC-LAG network devices.

On one end of MC-LAG is a MC-LAG client device that has one or more physical links in a link aggregation group (LAG). This client device does not need to be aware of MC-LAG. On the other side of MC-LAG are two MC-LAG network devices. Each of these network devices has one or more physical links connected to a single client device. The network devices coordinate with each other to ensure that data traffic is forwarded properly.

MC-LAG includes the following functionality:

- Active standby mode is supported using Link Aggregation Control Protocol (LACP)
- MC-LAG operates only between two chassis.
- Layer 2 circuit functions are supported with **ether-ccc** encapsulation.
- VPLS functions are supported with **ether-vpls** and **vlan-vpls**.

To enable MC-LAG, include the **mc-ae** statement at the **[edit interfaces aeX aggregated-ether-options]** hierarchy level along with either the **encapsulation ethernet-ccc** or **encapsulation ethernet-vpls** statement at the **[edit interfaces aeX]** hierarchy level:

```
[edit interfaces aeX]
encapsulation (ethernet-ccc | ethernet-vpls);
aggregated-ether-options {
  mc-ae {
    chassis-id chassis-id;
    mc-ae-id mc-ae-id;
    mode (active-active | active-standby);
    redundancy-group group-id;
    status-control (active | standby);
  }
}
```

To delete a MC-LAG interface from the configuration, issue the **delete interfaces aeX aggregated-ether-options mc-ae** command at the **[edit]** hierarchy level in configuration mode:

```
[edit]
user@host# delete interfaces aeX aggregated-ether-options mc-ae
```

#### Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 80
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 88
- show interfaces mc-ae

## Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview

MX Series routers support active-active bridging and virtual router redundancy protocol (VRRP) over Integrated routing and bridging (IRB). This is a common scenario used in data centers. This section provides an overview of the supported functionality.

Active-active bridging and VRRP over IRB support extends multichassis link aggregation group (MC-LAG) by adding the following functionality:

- Interchassis link (ICL) pseudowire interface or Ethernet interface (ICL-PL field) for active-active bridging
- Active-active bridging
- VRRP over IRB for active-active bridging
- A single bridge domain cannot correspond to two redundancy group IDs

The topologies shown in Figure 1 on page 80 and Figure 2 on page 80 are supported. These figures use the following abbreviations:

- Aggregated Ethernet (AE)
- Interchassis link (ICL)
- Multichassis link (MCL)

Figure 1: Single Multichassis Link

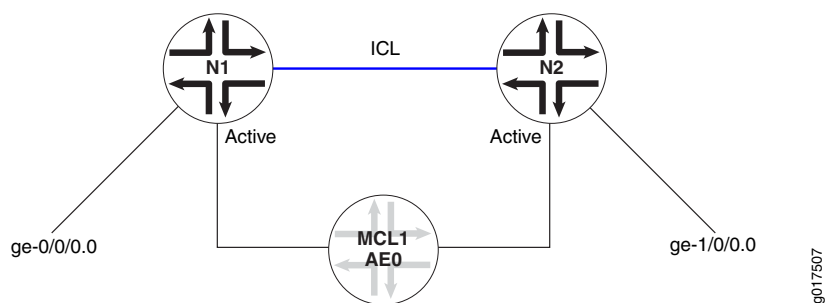
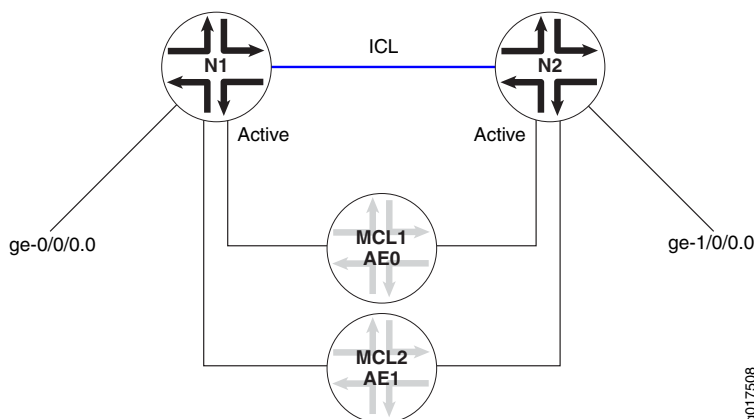


Figure 2: Dual Multichassis Link

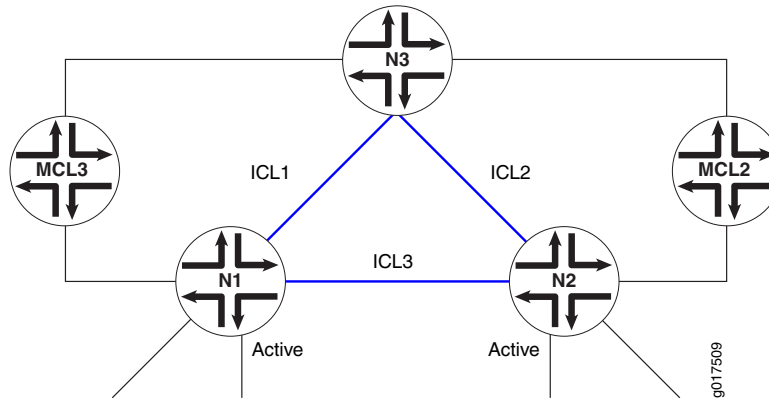


The following functionality is not supported:

- Virtual private LAN service (VPLS) within the core
- Bridged core
- Topology as described in Rule 4 of “Data Traffic Forwarding Rules” on page 83
- Routed multichassis aggregated Ethernet (RMC-AE), where the VRRP backup master is used in the edge of the network
- Track object, where in the case of an MC-LAG, the status of the uplinks from the provider edge can be monitored and the MC-LAG can act on the status
- Name string being specified as **service-id**

The topologies shown in Figure 3 on page 81, Figure 4 on page 81 and Figure 5 on page 82 are not supported:

**Figure 3: Interchassis Data Link Between Active-Active Nodes**



**Figure 4: Active-Active MC-LAG with Single MC-LAG**

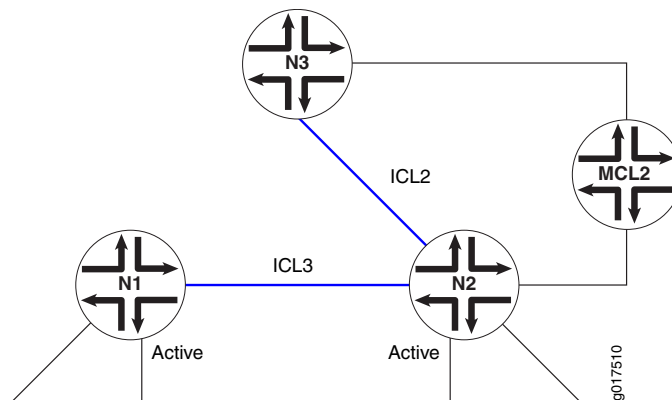
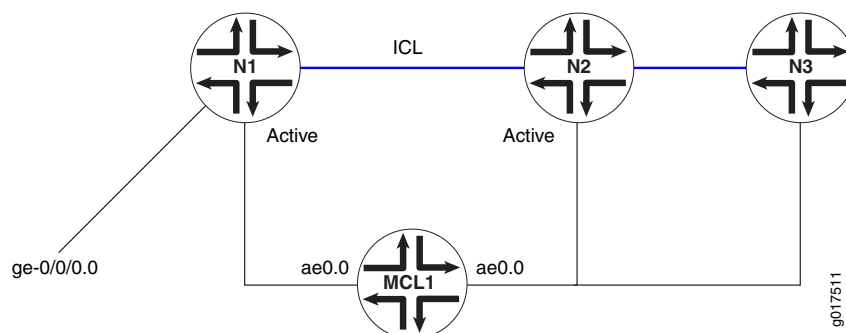


Figure 5: Active-Active MC-LAG with Multiple Nodes on a Single Multichassis Link



**NOTE:** A redundancy group cannot span more than two routers.

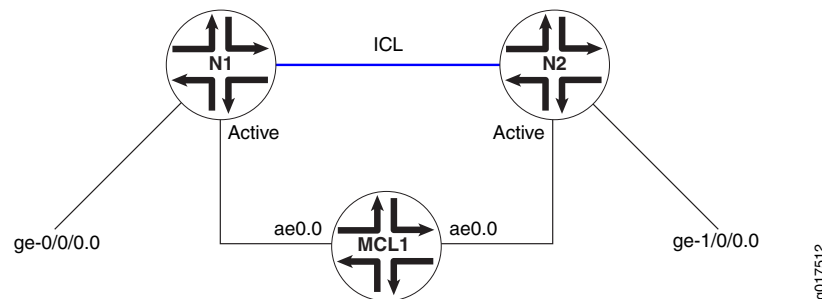
When configured to be active-active, the client device load balances the traffic to the peering MC-LAG network devices. In a bridging environment, this could potentially cause the following problems:

- Traffic received on the MC-LAG from one MC-LAG network device could be looped back to the same MC-LAG on the other MC-LAG network device.
- Duplicated packets could be received by the MC-LAG client device.
- Traffic could be unnecessarily forwarded on the interchassis link.

To better illustrate the problems listed above, consider Figure 6 on page 83, where an MC-LAG device MCL1 and single-homed clients **ge-0/0/0.0** and **ge-1/0/0.0** are allowed to talk to each other through an ICL:

- Traffic received on network routing instance N1 from MCL1 could be flooded to ICL to reach network routing instance N2. Once it reaches network routing instance N2, it could be flooded back to MCL1.
- Traffic received on interface **ge-0/0/0.0** could be flooded to MCL1 and ICL on network routing instance N1. Once network routing instance N2 receives such traffic from ICL, it could be again flooded to MCL1.
- If interface **ge-1/0/0.0** does not exist on network routing instance N2, traffic received from interface **ge-0/0/0.0** or MCL1 on network routing instance N1 could be flooded to network routing instance N2 through ICL unnecessarily since interface **ge-0/0/0.0** and MCL1 could reach each other through network routing instance N1.

Figure 6: MC-LAG Device and Single-Homed Client



## Data Traffic Forwarding Rules

In active-active bridging and VRRP over IRB topographies, network interfaces are categorized into three different interface types, as follows:

**S-Links**—Single-homed link (S-Link) terminating on MC-LAG-N device or MC-LAG in active-standby mode. In Figure 6 on page 83, interfaces **ge-0/0/0.0** and **ge-1/0/0.0** are S-Links.

**MC-Links**—MC-LAG links. In Figure 6 on page 83, interface **ae0.0** is the MC-Link.

**ICL**—Interchassis data link.

Based on incoming and outgoing interface types, some constraints are added to the Layer 2 forwarding rules for MC-LAG configurations, as described in the data traffic forwarding rules. Note that if only one of the MC-LAG member link is in the UP state, it is considered an S-Link.

The following data traffic forwarding rules apply:

1. When an MC-LAG network receives a packet from a local MC-Link or S-Link, the packet is forwarded to other local interfaces, including S-Links and MC-Links based on the normal Layer 2 forwarding rules and on the configuration of the **mesh-group** and **no-local-switching** statements. If MC-Links and S-Links are in the same mesh group and their **no-local-switching** statements are enabled, the received packets are only forwarded upstream and not sent to MC-Links and S-Links.

2.



**NOTE:** The functionality described in rule 2 is not supported.

The following circumstances determine whether or not an ICL receives a packet from a local MC-Link or S-Link:

- a. If the peer MC-LAG network device has S-Links or MC-LAGs that do not reside on the local MC-LAG network device.
- b. Whether or not interfaces on two peering MC-LAG network devices are allowed to talk to each other.

Only if both a. and b. are true, is traffic always forwarded to the ICL.

3. When an MC-LAG network receives a packet from the ICL, the packet is forwarded to all local S-Links and active MC-LAGs that do not exist in the MC-LAG network that the packet comes from.

4.



**NOTE:** The topology shown in Figure 7 on page 84 is not supported.

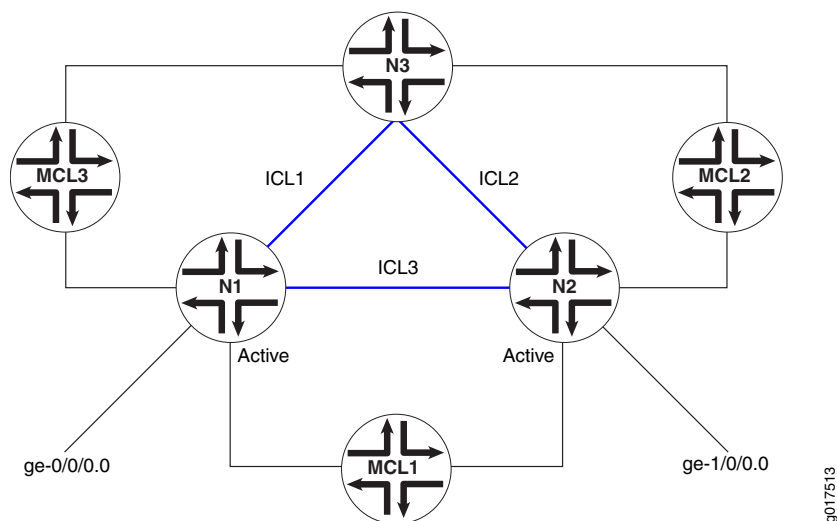
In certain cases, for example the topology shown in Figure 7 on page 84, there could be a loop caused by the ICL. To break the loops, one of the following mechanisms could be used:

- a. Run certain protocols, such as spanning tree protocol (STP). In this case, whether packets received on one ICL are forwarded to other ICLs is determined by using Rule 3.
- b. Configure the ICL to be fully meshed among the MC-LAG network devices. In this case, traffic received on the ICL would be not be forwarded to any other ICLs.

In either case, duplicate packets could be forwarded to the MC-LAG clients. Consider the topology shown in Figure 7 on page 84, where if network routing instance N1 receives a packet from **ge-0/0/0.0**, it could be flooded to ICL1 and ICL3.

When receiving from ICL1 and ICL3, network routing instances N3 and N2 could flood the same packet to MCL2, as shown in Figure 7 on page 84. To prevent this from happening, the ICL designated forwarder should be elected between MC-LAG peers and traffic received on an ICL could be forwarded to the active-active MC-LAG client by the designated forwarder only.

**Figure 7: Loop Caused by the ICL Links**



5. When received from an ICL, traffic should not be forwarded to the core-facing client link connection between two provider edge (PE) devices (C-Link) if the peer chassis's (where the traffic is coming from) C-Link is UP.



## MAC Address Management

If an MC-LAG is configured to be active-active, upstream and downstream traffic could go through different MC-LAG network devices. Since the media access control address (MAC address) is learned only on one of the MC-LAG network devices, the reverse direction's traffic could be going through the other MC-LAG network and flooded unnecessarily. Also, a single-homed client's MAC address is only learned on the MC-LAG network device it is attached to. If a client attached to the peer MC-LAG network needs to communicate with that single-homed client, then traffic would be flooded on the peer MC-LAG network device. To avoid unnecessary flooding, whenever a MAC address is learned on one of the MC-LAG network devices, it gets replicated to the peer MC-LAG network device. The following conditions should be applied when MAC address replication is performed:

- MAC addresses learned on a MC-LAG of one MC-LAG network device should be replicated as learned on the same MC-LAG of the peer MC-LAG network device.
- MAC addresses learned on single-homed customer edge (CE) clients of one MC-LAG network device should be replicated as learned on ICL-PL interface of the peer MC-LAG network device.
- MAC addresses learned on MC-LAG VE clients of one MC-LAG network device should be replicated as learned on the corresponding VE interface of the peer MC-LAG network device.
- MAC address learning on an ICL is disabled from the data path. It depends on software to install MAC addresses replicated through interchassis control protocol (ICCP).

---

### MAC Aging

MAC aging support in the Junos OS extends aggregated Ethernet logic for a specified MC-LAG. A MAC address in software is deleted until all Packet Forwarding Engines have deleted the MAC address. In the case of an MC-LAG, a remote provider edge is treated as a remote Packet Forwarding Engine and has a bit in the MAC data structure.

## Layer 3 Routing

In general, when an MC-LAG is configured to provide Layer 3 routing functions to downstream clients, the MC-LAG network peers should be configured to provide the same gateway address to the downstream clients. To the upstream routers, the MC-LAG network peers could be viewed as either equal-cost multi path (ECMP) or two routes with different preference values.

Junos OS supports active-active MC-LAGs using VRRP over IRB. Configuration of IP addresses on the MC-LAG members without VRRP is not supported.

To ensure that Layer 3 operates properly, instead of dropping the Layer 3 packet, the VRRP slave attempts to perform routing functions if the packet is received on an MC-LAG. A VRRP slave sends and responds to address resolution protocol (ARP) requests.

For ARP, the same issue exists as with Layer 2 MAC addresses. Once ARP is learned, it must be replicated to the MC-LAG through ICCP. The peer must install an ARP route based on the ARP information received through ICCP.

For ARP aging, ARP requests on the MC-LAG peers can be aged out independently.

## Address Resolution Protocol Active-Active MC-LAG Support Methodology

Suppose one of the PE routers issues an ARP request and another PE router gets the response and, because of the aggregated Ethernet distribution logic, the ARP resolution is not successful. Junos OS uses ARP response packet snooping to perform active-active multichassis link aggregation group support, providing easy synchronization without the need to maintain any specific state.

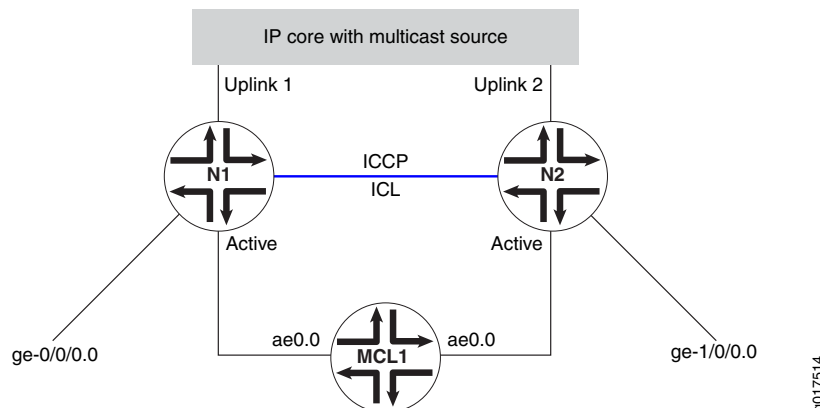
## IGMP Snooping on Active-Active MC-LAG

For multicast to work in an active-active MC-LAG scenario, the typical topology is as shown in Figure 8 on page 86 and Figure 9 on page 87 with interested receivers over S-links and MC-Links. Starting in Junos OS Release 11.2, support is extended for sources connected over Layer 2 interface.

If an MC-LAG is configured to be active-active, reports from MC-LAG clients could reach any of the MC-LAG network device peers. Therefore the IGMP snooping module needs to replicate the states such that the Layer 2 multicast route state on both peers are the same. Additionally for S-Link clients, snooping needs to replicate these joins to its snooping peer, which in the case of Layer 3 connected source, passes this information to the PIM on IRB to enable the designated router to pull traffic for these groups,

The ICL should be configured as a router facing interface. For the scenario where traffic arrives via a Layer 3 interface, it is a requirement to have PIM and IGMP enabled on the IRB interface configured on the MC-LAG network device peers.

**Figure 8: Multicast topology with source connected via Layer 3**



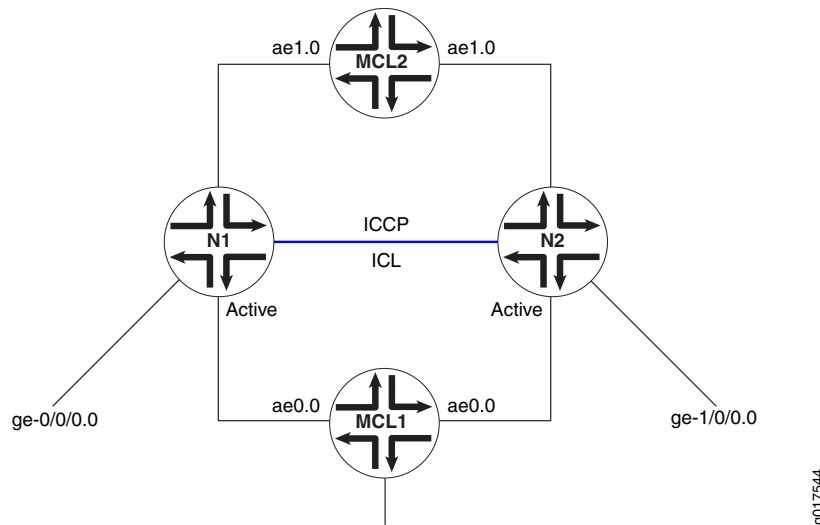
With reference to Figure 8 on page 86, either N1 or N2 becomes a designated router (for this example, N1 is the designated router). Router N1 would therefore pull the multicast traffic from the core. Once multicast data hits the network device N1, the data is forwarded based on the snooping learned route.

For MC-Link clients, data is forwarded via N1. In the case of failover of the MC-Links, the data reaches the client via N2. For S-Link clients on N1, data would be forwarded via normal snooping routes.

For S-Link clients on N2, data is forwarded via the ICL interface. Layer 2 multicast routes on N1 do not show these groups unless there is interest for the same group over MC-Links or over S-Links on N1. For IRB scenario, the IGMP membership and Layer 3 multicast route on N1 does however show these groups learned over the IRB interface.

Therefore, for a case where a specific group interest is only on the S-Link on N2, data arriving on N1 reaches N2 via the default route and the Layer 2 multicast route on N2 has the S-Link in the outgoing interface list.

**Figure 9: Multicast topology with source connected via MC-Link**



In Figure 9 on page 87, MCL1 and MCL2 are on different devices and the multicast source or IGMP querier is connected via MCL2. The data forwarding behavior seen is similar to that explained for multicast topology with source connected via Layer 3.



**NOTE:** IGMP snooping should not be configured in proxy mode. There should be no IGMP hosts or IGMP/PIM routers sitting on the ICL interface.

## Up and Down Event Handling

The following conditions apply to up and down event handling:

1. If the interchassis control protocol (ICCP) connection is UP but the ICL interface becomes DOWN, the router configured as standby will bring down all the multichassis aggregated Ethernet interfaces shared with the peer which is connected to ICL. This will make sure that there are no loops in the network. Otherwise, both PEs will become PIM designated routers and, hence, forward multiple copies of the same packet to the customer edge.
2. If the ICCP connection is UP and the ICL comes UP, the router configured as standby will bring up the multichassis aggregated Ethernet interfaces shared with the peer.
3. If both the ICCP connection and the ICL are DOWN, the router configured as standby will bring up the multichassis aggregated Ethernet interfaces shared with the peer.

4. The layer 2 address learn daemon (l2ald) does not store the information about a MAC address learned from a peer in the kernel. If l2ald restarts, and if the MAC address was not learned from the local multichassis aggregated Ethernet interface, l2ald will clear the MAC addresses and this will cause the router to flood the packets destined to this MAC address. This behavior is similar to that in a Routing Engine switchover. (Please note that currently l2ald runs on a Routing Engine only when it is a master). Also, during the time l2ald is DOWN, ARP packets received from an ICCP peer will be dropped. ARP retry will take care of this situation. This will be the case with Routing Engine switchover too.
5. If ICCP restarts, l2ald will unremember the fact that a MAC address was learned from a peer and, if the MAC address was learned only from the peer, that MAC address will be deleted and the packets destined to this MAC address will be flooded.

## Interchassis Control Protocol

Interchassis control protocol (ICCP) is used to sync configurations, states, and data.

ICCP supports the following types of state information:

- MC-LAG members and their operational states.
- Single-homed members and their operational states.

ICCP supports the following application database synchronization parameters:

- MAC addresses learned and to be aged.
- ARP info learned over IRB.

## Interchassis Control Protocol Message

ICCP messages and attribute-value pairs (AVPs) are used for synchronizing MAC address and ARP information.

### Related Documentation

- [Configuring Multichassis Link Aggregation on page 78](#)
- [Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 88](#)
- [multi-chassis-protection](#)
- [peer](#)
- [show interfaces mc-ae](#)

## Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers

---

The following sections describe the configuration of active-active bridging and VRRP over IRB in multichassis link aggregation (MC-LAG) on MX Series routers:

- [Configuring MC-LAG on page 89](#)
- [Configuring Interchassis Link Label on page 89](#)

- Configuring Multiple Chassis on page 90
- Configuring Service ID on page 90
- Configuring IGMP Snooping for Active-Active MC-LAG on page 92

## Configuring MC-LAG

An MC-LAG is composed of logical link aggregation groups (LAGs) and is configured under the **[edit interfaces aeX]** hierarchy, as follows:

```
[edit]
interfaces {
  ae0 {
    encapsulation ethernet-bridge;
    multi-chassis-protection {
      peer 10.10.10.10 {
        interface ge-0/0/0;
      }
    }
    aggregated-ether-options {
      mc-ae {
        mode active-active; # see note below
      }
    }
  }
}
```



**NOTE:** The **mode active-active** statement is valid only if encapsulation is **ethernet-bridge** or **extended-vlan-bridge**.

Use the **mode** statement to specify if a MC-LAG is **active-standby** or **active-active**. If the ICCP connection is UP and ICL comes UP, the router configured as standby will bring up the multichassis aggregated Ethernet (MC-AE) interfaces shared with the peer.

Using **multi-chassis-protection** at the physical interface level is a way to reduce the configuration at the logical interface level.

If the following assumption exists (follow the above example):

If there are  $n+1$  logical interfaces under **ae0**, from **ae0.0** through **ae0.n**, there will be  $n+1$  logical interfaces under **ge-0/0/0** as well, from **ge-0/0/0.0** through **ge-0/0/0.n**, each **ge-0/0/0** logical interface will be a protection link for the **ae0** logical interface.



**NOTE:** A bridge domain cannot have MC-AE logical interfaces which belong to different redundancy groups.

## Configuring Interchassis Link Label

Ethernet as interchassis link label (ICL-PL) (assumes interface **ge-0/0/0.0** is used to protect interface **ae0.0** of MC-LAG-1):

```
[edit]
```

```
interfaces {
  ae0 {
    ....
    unit 0 {
      multi-chassis-protection {
        peer 10.10.10.10 {
          interface ge-0/0/0.0;
        }
        ....
      }
      ...
    }
  }
}
```

The protection interface can be an Ethernet type interface like **ge**, **xe**, or an aggregated Ethernet (**ae**) interface.

## Configuring Multiple Chassis

A top-level hierarchy is used to specify multichassis-related configuration, as follows:

```
[edit]
multi-chassis {
  multi-chassis-protection {
    peer 10.10.10.10 {
      interface ge-0/0/0;
    }
  }
}
```

The above example specifies interface **ge-0/0/0** as the multichassis protection interface for all the multichassis aggregated Ethernet (MC-AE) interfaces which are also part of the peer. This can be overridden by specifying protection at the physical interface level and the logical interface level.

## Configuring Service ID

You must configure the same unique network-wide configuration for a service in the set of PEs providing the service. You can configure the service IDs under the **[edit interfaces *interface switch-options*]** hierarchy level of the hierarchies shown in the following examples.

Global configuration (default logical system)	<pre>[edit interfaces <i>interface-name</i>] switch-options {   service-id 10; } routing-instances {   r1 {     switch-options {       service-id 10;     }   } }</pre>
Logical systems	<pre>logical-system {</pre>

```

ls1 {
  switch-options {
    service-id 10;
  }
}
}
logical-system {
  ls1 {
    routing-instances {
      r1 {
        switch-options {
          service-id 10;
        }
      }
    }
  }
}
}

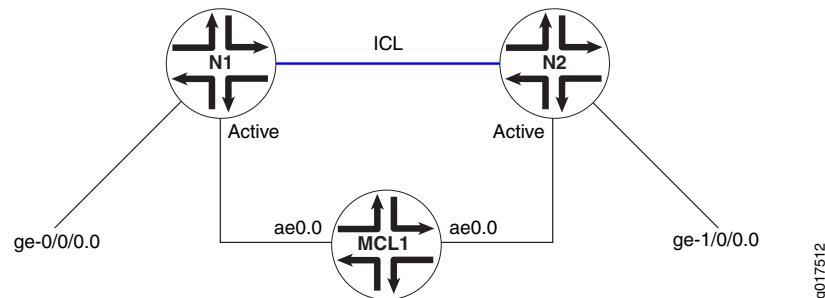
```



**NOTE:** Using a service name per bridge domain is not supported.

In the example shown in Figure 10 on page 91, network routing instances N1 and N2, both for the same service ID, are configured with same service-id in both N1 and N2. Use of a name string instead of a number is not supported.

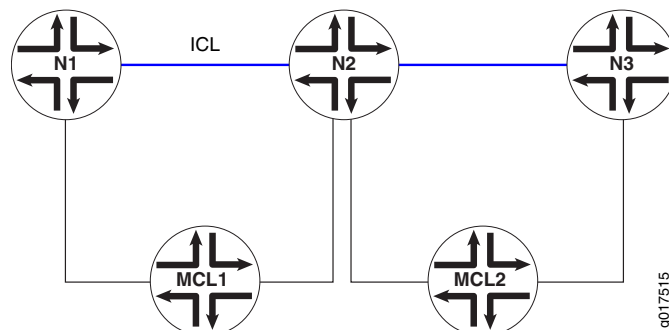
**Figure 10: N1 and N2 for the same service with same service ID**



The following configuration restrictions apply:

- The service ID must be configured when the MC-AE interface is configured and a MC-AE logical interface is part of a bridge domain. This requirement is enforced.
- A single bridge domain cannot correspond to two redundancy group IDs.

**Figure 11: Bridge Domain with Logical Interfaces from Two MC-AE Interfaces**



In Figure 11 on page 92, it is possible to configure a bridge domain consisting of logical interfaces from two MC-AE interfaces and map them to a separate redundancy group ID, which is not supported. A service should be mapped one-to-one with the redundancy group providing the service. This requirement is enforced.

To display the MC-AE configuration, use the **show interfaces *mc-ae*** command. For more information, see the [Junos OS Interfaces Command Reference](#).

## Configuring IGMP Snooping for Active-Active MC-LAG

- For the multicast solution to work, the following must be configured:
  - The multichassis protection link should be configured as a router-facing interface. Assuming the **ge-0/0/0** interface is configured as a multichassis protection link, the configuration example uses **ge-0/0/0.0**.

```
[edit bridge-domain bd-name]
protocols {
  igmp-snooping {
    interface ge-0/0/0.0 {
      multicast-router-interface;
    }
  }
}
```

In this example configuration, **ge-0/0/0.0** is an ICL interface.

- The **multichassis-lag-replicate-state** statement options should be configured under **multicast-snooping-options** statement for that bridge domain.



**NOTE:** Snooping with active-active MC-LAG is only supported in non-proxy mode and only for deployment where traffic comes via a Layer 3 interface. For such scenarios, the IRB interface should have PIM and IGMP configured.

### Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 80



- Configuring Multichassis Link Aggregation on page 78
- mc-ae
- multi-chassis-protection
- peer
- show interfaces irb
- show interfaces mc-ae

## IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview

---

- IGMP snooping in MC-LAG active-active on MX Series Routers functionality on page 93
- Typically supported network topology for IGMP snooping with MC-LAG active-active bridging on page 95
- Control plane state updates triggered by packets received on remote chassis on page 95
- Data forwarding on page 96
- Pure Layer 2 topology without integrated routing and bridging on page 97
- Qualified learning on page 97
- Data forwarding with qualified learning on page 98
- Static groups on single homed interfaces on page 98
- Router facing interfaces as multichassis links on page 98

### IGMP snooping in MC-LAG active-active on MX Series Routers functionality

MX Series routers support multichassis link aggregation group (MC-LAG) active-active and IGMP snooping in active-standby mode. MC-LAG allows one device to form a logical LAG interface with two or more network devices. MC-LAG provides additional benefits including node level redundancy, multi-homing, and loop-free layer-2 network without running STP. The following features are supported:

- State synchronization between peers for IGMP snooping in a bridge domain with only Layer 2 interfaces
- Qualified learning
- Router facing multichassis links

MX Series routers support the following enhancements to active-active bridging and virtual router redundancy protocol (VRRP) over integrated routing and bridging (IRB):

- MC-LAG support for IGMP snooping in a pure Layer 2 switch
- MC-LAG support for IGMP snooping in bridge domains doing qualified learning
- Support for MC-Links being router facing interfaces

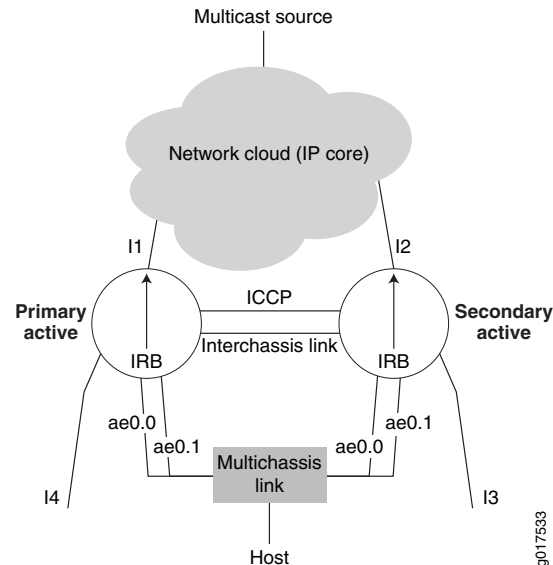
The following functions are not supported:

- MC-LAG for VPLS instances
- MC-Links trunk ports
- Proxy mode for active-active
- Adding interchassis links to outgoing interfaces on an as needed basis. Interchassis links can be added to the outgoing interface list as router facing interfaces.

## Typically supported network topology for IGMP snooping with MC-LAG active-active bridging

Figure 12 on page 95 depicts a typical network topology over which IGMP snooping with MC-LAG active-active is supported.

**Figure 12: Typical network over which active-active is supported**



Interfaces I3 and I4 are single-homed interfaces. The multichassis links (MC-Link) ae0.0 and ae0.1 belong to the same bridge domain in both the chassis. Interfaces I3, ae0.0 and ae0.1 are in the same bridge domain in S-A. Interfaces I4, ae0.0 and ae0.1 are in the same bridge domain in the primary active (P-A) router. Interfaces I3, I4, ae0.0 and ae0.1 are in the same learning domain as is the interchassis link (ICL) connecting the two chassis.

The primary active router is the chassis in which the integrated routing and bridging has become PIM-DR. The secondary active router is the chassis in which integrated routing and bridging is not PIM DR. Router P-A is the chassis responsible for pulling traffic from the IP core. Hence, PIM-DR election is used to avoid duplication of data traffic.

Learning domains are described in “Qualified learning” on page 97.

For the IGMP speakers (hosts and routers) in the learning domain, P-A and S-A together should appear as one device with interfaces I4, I3, ae0.0 and ae0.1.

No duplicate control packets should be sent on multichassis links, meaning the control packet should be sent through only one link.

## Control plane state updates triggered by packets received on remote chassis

The membership state in Layer 3 multicast routing is updated as a result of reports learned on remote legs of multichassis links and s-links attached to the remote chassis.

The membership state and routing entry in snooping is updated when reports are received on the remote legs of a multichassis link.

When reports are received on S-links attached to the remote chassis the membership state or routing entry in snooping is not updated.

The list of <s,g>s for which the state is maintained is the same in both the chassis under snooping as long as the outgoing interface lists involve only multichassis links.

## Data forwarding

This discussion assumes integrated routing and bridging on P-A is the PIM-DR. It pulls the traffic from sources in the core. Traffic might also come on Layer 2 interfaces in the bridge domain. For hosts directly connected to the P-A chassis, there is no change in the way data is delivered.

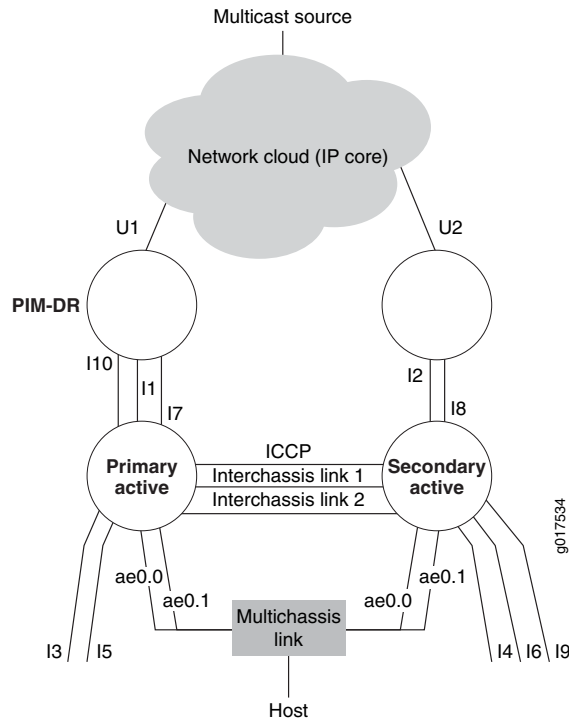
For delivering traffic to hosts connected to S-A (which is the non-DR) on the single-homed link like I3, we rely on interchassis link. The traffic that hits P-A is sent over ICL to S-A to be delivered to the links that have reported interests in s,g and the links that are router facing.

When ae0 leg in P-A goes down, the hosts connected to the multichassis link will receive traffic via ICL. In S-A, traffic received on ICL is sent to multichassis links in the outgoing interface list for which the ae counterpart in P-A is down.

## Pure Layer 2 topology without integrated routing and bridging

Figure 13 on page 97 illustrates the chassis connecting to the PIM-DR is the primary active router and the other is the secondary active.

**Figure 13: Layer 2 configuration without integrated routing and bridging**



## Qualified learning

In this application, interfaces I1, I2, I3, I4, I5, I6, I7, I8, I9 and I10 are single-homed interfaces. The multichassis links ae0.0 and ae0.1 belong to the same bridge domain in both the chassis. Interfaces I10, I1, I7, I3, I5, ae0.0 and ae0.1 are in same bridge domain, bd1 in P-A. Interfaces I9, I2, I8, I4, I6, ae0.0 and ae0.1 are in same bridge domain, bd1 in S-A.

This discussion assumes the following configuration:

- In Primary Active and S-A, qualified learning is ON in bd1.
- Interfaces I1, I2, I3, ae0.0 and I4 belong to vlan1, learning domain ld1.
- Interfaces I7, I8, I5, ae0.1 and I6 belong to vlan2, learning domain ld2.
- Interfaces I9 and I10 belong to vlan3, learning domain ld3.

For the IGMP speakers (hosts and routers) in the same learning domain ld1, P-A and S-A linked should appear to be one switch.

For the IGMP speakers (hosts and routers) in the same learning domain ld2, P-A and S-A linked should appear to be one switch.

Since there are no multichassis links in learning domain ld3, for the IGMP speakers (hosts and routers) in learning domain ld3, P-A and S-A will not appear to be one switch.

This discussion assumes interchassis link ICL1 corresponds to learning domain ld1 and interchassis link ICL2 corresponds to learning domain ld2.

Control packet flow is supported, with the exception of passing information to IRB.

### Data forwarding with qualified learning

This discussion assumes one learning domain (LD), ld1, and further assumes interface I1 on router P-A is connected to the PIM-DR in the learning domain and pulls the traffic from sources in the core.

For delivering traffic to hosts connected to router S-A (which is the non-DR) on the single-homed link like I2, I4 (belonging to ld1), we rely on ICL1. The traffic that hits router P-A on interface I1 is sent over interchassis link ICL1 to router S-A to be delivered to the links that have reported interests in s,g or the links that are router facing in learning domain ld1.

When the interface ae0 leg in router P-A goes down, the hosts connected to the multichassis link receive traffic from interface I1 via the interchassis link ICL1. In router S-A, traffic received on interchassis link ICL1 is sent to multichassis links in the outgoing interface list for which the aggregated Ethernet counterpart in router P-A is down.

It is further assumed that interface I9 in router S-A belongs to the learning domain ld3 with interests in s,g, and that interface I10 in learning domain ld3 in router P-A receives traffic for s,g. Interface I9 does not receive data in this topology because there are no multichassis links (in a-a mode) and hence no interchassis link in learning domain ld3.

### Static groups on single homed interfaces

For multichassis links, the static group configuration should exist on both legs and synchronization with the other chassis is not required.

Synchronization of the static groups on single homed interfaces between the chassis is not supported, however the addition of logical interfaces to the default outgoing interface list supports traffic delivery to the interface within a static configuration.

### Router facing interfaces as multichassis links

IGMP queries could arrive on either leg of the multichassis links but in both peers, the multichassis link should be considered as router facing.

Reports should exit only once from the multichassis link, that is from only one leg.

The following MC-LAG support for IGMP snooping in IRB is provided:

- Non-proxy snooping
- Logical interfaces must be outgoing interfaces for all routes including the default route
- IGMP snooping in a pure Layer 2 switch

- IGMP snooping in bridge domains doing qualified learning
- Router facing interface MC-Links

The following features are not supported:

- Proxy mode for active-active
- MC-LAG support for VPLS instances
- Trunk ports as multichassis links
- Adding logical interfaces to outgoing interfaces on need basis. However, logical interfaces are always added as a router facing interface to the outgoing interface list.

#### Related Documentation

- Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers on page 99
- Example: Configuring IGMP Snooping
- `igmp-snooping`
- `multicast-router-interface`
- `show l2-learning instance`

## Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers

You can use the bridge-domain statement's `service-id id` option to specify the multichassis aggregated Ethernet configuration.

- The **service-id** statement is mandatory for non-single VLAN type bridge domains (**none**, **all** or **vlan-id-tags:dual**).
- It is optional for bridge domains with a VID defined.
- If no service-id is defined in the latter case, it will be picked up from the RTT's **service-id** configuration.
- The bridge level service-id is required to link related bridge domains across peers, and should be configured with the same value.
- The service-id values share the name space across all bridging and routing instances, and across peers. Thus, duplicate values for service-ids are not permitted across these entities.
- A change of bridge **service-id** is considered catastrophic, and the bridge domain is reincarnated.

This procedure allows you to enable or disable the replication feature. This option applies to all instances.

To configure IGMP snooping in active-standby mode:

1. Use the **multichassis-lag-replicate-state** statement at the **multicast-snooping-options** hierarchy level in the master instance.

```
multicast-snooping-options {
```

```
...
multichassis-lag-replicate-state; # REQUIRED
}
```

The interchassis link, **interface *icl-intf-name***, of the learning domain should be a router facing interface.

1. Use the **interface *icl-intf-name*** statement at the **protocols igmp-snooping** hierarchy level, as shown in the following example:

```
protocols {
  igmp-snooping {
    interface icl-intf-name {
      multicast-router-interface;
    }
  }
}
```

**Related  
Documentation**

- IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview on page 93
- Example: Configuring IGMP Snooping
- igmp-snooping
- multicast-router-interface
- show l2-learning instance

---

## Configuring Aggregated Ethernet Link Protection

You can configure link protection for aggregated Ethernet interfaces to provide QoS on the links during operation.

On aggregated Ethernet interfaces, you designate a primary and backup link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router or switch. When the primary link fails, traffic is routed through the backup link. Because some traffic loss is unavoidable, egress traffic is not automatically routed back to the primary link when the primary link is reestablished. Instead, you manually control when traffic should be diverted back to the primary link from the designated backup link.

- Configuring Link Protection for Aggregated Ethernet Interfaces on page 100
- Configuring Primary and Backup Links for Link Aggregated Ethernet Interfaces on page 101
- Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup Link on page 101
- Disabling Link Protection for Aggregated Ethernet Interfaces on page 101

## Configuring Link Protection for Aggregated Ethernet Interfaces

Aggregated Ethernet interfaces support link protection to ensure QoS on the interface.



To configure link protection:

1. Specify that you want to configure the options for an aggregated Ethernet interface.

```
user@host# edit interfaces aex aggregated-ether-options
```

2. Configure the link protection mode.

```
[edit interfaces aex aggregated-ether-options]  
user@host# set link-protection
```

## Configuring Primary and Backup Links for Link Aggregated Ethernet Interfaces

To configure link protection, you must specify a primary and a secondary, or backup, link.

To configure a primary link and a backup link:

1. Configure the primary logical interface.

```
[edit interfaces interface-name]  
user@host# set (fastether-options | gigether-options) 802.3ad aex primary
```

2. Configure the backup logical interface.

```
[edit interfaces interface-name]  
user@host# set (fastether-options | gigether-options) 802.3ad aex backup
```

## Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup Link

On aggregated Ethernet interfaces, you designate a primary and backup link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router or switch. When the primary link fails, traffic is routed through the backup link. Because some traffic loss is unavoidable, egress traffic is not automatically routed back to the primary link when the primary link is reestablished. Instead, you manually control when traffic should be diverted back to the primary link from the designated backup link.

To manually control when traffic should be diverted back to the primary link from the designated backup link, enter the following operational command:

```
user@host> request interface revert aex
```

## Disabling Link Protection for Aggregated Ethernet Interfaces

To disable link protection, issue the **delete interface revert aex** configuration command.

```
user@host# delete interfaces aex aggregated-ether-options link-protection
```

## Configuring the Number of Aggregated Ethernet Interfaces on the Device

---

By default, no aggregated Ethernet interfaces are created. You must set the number of aggregated Ethernet interfaces on the routing device before you can configure them.

The maximum number of aggregated devices you can configure is 128. The aggregated interfaces are numbered from **ae0** through **ae127**.

1. Specify that you want to access the aggregated Ethernet configuration on the device.

```
user@host# edit chassis aggregated-devices ethernet
```

2. Set the number of aggregated Ethernet interfaces.

```
[edit chassis aggregated-devices ethernet]  
user@host# set device-count number
```

You must also specify the constituent physical links by including the **802.3ad** statement at the `[edit interfaces interface-name fastether-options]` or `[edit interfaces interface-name gigether-options]` hierarchy level.

#### Related Documentation

- For information about physical links, see [Configuring an Aggregated Ethernet Interface](#) on page 77
- For a sample configuration, see [Example: Configuring Aggregated Ethernet Interfaces](#) on page 354
- For information about configuring aggregated devices, see the [Junos OS System Basics Configuration Guide](#).

---

## Configuring Aggregated Ethernet LACP

For aggregated Ethernet interfaces, you can configure the Link Aggregation Control Protocol (LACP). LACP is one method of bundling several physical interfaces to form one logical interface. You can configure both VLAN-tagged and untagged aggregated Ethernet with or without LACP enabled.

For MC-LAG, you must specify the **system-id** and **admin key**. MC-LAG peers use the same **system-id** while sending the LACP messages. The **system-id** can be configured on the MC-LAG network device and synchronized between peers for validation.

LACP exchanges are made between actors and partners. An actor is the local interface in an LACP exchange. A partner is the remote interface in an LACP exchange.

LACP is defined in IEEE 802.3ad, *Aggregation of Multiple Link Segments*.

LACP was designed to achieve the following:

- Automatic addition and deletion of individual links to the aggregate bundle without user intervention
- Link monitoring to check whether both ends of the bundle are connected to the correct group

The Junos implementation of LACP provides link monitoring but not automatic addition and deletion of links.

The LACP mode can be active or passive. If the actor and partner are both in passive mode, they do not exchange LACP packets, which results in the aggregated Ethernet links not coming up. If either the actor or partner is active, they do exchange LACP packets. By default, LACP is turned off on aggregated Ethernet interfaces. If LACP is configured, it is in passive mode by default. To initiate transmission of LACP packets and response to LACP packets, you must configure LACP in active mode.

To enable LACP active mode, include the **lACP** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level, and specify the **active** option:

```
[edit interfaces interface-name aggregated-ether-options]
lACP {
  active;
}
```

To restore the default behavior, include the **lACP** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level, and specify the **passive** option:

```
[edit interfaces interface-name aggregated-ether-options]
lACP {
  passive;
}
```

For more information, see the following sections:

- Configuring the LACP Interval on page 103
- Configuring LACP Link Protection on page 104
- Tracing LACP Operations on page 106
- Example: Configuring Aggregated Ethernet LACP on page 107

## Configuring the LACP Interval

By default, the actor and partner send LACP packets every second. You can configure the interval at which the interfaces send LACP packets by including the **periodic** statement at the **[edit interfaces *interface-name* aggregated-ether-options lACP]** hierarchy level:

```
[edit interfaces interface-name aggregated-ether-options lACP]
periodic interval;
```

The interval can be fast (every second) or slow (every 30 seconds). You can configure different periodic rates on active and passive interfaces. When you configure the active and passive interfaces at different rates, the transmitter honors the receiver's rate.



**NOTE:** Source address filtering does not work when LACP is enabled. For more information about source address filtering, see “Enabling Ethernet MAC Address Filtering” on page 38.

Percentage policers are not supported on aggregated Ethernet interfaces with the CCC protocol family configured. For more information about percentage policers, see the *Junos OS Routing Policy Configuration Guide*.

Generally, LACP is supported on all untagged aggregated Ethernet interfaces. For more information, see “Configuring Untagged Aggregated Ethernet Interfaces” on page 108.

For M Series Multiservice Edge Routers with enhanced Flexible PIC Concentrators (FPCs) and T Series routers, LACP over VLAN-tagged aggregated Ethernet interfaces is supported. For 8-port, 12-port, and 48-port Fast Ethernet PICs, LACP over VLAN-tagged interfaces is not supported.

LACP Fast Periodic, which is achieved by configuring fast (every second) interval for periodic transmission of LACP packets, is supported with graceful Routing Engine switchover (GRES) on MX Series routers only.

---

## Configuring LACP Link Protection



**NOTE:** When using LACP link protection, you can configure only two member links to an aggregated Ethernet interface: one active and one standby.

To force active and standby links within an aggregated Ethernet, you can configure LACP link protection and system priority at the aggregated Ethernet interface level using the **link-protection** and **system-priority** statements. Configuring values at this level results in only the configured interfaces using the defined configuration. LACP interface configuration also enables you to override global (chassis) LACP settings.

LACP link protection also uses port priority. You can configure port priority at the Ethernet interface **[gigether-options]** hierarchy level using the **port-priority** statement. If you choose not to configure port priority, LACP link protection uses the default value for port priority (127).



**NOTE:** LACP link protection supports per-unit scheduling configuration on aggregated Ethernet interfaces.

---

### Enabling LACP Link Protection

To enable LACP link protection for an aggregated Ethernet interfaces, use the **link-protection** statement at the **[edit interfaces aeX aggregated-ether-options lacp]** hierarchy level:

```
[edit interfaces aeX aggregated-ether-options lacp]
```

```

link-protection;
  disable;
  revertive;
  non-revertive;
}

```

By default, LACP link protection reverts to a higher-priority (lower-numbered) link when that higher-priority link becomes operational or a link is added to the aggregator that is determined to be higher in priority. However, you can suppress link calculation by adding the **non-revertive** statement to the LACP link protection configuration. In nonrevertive mode, once a link is active and collecting and distributing packets, the subsequent addition of a higher-priority (better) link does not result in a switch and the current link remains active.

If LACP link protection is configured to be nonrevertive at the global (**[edit chassis]** hierarchy) level, you can add the **revertive** statement to the LACP link protection configuration to override the nonrevertive setting for the interface. In revertive mode, the addition of a higher-priority link to the aggregator results in LACP performing a priority recalculation and switching from the current active link to the new active link.



**CAUTION:** If both ends of an aggregator have LACP link protection enabled, make sure to configure both ends of the aggregator to use the same mode. Mismatching LACP link protection modes can result in lost traffic.

We strongly recommend you to use LACP on both ends of the aggregator, when you connect an aggregated Ethernet interface with two member interfaces of MX Series routers to any other vendor device. Otherwise, the vendor device (say a Layer 2 switch, or a router), will not be able to manage the traffic coming from the two link aggregated Ethernet bundle. As a result, you might observe the vendor device sending back the traffic to the backup member link of the aggregated Ethernet interface.

Currently, MX-MPC2-3D, MX-MPC2-3D-Q, MX-MPC2-3D-EQ, MX-MPC1-3D, MX-MPC1-3D-Q, and MPC-3D-16XGE-SFP do not drop traffic coming back to the backup link, whereas DPCE-R-Q-20GE-2XGE, DPCE-R-Q-20GE-SFP, DPCE-R-Q-40GE-SFP, DPCE-R-Q-4XGE-XFP, DPCE-X-Q-40GE-SFP, and DPCE-X-Q-4XGE-XFP drop traffic coming to the backup link.

### Configuring LACP System Priority

To configure LACP system priority for aggregated Ethernet interfaces on the interface, use the **system-priority** statement at the **[edit interfaces aeX aggregated-ether-options lacp]** hierarchy level:

```

[edit interfaces aeX aggregated-ether-options lacp]
system-priority;

```

The system priority is a 2-octet binary value that is part of the LACP system ID. The LACP system ID consists of the system priority as the two most-significant octets and the interface MAC address as the six least-significant octets. The system with the numerically

lower value for system priority has the higher priority. By default, system priority is 127, with a range of 0 to 65,535.

### Configuring LACP Port Priority

---

To configure LACP port priority for aggregated Ethernet interfaces, use the **port-priority** statement at the **[edit interfaces *interface-name* gigether-options 802.3ad aeX lacp]** or **[edit interfaces *interface-name* fastether-options 802.3ad aeX lacp]** hierarchy levels:

```
[edit interfaces interface-name gigether-options 802.3ad aeX lacp]
port-priority priority;
```

The port priority is a 2-octet field that is part of the LACP port ID. The LACP port ID consists of the port priority as the two most-significant octets and the port number as the two least-significant octets. The system with the numerically lower value for port priority has the higher priority. By default, port priority is 127, with a range of 0 to 65,535.

Port aggregation selection is made by each system based on the highest port priority and are assigned by the system with the highest priority. Ports are selected and assigned starting with the highest priority port of the highest priority system and working down in priority from there.



**NOTE:** Port aggregation selection (discussed above) is performed for the active link when LACP link protection is enabled. Without LACP link protection, port priority is not used in port aggregation selection.

### Tracing LACP Operations

To trace the operations of the LACP process, include the **traceoptions** statement at the **[edit protocols lacp]** hierarchy level:

```
[edit protocols lacp]
traceoptions {
  file <filename> <files number> <size size> <world-readable | no-world-readable>;
  flag <flag>;
  no-remote-trace;
}
```

You can specify the following flags in the **protocols lacp traceoptions** statement:

- **all**—All LACP tracing operations
- **configuration**—Configuration code
- **packet**—Packets sent and received
- **process**—LACP process events
- **protocol**—LACP protocol state machine
- **routing-socket**—Routing socket events
- **startup**—Process startup events

For general information about tracing, see the tracing and logging information in the [Junos OS System Basics Configuration Guide](#).

### Example: Configuring Aggregated Ethernet LACP

Configure aggregated Ethernet LACP over a VLAN-tagged interface:

<b>LACP with VLAN-Tagged Aggregated Ethernet</b>	<pre>[edit interfaces] fe-5/0/1 {   fastether-options {     802.3ad ae0;   } } ae0 {   aggregated-ether-options {     lacp {       active;     }   }   vlan-tagging;   unit 0 {     vlan-id 100;     family inet {       address 10.1.1.2/24 {         vrrp-group 0 {           virtual-address 10.1.1.4;           priority 200;         }       }     }   } }</pre>
--	---

Configure aggregated Ethernet LACP over an untagged interface:

<b>LACP with Untagged Aggregated Ethernet</b>	<pre>[edit interfaces] fe-5/0/1 {   fastether-options {     802.3ad ae0;   } } ae0 {</pre>
---	--

```

aggregated-ether-options {
  lacp {
    active;
  }
}
unit 0 {
  family inet {
    address 10.1.1.2/24 {
      vrrp-group 0 {
        virtual-address 10.1.1.4;
        priority 200;
      }
    }
  }
}
}

```

- Related Documentation**
- [lacp on page 386](#)
  - [link-protection on page 390](#)
  - [traceoptions](#)

## Configuring Untagged Aggregated Ethernet Interfaces

When you configure an untagged Aggregated Ethernet interface, the existing rules for untagged interfaces apply. These rules are as follows:

- You can configure only one logical interface (unit 0) on the port. The logical unit 0 is used to send and receive LACP or marker protocol data units (PDUs) to and from the individual links.
- You cannot include the **vlan-id** statement in the configuration of the logical interface.

Table 7 on page 108 lists untagged aggregated Ethernet and LACP support by PIC and router.

**Table 7: Untagged Aggregated Ethernet and LACP Support by PIC and Platform**

PIC Type	M Series	LACP	T Series	LACP
4-port Fast Ethernet PIC Type 1	Yes	Yes	Yes	Yes
1-port Gigabit Ethernet PIC Type 1	Yes	Yes	Yes	Yes
2-port Gigabit Ethernet PIC Type 2	Yes	Yes	Yes	Yes
4-port Gigabit Ethernet PIC Type 2	Yes	Yes	Yes	Yes
1-port 10-Gigabit Ethernet M160	Yes	Yes	NA	NA
10-port Gigabit Ethernet PIC Type 3	Yes (M120, M320)	Yes	Yes	Yes



**Table 7: Untagged Aggregated Ethernet and LACP Support by PIC and Platform (*continued*)**

PIC Type	M Series	LACP	T Series	LACP
1-port 10-Gigabit Ethernet PIC Type 3	N/A	NA	Yes	Yes
8-port Gigabit Ethernet PIC Type 3	Yes	Yes	Yes	Yes

The 8-port Fast Ethernet PIC does not support untagged aggregated Ethernet or LACP.

Syslog messages are logged if you try to configure an untagged aggregated Ethernet interface using an unsupported PIC type.

For more information about configuring LACP, see “Configuring Aggregated Ethernet LACP” on page 102.

### Example: Configuring Untagged Aggregated Ethernet Interfaces

Configure an untagged aggregated Ethernet interface by omitting the **vlan-tagging** and **vlan-id** statements from the configuration:

```
[edit interfaces]
fe-5/0/1 {
  fastether-options {
    802.3ad ae0;
  }
}
ae0 {
  unit 0 {
    family inet {
      address 13.1.1.2/24 {
        vrrp-group 0 {
          virtual-address 13.1.1.4;
          priority 200;
        }
      }
    }
  }
}
```

### Configuring Aggregated Ethernet Link Speed

On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. If you include in the aggregated Ethernet interface an individual link that has a speed different from the speed you specify in the **link-speed** parameter, an error message will be logged.

To set the required link speed:

1. Specify that you want to configure the aggregated Ethernet options.

```
user@host# edit interfaces interface-name aggregated-ether-options
```

2. Configure the link speed.

```
[edit interfaces interface-name aggregated-ether-options ]  
user@host# set link-speed speed
```

*speed* can be in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Aggregated Ethernet interfaces on the M120 router can have one of the following speed values:

- **100m**—Links are 100 Mbps.
- **10g**—Links are 10 Gbps.
- **1g**—Links are 1 Gbps.
- **OC192**—Links are OC192 or STM64c.

Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speeds:

- **10m**
- **100m**
- **1g**
- **10g**
- **50g**

---

## Configuring Aggregated Ethernet Minimum Links

On aggregated Ethernet interfaces, you can configure the minimum number of links that must be up for the bundle as a whole to be labeled **up**. By default, only one link must be up for the bundle to be labeled **up**.

To configure the minimum number of links:

1. Specify that you want to configure the aggregated Ethernet options.

```
user@host# edit interfaces interface-name aggregated-ether-options
```

2. Configure the minimum number of links.

```
[edit interfaces interface-name aggregated-ether-options]  
user@host# set minimum-links number
```

On M120, M320, MX Series, T Series, and TX Matrix routers with Ethernet interfaces, the valid range for **minimum-links *number*** is 1 through 16. When the maximum value (16) is specified, all configured links of a bundle must be up for the bundle to be labeled **up**.

On all other routers and on EX Series switches, other than EX8200 switches, the range of valid values for **minimum-links *number*** is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled **up**.

On EX8200 switches, the range of valid values for **minimum-links number** is 1 through 12. When the maximum value (12) is specified, all configured links of a bundle must be up for the bundle to be labeled **up**.

If the number of links configured in an aggregated Ethernet interface is less than the minimum link value configured under the **aggregated-ether-options** statement, the configuration commit fails and an error message is displayed.

## Configuring Multicast Statistics Collection on Aggregated Ethernet Interfaces

T Series and TX Matrix routers support multicast statistics collection on aggregated Ethernet interfaces in both ingress and egress directions. The multicast statistics functionality can be configured on a physical interface thus enabling multicast accounting for all the logical interfaces below the physical interface.

The multicast statistics information is displayed only when the interface is configured with the **multicast-statistics** statement, which is not enabled by default.

Multicast statistics collection requires at least one logical interface is configured with family inet or inet6; otherwise, the commit for **multicast-statistics** will fail.

The multicast in/out statistics can be obtained via interfaces statistics query through CLI and via MIB objects through SNMP query.

To configure multicast statistics:

1. Include the **multicast-statistics** statement at the **[edit interfaces interface-name]** hierarchy level.

An example of a multicast statistics configuration for an aggregated Ethernet interface follows:

```
[edit interfaces]
ae0 {
    multicast-statistics;
}
```

To display multicast statistics, use the **show interfaces *interface-name* statistics detail** command.

### Related Documentation

- **multicast-statistics**
- Configuring Multicast Statistics Collection on Ethernet Interfaces on page 45

## Configuring Hierarchical Scheduler on Aggregated Ethernet Interfaces Without Link Protection

On aggregated Ethernet interfaces configured on the IQ2 PIC, you can configure the hierarchical scheduler in non-link-protect mode. The M120, MX Series, and T Series routers with aggregated Ethernet IQ2 PICs in non-link-protect mode support the following scheduler functions:

- Per unit scheduler
- Hierarchical scheduler
- Shaping at the physical interface

To configure the hierarchical scheduler on aggregated Ethernet interfaces in the non link-protect mode, include the **hierarchical-scheduler** statement at the **[edit interfaces aeX]** hierarchy level:

```
[edit interfaces aeX hierarchical-scheduler]
```

Prior to Junos OS Release 9.6, the hierarchical scheduler mode on these models required the **aggregated-ether-options** statement **link-protection** option, otherwise a configuration error occurs.

To specify the member link bandwidth derivation based on the equal division model (**scale**) or the replication model (**replicate**) on aggregated Ethernet interfaces, include the **member-link-scheduler (scale | replicate)** option at the **[edit class-of-service interfaces aeX]** hierarchy level. The default setting is **scale**.

```
[edit class-of-service interfaces aeX member-link-scheduler (scale | replicate)]
```



**NOTE:** In link-protect mode, only one link is active at a time and the other link acts as the backup link, whereas in a non link-protect mode, all the links of the aggregate bundle are active at the same time. There is no backup link. If a link goes down or a new link is added to the bundle, traffic redistribution occurs.

**Related Documentation**

- Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links
- For more information on the hierarchical scheduler (CoS), see the *Junos Class of Service Configuration Guide*.

---

## Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers

This section describes configuration of symmetrical load balancing on an 802.3ad link aggregation group (LAG) on MX Series routers.

- Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview on page 112
- Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers on page 113
- Example Configurations on page 116

### Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview

MX Series routers with Aggregated Ethernet PICs support symmetrical load balancing on an 802.3ad LAG. This feature is significant when two MX Series routers are connected

transparently through deep packet inspection (DPI) devices over an LAG bundle. DPI devices keep track of flows and require information of a given flow in both forward and reverse directions. Without symmetrical load balancing on an 802.3ad LAG, the DPIs could misunderstand the flow, leading to traffic disruptions. By using this feature, a given flow of traffic (duplex) is ensured for the same devices in both directions.

Symmetrical load balancing on an 802.3ad LAG utilizes a mechanism of interchanging the source and destination addresses for a hash computation of fields, such as source address and destination address. The result of a hash computed on these fields is used to choose the link of the LAG. The hash-computation for the forward and reverse flow must be identical. This is achieved by swapping source fields with destination fields for the reverse flow. The swapped operation is referred to as *complement hash computation* or **symmetric-hash complement** and the regular (or unswapped) operation as *symmetric-hash computation* or **symmetric-hash**. The swappable fields are MAC address, IP address, and port.

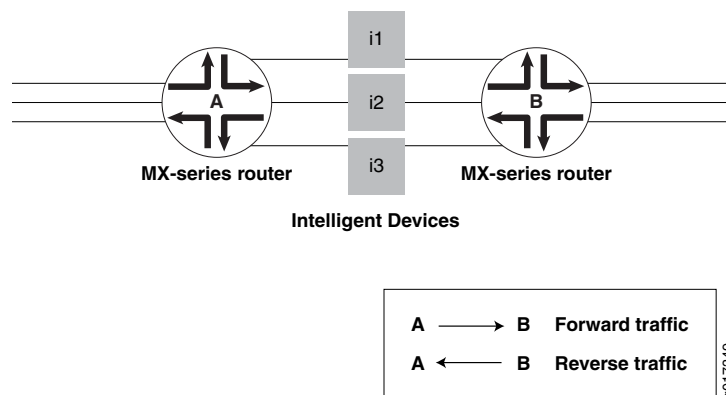
### Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers

You can specify whether symmetric hash or complement hash is done for load-balancing traffic. To configure symmetric hash, use the **symmetric-hash** statement at the **[edit forwarding-options hash-key family inet]** hierarchy level. To configure symmetric hash complement, use the **symmetric-hash complement** statement and option at the **[edit forwarding-options hash-key family inet]** hierarchy level.

These operations can also be performed at the PIC level by specifying a *hash key*. To configure a hash key at the PIC level, use the **symmetric-hash** or **symmetric-hash complement** statement at the **[edit chassis hash-key family inet]** and **[edit chassis hash-key family multiservice]** hierarchy levels.

Consider the example in Figure 14 on page 113.

**Figure 14: Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers**



Router A is configured with symmetric hash and Router B is configured with symmetric hash complement. Thus, for a given flow *fx*, post hash computation is from Router A to Router B through i2. The reverse traffic for the same flow *fx* is from Router B to Router A through the same i2 device as its hashing (done after swapping source and destination

fields) and returns the same link index; since it is performed on the interchanged source and destination addresses.

However, the link chosen may or may not correspond to what was attached to the DPI. In other words, the hashing result should point to the same links that are connected, so that the traffic flows through the same DPI devices in both directions. To make sure this happens, you need to also configure the counterpart ports (ports that are connected to same DPI-IN) with the identical link index. This is done when configuring a child-link into the LAG bundle. This ensures that the link chosen for a given hash result is always the same on either router.

Note that any two links connected to each other should have the same link index and these link indices must be unique in a given bundle.

**NOTE:**

The following restrictions apply when configuring symmetric load balancing on an 802.3ad LAG on MX Series routers:

- The Packet Forwarding Engine (PFE) can be configured to hash the traffic in either symmetric or complement mode. A single PFE complex cannot work simultaneously in both operational modes and such a configuration can yield undesirable results.
- The per-PFE setting overrides the chassis-wide setting only for the family configured. For the other families, the PFE complex still inherits the chassis-wide setting (when configured) or the default setting.
- Any change in the hash key configuration requires a reboot of the FPC for the changes to take effect.
- This feature supports VPLS, INET, and bridged traffic only.
- This feature cannot work in tandem with the **per-flow-hash-seed load-balancing** option. It requires that all the PFE complexes configured in complementary fashion share the same seed. A change in the seed between two counterpart PFE complexes may yield undesired results.

---

For additional information, see the [Junos OS VPNs Configuration Guide](#) and the [Junos OS System Basics Configuration Guide](#).

**Example Configuration Statements**

To configure 802.3ad LAG parameters at the bundle level:

```
[edit interfaces]
g(x)e-fpc/pic/port {
  gigether-options {
    802.3ad {
      bundle;
      link-index number;
    }
  }
}
```

where the **link-index *number*** ranges from 0 through 15.

You can check the link index configured above using the **show interfaces** command:

```
[edit forwarding-options hash-key]
family inet {
  layer-3;
  layer-4;
  symmetric-hash {
    [complement;]
  }
}
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3 {
        source-ip-only | destination-ip-only;
      }
      layer-4;
    }
  }
  symmetric-hash {
    [complement;]
  }
}
```

For load-balancing Layer 2 traffic based on Layer 3 fields, you can configure 802.3ad LAG parameters at a per PIC level. These configuration options are available under the chassis hierarchy as follows:

```
[edit chassis]
fpc X {
  pic Y {
    .
    .
    .
    hash-key {
      family inet {
        layer-3;
        layer-4;
        symmetric-hash {
          [complement;]
        }
      }
      family multiservice {
        source-mac;
        destination-mac;
        payload {
          ip {
            layer-3 {
              source-ip-only | destination-ip-only;
            }
            layer-4;
          }
        }
      }
      symmetric-hash {
```

```
        [complement;]  
      }  
    }  
  }  
  .  
  .  
  .  
}  
}
```

## Example Configurations

### Example Configurations of Chassis Wide Settings

---

**Router A**     user@host> show configuration forwarding-options hash-key  
family multiservice {  
  payload {  
    ip {  
      layer-3;  
    }  
  }  
  symmetric hash;  
}

**Router B**     user@host> show configuration forwarding-options hash-key  
family multiservice {  
  payload {  
    ip {  
      layer-3;  
    }  
  }  
  symmetric-hash {  
    complement;  
  }  
}

### Example Configurations of Per-Packet-Forwarding-Engine Settings

---

**Router A**     user@host> show configuration chassis fpc 2 pic 2 hash-key  
family multiservice {  
  payload {  
    ip {  
      layer-3;  
    }  
  }  
  symmetric hash;  
}

**Router B**     user@host> show configuration chassis fpc 2 pic 3 hash-key  
family multiservice {  
  payload {  
    ip {  
      layer-3;  
    }  
  }  
  symmetric-hash {



```
        complement;  
    }  
}
```



## CHAPTER 5

# Stacking and Rewriting Gigabit Ethernet VLAN Tags

- Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview on page 119
- Stacking and Rewriting Gigabit Ethernet VLAN Tags on page 120
- Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames on page 123
- Configuring Stacked VLAN Tagging on page 124
- Configuring Dual VLAN Tags on page 124
- Configuring Inner and Outer TPIDs and VLAN IDs on page 124
- Stacking a VLAN Tag on page 127
- Removing a VLAN Tag on page 128
- Removing the Outer and Inner VLAN Tags on page 128
- Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag on page 129
- Stacking Two VLAN Tags on page 129
- Rewriting the VLAN Tag on Tagged Frames on page 130
- Rewriting a VLAN Tag on Untagged Frames on page 131
- Rewriting a VLAN Tag and Adding a New Tag on page 133
- Rewriting the Inner and Outer VLAN Tags on page 134
- Examples: Stacking and Rewriting Gigabit Ethernet IQ VLAN Tags on page 134

## Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview

---

Stacking and rewriting VLAN tags allows you to use an additional (outer) VLAN tag to differentiate between customer edge (CE) routers that share one VLAN ID. A frame can be received on an interface, or it can be internal to the system (as a result of the **input-vlan-map** statement).

On IQ2 interfaces, 10-Gigabit Ethernet LAN/WAN PIC, IQ2-E interfaces, and MX Series interfaces, when a VLAN tag is pushed, the inner VLAN IEEE 802.1p bits are copied to the IEEE bits of the VLAN or VLANs being pushed. If the original packet is untagged, the IEEE bits of the VLAN or VLANs being pushed are set to 0.



**NOTE:** When swap-by-poppush is configured on the interface, when a VLAN tag is swapped, the inner VLAN IEEE 802.1p bits are copied to the IEEE bits of the VLAN being swapped. If swap-by-poppush is not configured on the interface, the VLAN IEEE 802.1p bits of the of the VLAN being swapped remains same.

---

You can stack and rewrite VLAN tags on the following interfaces:

- Gigabit Ethernet
- Gigabit Ethernet IQ
- 10-Gigabit Ethernet LAN/WAN PIC
- Gigabit Ethernet IQ2 and IQ2-E
- 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, and MX Series router Gigabit Ethernet Interfaces
- Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces with the VLAN encapsulation type configured to support Layer 2 tunneling protocols such as circuit cross-connect (CCC) or virtual private LAN service (VPLS) (as described in “802.1Q VLANs Overview” on page 47)

**Related  
Documentation**

- Stacking and Rewriting Gigabit Ethernet VLAN Tags on page 120

---

## Stacking and Rewriting Gigabit Ethernet VLAN Tags

---

You can configure rewrite operations to stack (**push**), remove (**pop**), or rewrite (**swap**) tags on single-tagged frames and dual-tagged frames. If a port is not tagged, rewrite operations are not supported on any logical interface on that port.

You can configure the following VLAN rewrite operations:

- **pop**—Remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
- **pop-pop**—For Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces, remove both the outer and inner VLAN tags of the frame.
- **pop-swap**—For Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces, remove the outer VLAN tag of the frame, and replace the inner VLAN tag of the frame with a user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.
- **push**—Add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag.
- **push-push**—For Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces, push two VLAN tags in front of the frame.

- **swap-push**—For Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces, replace the outer VLAN tag of the frame with a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.
- **swap-swap**—For Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces, replace both the inner and the outer VLAN tags of the incoming frame with a user-specified VLAN tag value.

You configure VLAN rewrite operations for logical interfaces in the input VLAN map for incoming frames and in the output VLAN map for outgoing frames. To configure the input VLAN map, include the **input-vlan-map** statement:

```
input-vlan-map {
  ...interface-specific configuration...
}
```

To configure the output VLAN map, include the **output-vlan-map** statement:

```
output-vlan-map {
  ...interface-specific configuration...
}
```

You can include both statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

The type of VLAN rewrite operation permitted depends upon whether the frame is single-tagged or dual-tagged. Table 8 on page 121 shows supported rewrite operations and whether they can be applied to single-tagged frames or dual-tagged frames. The table also indicates the number of tags being added or removed during the operation.

**Table 8: Rewrite Operations on Untagged, Single-Tagged, and Dual-Tagged Frames**

Rewrite Operation	Untagged	Single-Tagged	Dual-Tagged	Number of Tags
pop	No	Yes	Yes	– 1
push	Sometimes	Yes	Yes	+1
swap	No	Yes	Yes	0
push-push	Sometimes	Yes	Yes	+2
swap-push	No	Yes	Yes	+1
swap-swap	No	No	Yes	0
pop-pop	No	No	Yes	– 2

Table 8: Rewrite Operations on Untagged, Single-Tagged, and Dual-Tagged Frames (*continued*)

Rewrite Operation	Untagged	Single-Tagged	Dual-Tagged	Number of Tags
pop-swap	No	No	Yes	– 1

The rewrite operations **push** and **push-push** can be valid in certain circumstances on frames that are not tagged. For example, a single-tagged logical interface (interface 1) and a dual-tagged logical interface (interface 2) have the following configurations:

**Interface 1**    [edit interfaces *interface-name* unit *logical-unit-number*]  
                   input-vlan-map {  
                     pop;  
                   }  
                   output-vlan-map {  
                     push;  
                   }

**Interface 2**    [edit interfaces *interface-name* unit *logical-unit-number*]  
                   input-vlan-map {  
                     pop-pop;  
                   }  
                   output-vlan-map {  
                     push-push;  
                   }

When a frame is received on the interface as a result of the **input-vlan-map** operation, the frame is not tagged. As it goes out of the second interface, the **output-vlan-map** operation **push-push** is applied to it. The resulting frame will be dual-tagged at the logical interface output.

Depending on the VLAN rewrite operation, you configure the rewrite operation for the interface in the input VLAN map, the output VLAN map, or in both the input VLAN map and the output VLAN map. Table 9 on page 122 shows what rewrite operation combinations you can configure. “None” means that no rewrite operation is specified for the VLAN map.

Table 9: Applying Rewrite Operations to VLAN Maps

Input VLAN Map	Output VLAN Map								
	none	push	pop	swap	push-push	swap-push	swap-swap	pop-pop	swap-pop
none	Yes	No	No	Yes	No	No	Yes	No	No
push	No	No	Yes	No	No	No	No	No	No
pop	No	Yes	No	No	No	No	No	No	No
swap	Yes	No	No	Yes	No	No	No	No	No
push-push	No	No	No	No	No	No	No	Yes	No

Table 9: Applying Rewrite Operations to VLAN Maps (*continued*)

Input VLAN Map	Output VLAN Map								
	none	push	pop	swap	push-push	swap-push	swap-swap	pop-pop	swap-pop
swap-push	No	No	No	No	No	No	No	No	Yes
swap-swap	Yes	No	No	No	No	No	Yes	No	No
pop-pop	No	No	No	No	Yes	No	No	No	No
pop-swap	No	No	No	No	No	Yes	No	No	No

You must know whether the VLAN rewrite operation is valid and is applied to the input VLAN map or the output VLAN map. You must also know whether the rewrite operation requires you to include statements to configure the inner and outer TPIDs and inner and outer VLAN IDs in the input VLAN map or output VLAN map. For information about configuring inner and outer TPIDs and inner and outer VLAN IDs, see “Configuring Inner and Outer TPIDs and VLAN IDs” on page 124.

#### Related Documentation

- Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview on page 119
- Understanding swap-by-poppush
- swap-by-poppush

## Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames

For Gigabit Ethernet IQ interfaces, aggregated Ethernet with Gigabit Ethernet IQ interfaces, Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, you can configure frames with particular TPIDs to be processed as tagged frames. To do this, you specify up to eight IEEE 802.1Q TPID values per port; a frame with any of the specified TPIDs is processed as a tagged frame; however, with IQ2 and IQ2-E interfaces, only the first four IEEE 802.1Q TPID values per port are supported. To configure the TPID values, include the **tag-protocol-id** statement:

```
tag-protocol-id [ tpids ];
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* **gether-options** ethernet-switch-profile]
- [edit interfaces *interface-name* **aggregated-ether-options** ethernet-switch-profile]

All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces *interface-name* **gether-options** ethernet-switch-profile **tag-protocol-id** [ *tpids* ]] or [edit interfaces *interface-name* **aggregated-ether-options** ethernet-switch-profile **tag-protocol-id** [ *tpids* ]] hierarchy level.

## Configuring Stacked VLAN Tagging

---

To configure stacked VLAN tagging for all logical interfaces on a physical interface, include the **stacked-vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
  stacked-vlan-tagging;
```

If you include the **stacked-vlan-tagging** statement in the configuration, you must configure dual VLAN tags for all logical interfaces on the physical interface. For more information, see “Stacking a VLAN Tag” on page 127.

## Configuring Dual VLAN Tags

---

To configure dual VLAN tags on a logical interface, include the **vlan-tags** statement:

```
vlan-tags inner <tpid>.vlan-id outer <tpid>.vlan-id;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

The outer tag VLAN ID range is from 1 through 511 for normal interfaces, and from 512 through 4094 for VLAN CCC or VLAN VPLS interfaces. The inner tag is not restricted.

You must also include the **stacked-vlan-tagging** statement in the configuration. See “Examples: Stacking and Rewriting Gigabit Ethernet IQ VLAN Tags” on page 134.

## Configuring Inner and Outer TPIDs and VLAN IDs

---

For some rewrite operations, you must configure the inner or outer TPID values and inner or outer VLAN ID values. These values can be applied to either the input VLAN map or the output VLAN map.

On Ethernet IQ, IQ2, and IQ2-E interfaces; on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces; and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, to configure the inner TPID, include the **inner-tag-protocol-id** statement:

```
inner-tag-protocol-id tpid;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]**
- **[edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]**



- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

For the inner VLAN ID, include the **inner-vlan-id** statement. For the outer TPID, include the **tag-protocol-id** statement. For the outer VLAN ID, include the **vlan-id** statement:

```
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
output-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
```

For aggregated Ethernet interfaces using Gigabit Ethernet IQ interfaces, include the **tag-protocol-id** statement for the outer TPID. For the outer VLAN ID, include the **vlan-id** statement:

```
input-vlan-map {
  (pop | push | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
output-vlan-map {
  (pop | push | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

The VLAN IDs you define in the input VLAN maps are stacked on top of the VLAN ID bound to the logical interface. For more information about binding a VLAN ID to the logical interface, see “802.1Q VLANs Overview” on page 47.

All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces *interface-name* **gether-options ethernet-switch-profile tag-protocol-id [ *tpids* ]**] hierarchy level or [edit interfaces *interface-name* **aggregated-ether-options ethernet-switch-profile tag-protocol-id [ *tpids* ]**] hierarchy level.

For more information, see “Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames” on page 123.

Table 10 on page 126 and Table 11 on page 126 specify when these statements are required. Table 10 on page 126 indicates valid statement combinations for rewrite operations for the input VLAN map. “No” means the statement must not be included in the input VLAN map for the rewrite operation. “Optional” means the statement may be optionally specified for the rewrite operation in the input VLAN map. “Any” means that you must include the **vlan-id** statement, **tag-protocol-id** statement, **inner-vlan-id** statement, or **inner-tag-protocol-id** statement.

**Table 10: Rewrite Operations and Statement Usage for Input VLAN Maps**

Rewrite Operation	Input VLAN Map Statements			
	vlan-id	tag-protocol-id	inner-vlan-id	inner-tag-protocol-id
push	Optional	Optional	No	No
pop	No	No	No	No
swap	Any	Any	No	No
push-push	Optional	Optional	Optional	optional
swap-push	Optional	Optional	Any	Any
swap-swap	Optional	Optional	Any	Any
pop-swap	No	No	Any	Any
pop-pop	No	No	No	No

Table 11 on page 126 indicates valid statement combinations for rewrite operations for the output VLAN map. “No” means the statement must not be included in the output VLAN map for the rewrite operation. “Optional” means the statement may be optionally specified for the rewrite operation in the output VLAN map.

**Table 11: Rewrite Operations and Statement Usage for Output VLAN Maps**

Rewrite Operation	Output VLAN Map Statements			
	vlan-id	tag-protocol-id	inner-vlan-id	inner-tag-protocol-id
push	No	Optional	No	No
pop	No	No	No	No
swap	No	Optional	No	No
push-push	No	Optional	No	Optional

Table 11: Rewrite Operations and Statement Usage for Output VLAN Maps (*continued*)

	Output VLAN Map Statements			
swap-push	No	Optional	No	Optional
swap-swap	No	Optional	No	Optional
pop-swap	No	No	No	Optional
pop-pop	No	No	No	No

The following examples use Table 10 on page 126 and Table 11 on page 126 and show how the **pop-swap** operation can be configured in an input VLAN map and an output VLAN map:

Input VLAN Map with inner-vlan-id Statement, Output VLAN Map with Optional inner-tag-protocol-id Statement

```
[edit interfaces interface-name unit logical-unit-number]
input-vlan-map {
  pop-swap;
  inner-vlan-id number;
}
output-vlan-map {
  pop-swap;
  inner-tag-protocol-id tpid;
}
```

Input VLAN Map with inner-tag-protocol-id Statement, Output VLAN Map with Optional inner-tag-protocol-id Statement

```
[edit interfaces interface-name unit logical-unit-number]
input-vlan-map {
  pop-swap;
  inner-tag-protocol-id tpid;
}
output-vlan-map {
  pop-swap;
  inner-tag-protocol-id tpid;
}
```

Input VLAN Map with inner-tag-protocol-id and inner-vlan-id Statements

```
[edit interfaces interface-name unit logical-unit-number]
input-vlan-map {
  pop-swap;
  inner-vlan-id number;
  inner-tag-protocol-id tpid;
}
```

## Stacking a VLAN Tag

To stack a VLAN tag on all tagged frames entering or exiting the interface, include the **push**, **vlan-id**, and **tag-protocol-id** statements in the input VLAN map or the output VLAN map:

```
input-vlan-map {
  push;
  vlan-id number;
```

```
    tag-protocol-id tpid;  
  }  
  output-vlan-map {  
    push;  
    tag-protocol-id tpid;  
  }
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

If you include the **push** statement in an interface's input VLAN map, see Table 9 on page 122 for information about permissible rewrite operations,

The VLAN IDs you define in the input VLAN maps are stacked on top of the VLAN ID bound to the logical interface. For more information about binding a VLAN ID to the logical interface, see “802.1Q VLANs Overview” on page 47.

All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces *interface-name* **giether-options ethernet-switch-profile tag-protocol-id [ *tpids* ]**] hierarchy level. For more information, see “Configuring Inner and Outer TPIDs and VLAN IDs” on page 124.

---

## Removing a VLAN Tag

To remove a VLAN tag from all tagged frames entering or exiting the interface, include the **pop** statement in the input VLAN map or output VLAN map:

```
pop;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

---

## Removing the Outer and Inner VLAN Tags

On Ethernet IQ, IQ2 and IQ2-E interfaces, on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series

routers, to remove both the outer and inner VLAN tags of the frame, include the **pop-pop** statement in the input VLAN map or output VLAN map:

**pop-pop;**

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

See Table 10 on page 126 and Table 11 on page 126 for information about configuring inner and outer VLAN ID values and inner and outer TPID values required for VLAN maps.

---

## Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag

On Ethernet IQ, IQ2 and IQ2-E interfaces, on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, to remove the outer VLAN tag of the frame and replace the inner VLAN tag of the frame with a user-specified VLAN tag value, include the **pop-swap** statement in the input VLAN map or output VLAN map:

**pop-swap;**

The inner tag becomes the outer tag in the final frame.

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

See Table 10 on page 126 and Table 11 on page 126 for information about configuring inner and outer VLAN ID values and inner and outer TPID values required for VLAN maps.

---

## Stacking Two VLAN Tags

On Ethernet IQ, IQ2 and IQ2-E interfaces, on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, to push two VLAN tags in front of tagged frames entering or exiting the interface, include the **push-push** statement in the input VLAN map or the output VLAN map:

**push-push;**

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

See Table 10 on page 126 and Table 11 on page 126 for information about configuring inner and outer VLAN ID values and inner and outer TPID values required for VLAN maps.

---

## Rewriting the VLAN Tag on Tagged Frames

---

To rewrite the VLAN tag on all tagged frames entering the interface to a specified VLAN ID and TPID, include the **swap**, **tag-protocol-id**, and **vlan-id** statements in the input VLAN map:

```
input-vlan-map {  
    swap;  
    vlan-id number;  
    tag-protocol-id tpid;  
}
```

To rewrite the VLAN tag on all tagged frames exiting the interface to a specified VLAN ID and TPID, include the **swap** and **tag-protocol-id** statements in the output VLAN map:

```
output-vlan-map {  
    swap;  
    vlan-id number;  
    tag-protocol-id tpid;  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]

You cannot include both the **swap** statement and the **vlan-id** statement in the output VLAN map configuration. If you include the **swap** statement in the configuration, the VLAN ID in outgoing frames is rewritten to the VLAN ID bound to the logical interface. For more information about binding a VLAN ID to the logical interface, see “802.1Q VLANs Overview” on page 47.

The swap operation works on the outer tag only, whether or not you include the **stacked-vlan-tagging** statement in the configuration. For more information, see “Examples: Stacking and Rewriting Gigabit Ethernet IQ VLAN Tags” on page 134.

## Rewriting a VLAN Tag on Untagged Frames

On M320, M120, and MX Series routers with Gigabit Ethernet IQ, IQ2, and IQ2E PICs, 10-Gigabit Ethernet IQ, IQ2, and IQ2E PICs, and on MX Series 40-port Gigabit Ethernet R, 40-port Gigabit Ethernet R EQ, 4-port 10-Gigabit Ethernet R, and 4-port 10-Gigabit Ethernet R EQ DPCs, you can rewrite VLAN tags on untagged incoming and outgoing frames under **ethernet-ccc** and **ethernet-vpls** encapsulations. On MX Series routers with IQ2 and IQ2-E PICs, you can perform all rewrite VLAN tag operations. These features provide added flexibility.

Consider a network where two provider edges (PE) are connected by a Layer 2 circuit. PE1 is receiving traffic on an untagged port while the corresponding port on PE2 is tagged. In the normal case, packets coming from PE1 will be dropped at PE2 because it is expecting tagged packets. However, if PE1 can push a VLAN tag on the incoming packet before sending it across to PE2, you can ensure that packets are not dropped. To make it work in both directions, PE1 must strip the VLAN tag from outgoing packets. Therefore, a push on the ingress side is always paired with a pop on the egress side.

The rewrite operations represented by the following statement options are supported under **ethernet-ccc** and **ethernet-vpls** encapsulations:

- **push**—A VLAN tag is added to the incoming untagged frame.
- **pop**—VLAN tag is removed from the outgoing frame.
- **push-push**—An outer and inner VLAN tag are added to the incoming untagged frame.
- **pop-pop**—Both the outer and inner VLAN tags of the outgoing frame are removed.

IQ2 and 10-Gigabit Ethernet PICs support all rewrite operations described above. Details on the possible combinations of usage are explained later in this section.



**NOTE:** The **push-push** and **pop-pop** operations are not supported on the Gigabit Ethernet IQ PIC.

For the **input-vlan-map** statement, only the **push** and **push-push** options are supported because it does not make sense to remove a VLAN tag from an incoming untagged frame. Similarly, only the **pop** and **pop-pop** options are supported for the **output-vlan-map** statement. Also, with the **push** and **push-push** options, the tag parameters have to be explicitly specified. Apart from this, the other rules for configuring the **input-vlan-map** and **output-vlan-map** statements are the same as for tagged frames. Table 12 on page 132 through Table 14 on page 132 explain the rules in more detail.

For the **input-vlan-map** statement, only the **push** and **push-push** options are supported because it does not make sense to remove a VLAN tag from an incoming untagged frame. Similarly, only the **pop** and **pop-pop** options are supported for the **output-vlan-map** statement. Also, with the **push** and **push-push** options, the **vlan-id** parameters (**vlan-id** for **push** and **vlan-id** or **inner-vlan-id** for **push-push**) have to be explicitly specified. TPID however, is optional and the default value of **0x8100** is set if not configured. Apart from

this, the other rules for configuring the **input-vlan-map** and **output-vlan-map** statements are the same as for tagged frames.

**Table 12: Input VLAN Map Statements Allowed for ethernet-ccc and ethernet-vpls Encapsulations**

Operation	vlan-id	tag-protocol-id	inner-vlan-id	inner-tag-protocol-id
<b>push</b>	Yes	Optional	No	Optional
<b>push-push</b>	Yes	Optional	Yes	Optional

**Table 13: Output VLAN Map Statements Allowed for ethernet-ccc and ethernet-vpls Encapsulations**

Operation	vlan-id	tag-protocol-id	inner-vlan-id	inner-tag-protocol-id
<b>pop</b>	No	No	No	No
<b>pop-pop</b>	No	No	No	No

**Table 14: Rules for Applying Rewrite Operations to VLAN Maps**

Output VLAN Map				
Input VLAN Map	None	pop	pop-pop	
<b>None</b>	Yes	No	No	
<b>push</b>	No	Yes	No	
<b>push-push</b>	No	No	Yes	

**Example: push and pop with Ethernet CCC Encapsulation**

```
ge-3/1/0 {
  encapsulation ethernet-ccc;
  unit 0 {
    encapsulation ethernet-ccc;
    input-vlan-map {
      push;
      tag-protocol-id 0x8100;
      vlan-id 600;
    }
    output-vlan-map pop;
    family ccc;
  }
}
```

**Example: push-push and pop-pop with Ethernet CCC Encapsulation**

```
ge-3/1/0 {
  encapsulation ethernet-ccc;
  unit 0 {
    encapsulation ethernet-ccc;
    input-vlan-map {
```



```

        push-push;
        tag-protocol-id 0x8100;
        inner-tag-protocol-id 0x8100;
        vlan-id 600;
        inner-vlan-id 575;
    }
    output-vlan-map pop-pop;
    family ccc;
}
}

```

**Example: push and pop  
with Ethernet VPLS  
Encapsulation**

```

ge-3/1/0 {
    encapsulation ethernet-vpls;
    unit 0 {
        encapsulation ethernet-vpls;
        input-vlan-map {
            push;
            tag-protocol-id 0x8100;
            vlan-id 700;
        }
        output-vlan-map pop;
        family vpls;
    }
}

```

**Example: push-push  
and pop-pop with  
Ethernet VPLS  
Encapsulation**

```

ge-3/1/0 {
    encapsulation ethernet-vpls;
    unit 0 {
        encapsulation ethernet-vpls;
        input-vlan-map {
            push-push;
            tag-protocol-id 0x8100;
            inner-tag-protocol-id 0x8100;
            vlan-id 600;
            inner-vlan-id 575;
        }
        output-vlan-map pop-pop;
        family vpls;
    }
}

```

You can use the **show interface *interface-name*** command to display the status of a modified VLAN map for the specified interface.

## Rewriting a VLAN Tag and Adding a New Tag

On Ethernet IQ, IQ2 and IQ2-E interfaces, on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, to replace the outer VLAN tag of the incoming frame with a user-specified VLAN tag value, include the **swap-push** statement in the input VLAN map or output VLAN map:

```

swap-push

```

A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

See Table 10 on page 126 and Table 11 on page 126 for information about configuring inner and outer VLAN ID values and inner and outer TPID values required for VLAN maps.

---

## Rewriting the Inner and Outer VLAN Tags

On Ethernet IQ, IQ2 and IQ2-E interfaces, on MX Series router Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, and on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, to replace both the inner and the outer VLAN tags of the incoming frame with a user-specified VLAN tag value, include the **swap-swap** statement in the input VLAN map or output VLAN map:

```
swap-swap;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit interfaces *interface-name* unit *logical-unit-number* output-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

See Table 10 on page 126 and Table 11 on page 126 for information about configuring inner and outer VLAN ID values and inner and outer TPID values required for VLAN maps.

---

## Examples: Stacking and Rewriting Gigabit Ethernet IQ VLAN Tags

Configure a VLAN CCC tunnel in which Ethernet frames enter the tunnel at interface **ge-4/0/0** and exit the tunnel at interface **ge-4/2/0**.

The following examples show how to perform the following tasks:

- Push a TPID and VLAN ID Pair on Ingress on page 135
- Stack Inner and Outer VLAN Tags on page 136
- Swap a VLAN ID on Ingress on page 136

- Swap a VLAN ID on Egress on page 137
- Swap a VLAN ID on Both Ingress and Egress on page 138
- Swap the Outer VLAN Tag and Push a New VLAN Tag on Ingress; Pop the Outer VLAN Tag and Swap the Inner VLAN Tag on Egress on page 138
- Swap a TPID and VLAN ID Pair for Both VLAN Tags on Ingress and on Egress on page 139
- Pop the Outer VLAN Tag and Swap the Inner VLAN Tag on Ingress; Swap the Outer VLAN Tag and Push a New VLAN Tag on Egress on page 139
- Pop a TPID and VLAN ID Pair on Ingress; Push a VLAN ID and TPID Pair on Egress on page 140
- Pop an Outer VLAN Tag to Connect an Untagged VPLS Interface to Tagged VPLS Interfaces on page 140

**Push a TPID and VLAN  
ID Pair on Ingress**

```
[edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id 0x9909;
    }
  }
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 512;
    input-vlan-map {
      push;
      tag-protocol-id 0x9909;
      vlan-id 520;
    }
    output-vlan-map pop;
  }
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 515;
    input-vlan-map {
      swap-push;
      vlan-id 520;
      inner-vlan-id 512;
    }
    output-vlan-map {
      pop-swap;
    }
  }
}
[edit protocols]
mpls {
  interface ge-4/0/0.0;
  interface ge-4/2/0.0;
```

```
    }
    connections {
      interface-switch vlan-tag-push {
        interface ge-4/0/0.0;
        interface ge-4/2/0.0;
      }
    }
  }
}
```

**Stack Inner and Outer  
VLAN Tags**

```
[edit interfaces]
ge-0/2/0 {
  stacked-vlan-tagging;
  mac 00.01.02.03.04.05;
  gigether-options {
    loopback;
  }
  unit 0 {
    vlan-tags outer 0x8100.200 inner 0x8100.200;
  }
}
```

**Swap a VLAN ID on  
Ingress**

```
[edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id 0x9100;
    }
  }
}
...
unit 1 {
  encapsulation vlan-ccc;
  vlan-id 1000;
  input-vlan-map {
    swap;
    tag-protocol-id 0x9100;
    vlan-id 2000;
  }
}
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 2000;
    input-vlan-map {
      swap;
      tag-protocol-id 0x9100;
      vlan-id 1000;
    }
  }
}
[edit protocols]
```

```

mpls {
  ...
  interface ge-4/0/0.1;
  interface ge-4/2/0.1;
}
connections {
  ...
  interface-switch vlan-tag-swap {
    interface ge-4/2/0.1;
    interface ge-4/0/0.1;
  }
}
}

Swap a VLAN ID on Egress [edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 1000;
  }
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id 0x8800;
    }
  }
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 2000;
    output-vlan-map {
      swap;
      tag-protocol-id 0x8800;
    }
  }
}
[edit protocols]
mpls {
  ...
  interface ge-4/0/0.1;
  interface ge-4/2/0.1;
}
connections {
  ...
  interface-switch vlan-tag-swap {
    interface ge-4/2/0.1;
    interface ge-4/0/0.1;
  }
}
}

```

**Swap a VLAN ID on  
Both Ingress and  
Egress**

```
[edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id [ 0x8800 0x9100 ];
    }
  }
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 1000;
    input-vlan-map {
      swap;
      tag-protocol-id 0x9100;
      vlan-id 2000;
    }
  }
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id [ 0x8800 0x9100 ];
    }
  }
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 2000;
    output-vlan-map {
      swap;
      tag-protocol-id 0x8800;
    }
  }
}
[edit protocols]
mpls {
  ...
  interface ge-4/0/0.1;
  interface ge-4/2/0.1;
}
connections {
  ...
  interface-switch vlan-tag-swap {
    interface ge-4/2/0.1;
    interface ge-4/0/0.1;
  }
}
```

**Swap the Outer VLAN  
Tag and Push a New  
VLAN Tag on Ingress;  
Pop the Outer VLAN**

```
[edit interfaces]
ge-1/1/0 {
  unit 1 {
    vlan-id 200;
  }
}
```

**Tag and Swap the  
Inner VLAN Tag on  
Egress**

```
input-vlan-map {
    swap-push;
    tag-protocol-id 0x9100;
    vlan-id 400;
    inner-tag-protocol-id 0x9100;
    inner-vlan-id 500;
}
output-vlan-map {
    pop-swap;
    inner-tag-protocol-id 0x9100;
}
}
```

**Swap a TPID and VLAN  
ID Pair for Both VLAN  
Tags on Ingress and on  
Egress**

```
[edit interfaces]
ge-1/1/0 {
    unit 0 {
        vlan-tags {
            inner 0x9100.425;
            outer 0x9200.525;
        }
        input-vlan-map {
            swap-swap;
            tag-protocol-id 0x9100;
            vlan-id 400;
            inner-tag-protocol-id 0x9100;
            inner-vlan-id 500;
        }
        output-vlan-map {
            swap-swap;
            tag-protocol-id 0x9200;
            inner-tag-protocol-id 0x9100;
        }
    }
}
```

**Pop the Outer VLAN  
Tag and Swap the  
Inner VLAN Tag on  
Ingress; Swap the  
Outer VLAN Tag and  
Push a New VLAN Tag  
on Egress**

```
[edit interfaces]
ge-1/1/0 {
    unit 0 {
        vlan-tags {
            inner 0x9100.425;
            outer 0x9200.525;
        }
        input-vlan-map {
            pop-swap;
            tag-protocol-id 0x9100;
            vlan-id 400;
        }
        output-vlan-map {
            swap-push;
            tag-protocol-id 0x9200;
            inner-tag-protocol-id 0x9100;
        }
    }
}
```

**Pop a TPID and VLAN ID Pair on Ingress; Push a VLAN ID and TPID Pair on Egress**

```
[edit interfaces]
ge-1/1/0 {
  unit 0 {
    vlan-tags {
      inner 0x9100.425;
      outer 0x9200.525;
    }
    input-vlan-map {
      pop-pop;
    }
    output-vlan-map {
      push-push;
      tag-protocol-id 0x9200;
      inner-tag-protocol-id 0x9100;
    }
  }
}
```

**Pop an Outer VLAN Tag to Connect an Untagged VPLS Interface to Tagged VPLS Interfaces**

```
[edit interfaces]
ge-1/1/0 {
  vlan-tagging;
  encapsulation extended-vlan-vpls;
  unit 0 {
    vlan-id 0;
    input-vlan-map {
      push;
      vlan-id 0;
    }
    output-vlan-map pop;
    family vpls;
  }
}
```



## CHAPTER 6

# Configuring Layer 2 Bridging Interfaces

- Layer 2 Bridging Interfaces Overview on page 141
- Configuring Layer 2 Bridging Interfaces on page 141

## Layer 2 Bridging Interfaces Overview

---

Bridging operates at Layer 2 of the OSI reference model while routing operates at Layer 3. A set of logical ports configured for bridging can be said to constitute a bridging domain.

A bridging domain can be created by configuring a routing instance and specifying the instance-type as **bridge**.

Integrated routing and bridging (IRB) is the ability to:

- Route a packet if the destination MAC address is the MAC address of the router and the packet **ethertype** is IPv4, IPv6, or MPLS.
- Switch all multicast and broadcast packets within a bridging domain at layer 2.
- Route a copy of the packet if the destination MAC address is a multicast address and the **ethertype** is IPv4 or IPv6.
- Switch all other unicast packets at Layer 2.
- Handle supported Layer 2 control packets such as STP and LACP.
- Handle supported Layer 3 control packets such as OSPF and RIP.

## Configuring Layer 2 Bridging Interfaces

---

You can configure an IRB logical interface at the **[edit interfaces ge-fpc /pic/port unit logical-unit-number]** hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
unit logical-unit-number {
}
```

You can configure Layer 3 information on the IRB logical interface by including the **irb** statement at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
irb {
```

```
    unit logical-unit-number {  
      family inet {  
        address address {  
        }  
      }  
    }  
  }  
}
```

For examples of Layer 2 bridging configuration, see the [Junos OS Routing Protocols Configuration Guide](#).

## Example: Configuring Layer 2 Bridging Interfaces

The following example configures an IRB logical interface and Layer 3 information on the interface.

```
[edit interfaces]  
ge-1/0/0 {  
  unit 0 {  
  }  
}  
irb {  
  unit 0 {  
    family inet {  
      address 192.168.12.1/28;  
    }  
  }  
}
```

## CHAPTER 7

# Configuring TCC and Layer 2.5 Switching

- TCC and Layer 2.5 Switching Overview on page 143
- Configuring VLAN TCC Encapsulation on page 143
- Configuring Ethernet TCC on page 144

## TCC and Layer 2.5 Switching Overview

---

Translational cross-connect (TCC) is a switching concept that allows you to forward traffic between a variety of Layer 2 protocols or circuits. It is similar to its predecessor, CCC. However, while CCC requires the same Layer 2 encapsulations on both sides of a router (such as Point-to-Point Protocol [PPP] or Frame Relay-to-Frame Relay), TCC lets you connect different types of Layer 2 protocols interchangeably. With TCC, combinations such as PPP-to-ATM and Ethernet-to-Frame Relay cross-connections are possible.

## Configuring VLAN TCC Encapsulation

---

VLAN TCC encapsulation allows circuits to have different media on either side of the forwarding path. VLAN TCC encapsulation supports TPID 0x8100 only. You must include configuration statements at the logical and physical interface hierarchy levels.

To configure VLAN TCC encapsulation, include the **encapsulation** statement and specify the **vlan-tcc** option:

```
[edit interfaces interface-name unit logical-unit-number]  
encapsulation vlan-tcc;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* ]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* ]

Additionally, configure the logical interface by including the **proxy** and **remote** statements:

```
proxy {  
    inet-address;  
}  
remote {
```

```
(inet-address | mac-address);  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family tcc]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family tcc]

The proxy address is the IP address of the non-Ethernet TCC neighbor for which the TCC router is acting as a proxy.

The remote address is the IP or MAC address of the remote router. The **remote** statement provides ARP capability from the TCC switching router to the Ethernet neighbor. The MAC address is the physical Layer 2 address of the Ethernet neighbor.

When VLAN TCC encapsulation is configured on the logical interface, you also must specify flexible Ethernet services on the physical interface. To specify flexible Ethernet services, include the **encapsulation** statement at the [edit interfaces *interface-name*] hierarchy level and specify the **flexible-ethernet-services** option:

```
[edit interfaces interface-name]  
encapsulation flexible-ethernet-services;
```

Extended VLAN TCC encapsulation supports TPIDs 0x8100 and 0x9901. Extended VLAN TCC is specified at the physical interface level. When configured, all units on that interface must use VLAN TCC encapsulation, and no explicit configuration is needed on logical interfaces.

One-port Gigabit Ethernet, 2-port Gigabit Ethernet, and 4-port Fast Ethernet PICs with VLAN tagging enabled can use VLAN TCC encapsulation. To configure the encapsulation on a physical interface, include the **encapsulation** statement at the [edit interfaces *interface-name*] hierarchy level and specify the **extended-vlan-tcc** option:

```
[edit interfaces interface-name]  
encapsulation extended-vlan-tcc;
```

For VLAN TCC encapsulation, all VLAN IDs from 1 through 1024 are valid. VLAN ID 0 is reserved for tagging the priority of frames.

Extended VLAN TCC is not supported on 4-port Gigabit Ethernet PICs.

---

## Configuring Ethernet TCC

For Layer 2.5 virtual private networks (VPNs) using an Ethernet interface as the TCC router, you can configure an Ethernet TCC.

To configure an Ethernet TCC, include the **encapsulation** statement and specify the **ethernet-tcc** option at the [edit interfaces *interface-name*] hierarchy level:

```
[edit interfaces interface-name]  
encapsulation ethernet-tcc;
```

For Ethernet TCC encapsulation, you must also configure the logical interface by including the **proxy** and **remote** statements:

```
proxy {
  inet-address;
}
remote {
  (inet-address | mac-address);
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family *tcc*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *tcc*]

The proxy address is the IP address of the non-Ethernet TCC neighbor for which the TCC router is acting as a proxy.

The remote address is the IP or MAC address of the remote router. The **remote** statement provides ARP capability from the TCC switching router to the Ethernet neighbor. The MAC address is the physical Layer 2 address of the Ethernet neighbor.

Ethernet TCC is supported on interfaces that carry IPv4 traffic only. For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC and extended VLAN CCC are not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC and extended VLAN TCC are not supported.

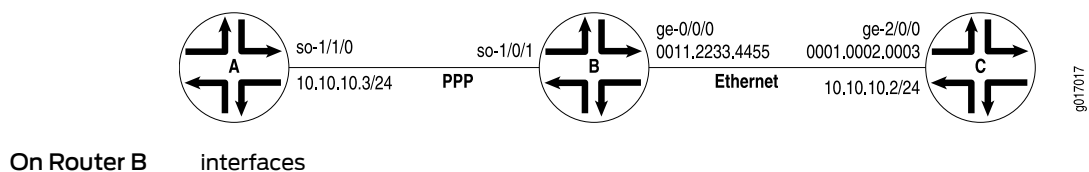
### Example: Configuring an Ethernet TCC or Extended VLAN TCC

Configure a full-duplex Layer 2.5 translational cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the TCC interface. Ethernet TCC encapsulation provides an Ethernet wide area circuit for interconnecting IP traffic. (See the topology in Figure 15 on page 145.)

The Router A-to-Router B circuit is PPP, and the Router B-to-Router C circuit accepts packets carrying standard TPID values.

If traffic flows from Router A to Router C, the Junos OS strips all PPP encapsulation data from incoming packets and adds Ethernet encapsulation data before forwarding the packets. If traffic flows from Router C to Router A, the Junos OS strips all Ethernet encapsulation data from incoming packets and adds PPP encapsulation data before forwarding the packets.

Figure 15: Topology of Layer 2.5 Translational Cross-Connect



Configure a full-duplex Layer 2.5 translational cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the TCC interface. Extended VLAN TCC encapsulation provides an Ethernet wide area circuit for interconnecting IP traffic. (See the topology in Figure 15 on page 145.)

**Configuring an Extended VLAN TCC** The Router A-to-Router B circuit is PPP, and the Router B-to-Router C circuit is Ethernet with VLAN tagging enabled.

```
On Router B interfaces
ge-0/0/0 {
  vlan-tagging;
  encapsulation extended-vlan-tcc;
  unit 0 {
    vlan-id 1;
    family tcc {
      proxy {
        inet-address 10.10.10.3;
      }
      remote {
        inet-address 10.10.10.2;
      }
    }
  }
}
```

## CHAPTER 8

# Configuring Static ARP Table Entries

- Static ARP Table Entries Overview on page 147
- Configuring Static ARP Table Entries on page 147

## Static ARP Table Entries Overview

---

For Fast Ethernet, Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces, you can configure static ARP table entries, defining mappings between IP and MAC addresses.

## Configuring Static ARP Table Entries

---

To configure static ARP table entries, include the **arp** statement:

```
arp ip-address (mac | multicast-mac) mac-address <publish>;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address*]

The IP address that you specify must be part of the subnet defined in the enclosing **address** statement.

To associate a multicast MAC address with a unicast IP address, include the **multicast-mac** statement.

Specify the MAC address as six hexadecimal bytes in one of the following formats: *nnnn.nnnn.nnnn* or *nn:nn:nn:nn:nn:nn*; for example, **0011.2233.4455** or **00:11:22:33:44:55**.

For unicast MAC addresses only, if you include the **publish** option, the router or switch replies to proxy ARP requests.



**NOTE:** By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the family inet statement. By including the arp statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet policer] hierarchy level, you can apply a specific ARP-packet policer to an interface. This feature is not available on EX Series switches.

When you need to conserve IP addresses, you can configure an Ethernet interface to be unnumbered by including the unnumbered-address statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level.



**NOTE:** The Junos OS supports the IPv6 static neighbor discovery cache entries, similar to the static ARP entries in IPv4.

---

### Example: Configuring Static ARP Table Entries

Configure two static ARP table entries on the router or switch's management interface:

```
[edit interfaces]
fxp0 {
  unit 0 {
    family inet {
      address 10.10.0.11/24 {
        arp 10.10.0.99 mac 0001.0002.0003;
        arp 10.10.0.101 mac 00:11:22:33:44:55 publish;
      }
    }
  }
}
```

- Related Documentation**
- Applying Policers
  - Configuring an Unnumbered Interface



## CHAPTER 9

# Configuring Unrestricted Proxy ARP

- Unrestricted Proxy ARP Overview on page 149
- Configuring Unrestricted Proxy ARP on page 150

## Unrestricted Proxy ARP Overview

---

By default, the Junos OS responds to an ARP request only if the destination address of the ARP request is local to the incoming interface.

For Ethernet interfaces, you can configure unrestricted proxy ARP, which enables the router to respond to any ARP request, on condition that the router has an active route to the destination address of the ARP request. The route is not limited to the incoming interface of the request, nor is it required to be a direct route.

You might want to configure unrestricted proxy ARP for routers that are acting as provider edge (PE) devices in Ethernet Layer 2 LAN switching domains.



**WARNING:** If you configure unrestricted proxy ARP, the proxy router replies to ARP requests for the target IP address on the same interface as the incoming ARP request. This behavior is appropriate for cable modem termination system (CMTS) environments, but might cause Layer 2 reachability problems if you enable unrestricted proxy ARP in other environments.

When an IP client broadcasts the ARP request across the Ethernet wire, the end node with the correct IP address responds to the ARP request and provides the correct MAC address. If the unrestricted proxy ARP feature is enabled, the router response is redundant and might fool the IP client into determining that the destination MAC address within its own subnet is the same as the address of the router.

While the destination address can be remote, the source address of the ARP request must be on the same subnet as the interface upon which the ARP request is received. For security reasons, this rule applies to both unrestricted and restricted proxy ARP.

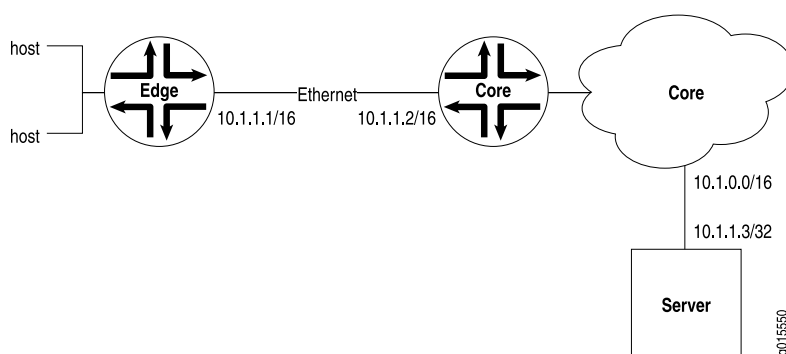
In most situations, you should not configure the router to perform unrestricted proxy ARP. Do so only for special situations, such as when cable modems are used. Figure 16 on

page 150 and Figure 17 on page 150 show examples of situations in which you might want to configure unrestricted proxy ARP.

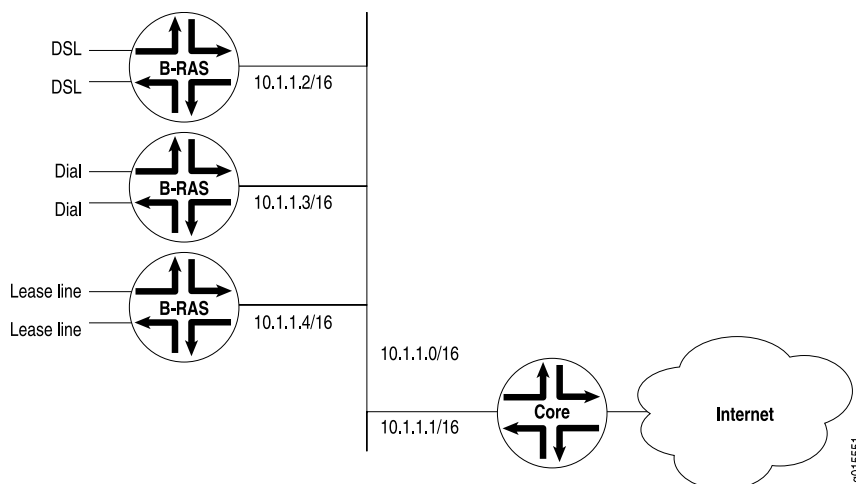
In Figure 16 on page 150, the edge device is not running any IP protocols. In this case, you configure the core router to perform unrestricted proxy ARP. The edge device is the client of the proxy.

In Figure 17 on page 150, the Broadcast Remote Access Server (B-RAS) routers are not running any IP protocols. In this case, you configure unrestricted proxy ARP on the B-RAS interfaces. This allows the core device to behave as though it is directly connected to the end users.

**Figure 16: Edge Device Case for Unrestricted Proxy ARP**



**Figure 17: Core Device Case for Unrestricted Proxy ARP**



## Configuring Unrestricted Proxy ARP

To configure unrestricted proxy ARP, include the **proxy-arp** statement:

```
proxy-arp;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* ]**

- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

To return to the default—that is, to disable unrestricted proxy ARP—delete the **proxy-arp** statement from the configuration:

```
[edit]
```

```
user@host# delete interfaces interface-name unit logical-unit-number proxy-arp
```

You can track the number of unrestricted proxy ARP requests processed by the router or switch by issuing the **show system statistics arp** operational mode command.



**NOTE:** When proxy ARP is enabled as default or unrestricted, the router responds to any ARP request as long as the router has an active route to the target address of the ARP request. This gratuitous ARP behavior can result in an error when the receiving interface and target response interface are the same and the end device (for example, a client) performs a duplicate address check. To prevent this error, configure the router interface with the **no-gratuitous-arp-reply** statement. See “Configuring Gratuitous ARP” on page 42 for information on how to disable responses to gratuitous ARP requests.



## CHAPTER 10

# Configuring MAC Address Validation on Static Ethernet Interfaces

- MAC Address Validation on Static Ethernet Interfaces Overview on page 153
- Configuring MAC Address Validation on Static Ethernet Interfaces on page 153
- Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors on page 154

### MAC Address Validation on Static Ethernet Interfaces Overview

---

MAC address validation enables the router to validate that received packets contain a trusted IP source and an Ethernet MAC source address.

MAC address validation is supported on AE, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces (with or without VLAN tagging) on MX Series routers only.

There are two types of MAC address validation that you can configure:

- Loose—Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not support the MAC address of the tuple

Continues to forward packets when the source address of the incoming packet does not match any of the trusted IP addresses.

- Strict—Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.

### Configuring MAC Address Validation on Static Ethernet Interfaces

---

To configure MAC address validation on static Ethernet interfaces, include the **mac-validate** (**loose** | **strict**) statement in the **[edit interfaces *interface-name* unit *logical-unit-number* family *family*]** hierarchy:

```
[edit interfaces interface-name unit logical-unit-number family family]  
mac-validate (loose | strict);
```

## Example of Strict MAC Validation on a Static Ethernet Interface

This example shows strict MAC address validation on a static Ethernet interface without VLAN tagging.

```
[edit interfaces]  
ge-2/1/9 {  
  unit 0 {  
    proxy-arp;  
    family inet {  
      mac-validate strict;  
      address 88.22.100.1/24 {  
        arp 88.22.100.3 mac 00:00:58:16:64:03;  
      }  
    }  
  }  
}
```

## Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors

---

The Junos OS provides the **no-neighbor-learn** configuration statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet]** and **[edit interfaces *interface-name* unit *interface-unit-number* family inet6]** hierarchy levels.

To disable ARP address learning by not sending arp-requests and not learning from ARP replies for IPv4 neighbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet]** hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet]  
no-neighbor-learn;
```

To disable neighbor discovery for IPv6 neighbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet6]** hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet6]  
no-neighbor-learn;
```

### Related Documentation

- [Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses](#)

# Enabling Passive Monitoring on Ethernet Interfaces

- Passive Monitoring on Ethernet Interfaces Overview on page 155
- Enabling Passive Monitoring on Ethernet Interfaces on page 156

## Passive Monitoring on Ethernet Interfaces Overview

---

The Monitoring Services I and Monitoring Services II PICs are designed to enable IP services. You can monitor IPv4 traffic if you have a Monitoring Services PIC installed in the router with the following PICs:

- 4-port Gigabit Ethernet PIC with SFPs
- 10-port Gigabit Ethernet PIC with SFPs
- 2-port Gigabit Ethernet PIC with SFPs
- 1-port 10-Gigabit Ethernet PIC



**NOTE:** The PICs listed above only support IPv4.

- 4-port 10-Gigabit Ethernet LAN/WAN PIC with XFP (T640 and T1600) (Supported on both WAN-PHY and LAN-PHY mode for both IPv4 and IPv6 addresses)

IPv4 Passive monitoring is also supported on Gigabit and 10-Gigabit Ethernet Interfaces on MX Series Universal Edge Routers.

In Junos OS Release 11.2 and later, interfaces configured on the following FPCs and PIC support IPv6 passive monitoring on the T640 and T1600:

- Enhanced Scaling FPC2
- Enhanced Scaling FPC3
- Enhanced Scaling FPC4
- Enhanced Scaling FPC4.1
- Enhanced II FPC1

- Enhanced II FPC2
- Enhanced II FPC3
- 4-port 10-Gigabit Ethernet LAN/WAN PIC with XFP (Supported on both WAN-PHY and LAN-PHY mode for both IPv4 and IPv6 addresses)



**NOTE:** Unlike IPv4 passive monitoring, IPv6 passive monitoring is not supported on Monitoring Services PICs. Users must configure port mirroring to forward the packets from the passive monitored ports to other interfaces.

**Related  
Documentation**

- Passive Monitoring on Ethernet Interfaces Overview on page 155

---

## Enabling Passive Monitoring on Ethernet Interfaces

---

On Ethernet interfaces, enable packet flow monitoring by including the **passive-monitor-mode** statement at the **[edit interfaces *interface-name* ]** hierarchy level:

```
[edit interfaces interface-name]  
passive-monitor-mode;
```

When you configure an interface in passive monitoring mode, the Packet Forwarding Engine silently drops packets coming from that interface and destined to the router itself. Passive monitoring mode also stops the Routing Engine from transmitting any packet from that interface. Packets received from the monitored interface can be forwarded to monitoring interfaces. If you include the **passive-monitor-mode** statement in the configuration:

- Gigabit and Fast Ethernet interfaces can support both per-port passive monitoring and per-VLAN passive monitoring. The destination MAC filter on the receive port of the Ethernet interfaces is disabled.
- Ethernet encapsulation options are not allowed.
- Ethernet interfaces do not support the **stacked-vlan-tagging** statement for both IPv4 and IPv6 packets in passive monitor mode.

For IPv4 monitoring services interfaces, enable packet flow monitoring by including the **family** statement at the **[edit interfaces *mo-fpc/pic/port unit logical-unit-number* ]** hierarchy level, specifying the **inet** option:

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number]  
family inet;
```

For conformity with cflowd record structure, you must include the **receive-options-packets** and **receive-ttl-exceeded** statements at the **[edit interfaces *mo-fpc/pic/port unit logical-unit-number* family inet]** hierarchy level:

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number family inet]  
receive-options-packets;  
receive-ttl-exceeded;
```



IPv6 passive monitoring is not supported on monitoring services PICs. A user must configure port mirroring to forward the packets from the passive monitored ports to other interfaces. In Junos OS Release 11.2 and later, interfaces configured on the following FPCs and PIC support IPv6 passive monitoring on the T640 and T1600:

- Enhanced Scaling FPC2
- Enhanced Scaling FPC3
- Enhanced II FPC1
- Enhanced II FPC2
- Enhanced II FPC3
- Enhanced Scaling FPC4
- Enhanced Scaling FPC4.1
- 4-port 10-Gigabit Ethernet LAN/WAN PIC with XFP (Supported on both WAN-PHY and LAN-PHY mode for both IPv4 and IPv6 addresses)

To configure port mirroring, include the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level.

For the monitoring services interface, you can configure multiservice physical interface properties. For more information, see [Configuring Multiservice Physical Interface Properties](#) and the [Junos OS Services Interfaces Configuration Guide](#).



## CHAPTER 12

# Configuring IEEE 802.1ag OAM Connectivity-Fault Management

- IEEE 802.1ag OAM Connectivity Fault Management Overview on page 159
- Creating the Maintenance Domain on page 161
- Configuring Maintenance Intermediate Points on page 162
- Creating a Maintenance Association on page 163
- Continuity Check Protocol on page 164
- Configuring a Maintenance Endpoint on page 166
- Configuring a Connectivity Fault Management Action Profile on page 170
- Configuring Linktrace Protocol in CFM on page 173
- Configuring Ethernet Local Management Interface on page 173
- Configuring Port Status TLV and Interface Status TLV on page 180
- Configuring MAC Flush Message Processing in CET Mode on page 192
- Configuring M120 and MX Series Routers for CCC Encapsulated Packets on page 195
- Configuring Rate Limiting of Ethernet OAM Messages on page 196
- Configuring 802.1ag Ethernet OAM for VPLS on page 198

## IEEE 802.1ag OAM Connectivity Fault Management Overview

---

Ethernet interfaces on M7i and M10i routers with the Enhanced CFEB (CFEB-E) and on M120, M320, MX Series, and T Series routers support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity-fault management (CFM). The goal of CFM is to monitor an Ethernet network that may comprise one or more service instances. Junos OS supports IEEE 802.1ag connectivity fault management.

In Junos OS Release 9.3 and later, CFM also supports aggregated Ethernet interfaces. On interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers, CFM is not supported on untagged aggregated Ethernet member links. MPCs and MICs do support CFM on untagged and tagged aggregated Ethernet logical interfaces.

Network entities such as operators, providers, and customers may be part of different administrative domains. Each administrative domain is mapped into one maintenance domain. Maintenance domains are configured with different level values to keep them separate. Each domain provides enough information for the entities to perform their own management, perform end-to-end monitoring, and still avoid security breaches.



**NOTE:** As a requirement for Ethernet OAM 802.1ag to work, distributed periodic packet management (PPM) runs on the Routing Engine and Packet Forwarding Engine (PFE) by default. You can only disable PPM on the PFE. To disable PPM on the PFE, include the `ppm no-delegate-processing` statement at the `[edit routing-options ppm]` hierarchy level.

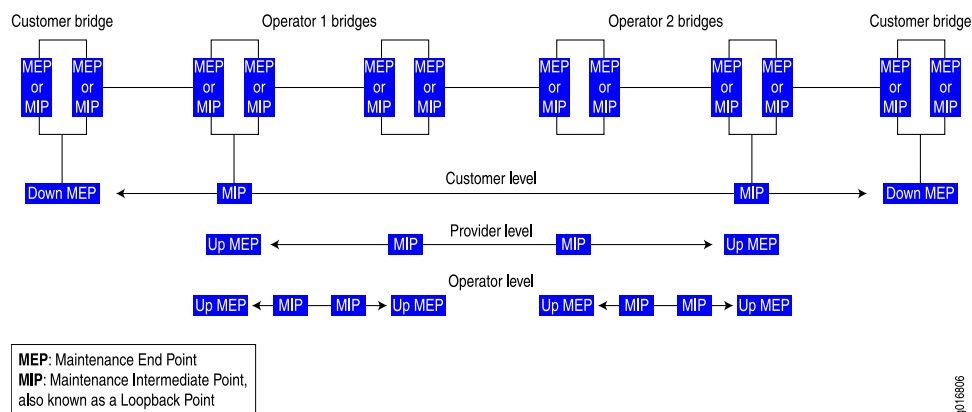
IEEE 802.1ag OAM supports graceful Routing Engine switchover (GRES). IEEE 802.1ag OAM is supported on untagged, single tagged, and stacked VLAN interfaces.

- Connectivity Fault Management Key Elements on page 160

## Connectivity Fault Management Key Elements

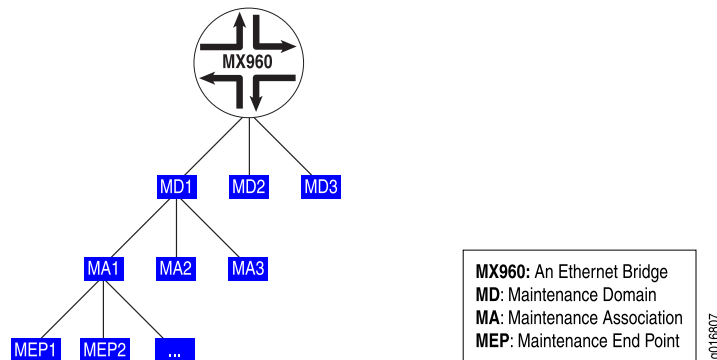
Figure 18 on page 160 shows the relationships among the customer, provider, and operator Ethernet bridges, maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs).

**Figure 18: Relationship Among MEPs, MIPs, and Maintenance Domain Levels**



A maintenance association is a set of MEPs configured with the same maintenance association identifier and maintenance domain level. Figure 19 on page 161 shows the hierarchical relationships between the Ethernet bridge, maintenance domains, maintenance associations, and MEPs.

Figure 19: Relationship Among Bridges, Maintenance Domains, Maintenance Associations, and MEPs



## Creating the Maintenance Domain

To enable CFM on an Ethernet interface, maintenance domains, maintenance associations, and MEPs must be created and configured.

To create a maintenance domain, include the **maintenance-domain *domain-name*** statement at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

Give the maintenance domain a name. Names can be in one of several formats:

- Configuring the Maintenance Domain Name Format on page 161
- Configuring the Maintenance Domain Level on page 161

## Configuring the Maintenance Domain Name Format

You can specify the maintenance domain name format as one of the following:

- A plain ASCII character string.
- A domain name service (DNS) format, a MAC address plus a two-octet identifier in the range from 0 through 65,535, or none.
- A MAC address plus a two-octet identifier in the range from 0 through 65,535.
- Or none.

If none is specified, the maintenance domain name is not used.

The default name format is an ASCII character string.

To configure the maintenance domain name format, include the **name-format (character-string | none | dns | mac+2octet)** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]** hierarchy level.

## Configuring the Maintenance Domain Level

The maintenance domain level is a mandatory parameter that indicates the nesting relationship between various maintenance domains. The level is embedded in each of

the CFM frames. CFM messages within a given level are processed by MEPs at that same level. For example, the operator domain can be level 0, the provider domain can be level 3, and the customer domain can be level 7.

To configure the maintenance domain level, include the **level *number*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]** hierarchy level.

## Configuring Maintenance Intermediate Points

---

MX Series routers support maintenance intermediate points (MIPs) for the Ethernet OAM 802.1ag CFM protocol at a bridge-domain level. This enables you to define a maintenance domain for each default level. The MIPs names are created as **default-level-number** at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain]** hierarchy level. Use the **bridge-domain**, **instance**, **virtual-switch**, and **mip-half-function** MIP options to specify the MIP configuration.



**NOTE:** Whenever a MIP is configured and a bridge domain is mapped to multiple maintenance domains or maintenance associations, it is essential that the **mip-half-function** value for all maintenance domains and maintenance associations be the same.

To display MIP configurations, use the **show oam ethernet connectivity-fault-management mip (bridge-domain | instance-name | interface-name)** command.

The following sections describe MIP configuration:

- Configuring MIP for Bridge Domains of a Virtual Switch on page 162
- Configuring the Maintenance Domain Bridge Domain on page 163
- Configuring the Maintenance Domain Instance on page 163
- Configuring the Maintenance Domain MIP Half Function on page 163

### Configuring MIP for Bridge Domains of a Virtual Switch

The default maintenance domain configuration allows MIP configuration for bridge domains for a default virtual switch or a user-defined virtual switch. You can use the **virtual-switch** and **bridge-domain** statements to specify which MIPs to enable for a user-defined virtual switch.

A bridge domain must be specified by name only if it is configured by including the **vlan-id *id*** statement under the **virtual-switch** statement.

If a bridge domain is configured with a range of VLAN IDs, then the VLAN IDs must be explicitly listed after the bridge domain name.

To configure a bridge domain under a user-defined virtual switch, include the **virtual-switch *name*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* default-*x*]** hierarchy level.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  domain-name default-x]
virtual-switch name {
  bridge-domain {
    name-1;
    name-2 {
      vlan-id [vlan-ids ];
    }
  }
}
```

### Configuring the Maintenance Domain Bridge Domain

The VLAN corresponds to the bridge domain.

To configure the bridge domain for the default virtual switch, include the **bridge-domain** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *maintenance-domain-name*]** hierarchy level.

### Configuring the Maintenance Domain Instance

To configure the maintenance domain instance for a VPLS routing instance, include the **instance** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain]** hierarchy level.

### Configuring the Maintenance Domain MIP Half Function

MIP Half Function (MHF) divides MIP functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loopback and linktrace messages to help isolate faults.

Whenever a MIP is configured and a bridge domain is mapped to multiple maintenance domains or maintenance associations, it is essential that the *MIP half function* value for all maintenance domains and maintenance associations be the same. To configure the MIP half function, include the **mip-half-function** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain]** hierarchy level.

**Related Documentation**

- Configuring a Maintenance Endpoint on page 166

### Creating a Maintenance Association

To create a maintenance association, include the **maintenance-association *ma-name*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name*]** hierarchy level.

Maintenance association names can be in one of the following formats:

- As a plain ASCII character string
- As the VLAN identifier of the VLAN you primarily associate with the maintenance association
- As a two-octet identifier in the range from 0 through 65,535
- As a name in the format specified by RFC 2685

The default short name format is an ASCII character string.

To configure the maintenance association short name format, include the **short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id)** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association *ma-name*]** hierarchy level.

---

## Continuity Check Protocol

The continuity check protocol is used for fault detection by a MEP within a maintenance association. The MEP periodically sends continuity check multicast messages. The receiving MEPs use the continuity check messages to build a MEP database of all MEPs in the maintenance association.

The continuity check protocol packets use the ethertype value 0x8902 and the multicast destination MAC address 01:80:c2:00:00:32.

- Configuring the Continuity Check on page 164
- Configuring the Continuity Check Hold Interval on page 164
- Configuring the Continuity Check Interval on page 165
- Configuring the Continuity Check Loss Threshold on page 165
- Continuity Measurement on page 165

### Configuring the Continuity Check

You can configure the following continuity check protocol parameters:

- **hold-interval** *minutes*
- **interval** *time*
- **loss-threshold** *number*

To enable the continuity check protocol, include the **continuity-check** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association *ma-name*]** hierarchy level.

### Configuring the Continuity Check Hold Interval

You can specify the continuity check hold interval. The hold interval is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes.



The hold interval logic runs a polling timer per CFM session level (not per remote MEP level) where the polling timer duration is equal to the configured hold time. When the polling timer expires, it deletes all the auto discovered remote MEP entries which have been in the failed state for a time period equal to or greater than the configured hold time. If the remote MEP completes the hold time duration in the failed state, then flushing will not occur until the next polling timer expires. Hence remote MEP flushing may not happen exactly at the configured hold time.

To configure the hold interval, include the **hold-interval** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* continuity-check]** hierarchy level.



**NOTE:** Hold timer based flushing is applicable only for auto discovered remote MEPs and not for statically configured remote MEPs.

## Configuring the Continuity Check Interval

You can specify the continuity check message (CCM) interval. The interval is the time between the transmission of CCMs. You can specify 10 minutes (**10m**), 1 minute (**1m**), 10 seconds (**10s**), 1 second (**1s**), 100 milliseconds (**100ms**), or 10 milliseconds (**10ms**). The default value is 1 minute.



**NOTE:** For the continuity check message interval to be configured for 10 milliseconds, periodic packet management (PPM) runs on the Routing Engine and Packet Forwarding Engine (PFE) by default. You can only disable PPM on the PFE. To disable PPM on the PFE, use the **no-delegate-processing** statement at the **[edit routing-options ppm]** hierarchy level.

To configure the interval, include the **interval** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* continuity-check]** hierarchy level.

## Configuring the Continuity Check Loss Threshold

You can specify the number of continuity check messages that can be lost before marking the MEP as down. The default value is three (PDUs).

To configure the loss threshold, include the **loss-threshold** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* continuity-check]** hierarchy level.

## Continuity Measurement

Continuity measurement is provided by an existing continuity check protocol. The continuity for every remote MEP is measured as the percentage of time that remote MEP was operationally up over the total administratively enabled time. Here, the operational uptime is the total time during which the CCM adjacency is active for a particular remote MEP and the administrative enabled time is the total time during which the local MEP is

active. You can also restart the continuity measurement by clearing the currently measured operational uptime and the administrative enabled time.

**Related  
Documentation**

- Displaying Continuity Measurement Statistics on page 238
- Clearing Continuity Measurement Statistics on page 238

---

## Configuring a Maintenance Endpoint

To configure the maintenance endpoint, include the **mep mep-id** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]** hierarchy level.

- Enabling Maintenance Endpoint Automatic Discovery on page 166
- Configuring the Maintenance Endpoint Direction on page 166
- Configuring the Maintenance Endpoint Interface on page 167
- Configuring the Maintenance Endpoint Priority on page 167
- Configuring the Maintenance Endpoint Lowest Priority Defect on page 167
- Configuring a Remote Maintenance Endpoint on page 168
- Configuring a Remote Maintenance Endpoint Action Profile on page 168
- Configuring Maintenance Endpoint Service Protection on page 169

### Enabling Maintenance Endpoint Automatic Discovery

You can enable the MEP to accept continuity check messages from all remote MEPs of the same maintenance association.

To configure automatic discovery, include the **auto-discovery** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]** hierarchy level.

### Configuring the Maintenance Endpoint Direction

You can specify the direction in which CFM packets are transmitted for the MEP.

Direction up continuity check messages (CCMs) are transmitted out of every logical interface that is part of the same bridging or VPLS instance except for the interface configured on this MEP.

Direction down CCMs are transmitted only out of the interface configured on this MEP.



**NOTE:** Ports in the Spanning Tree Protocol (STP) blocking state do not block CFM packets destined to a down MEP. Ports in an STP blocking state without the continuity check protocol configured do block CFM packets.

---

To configure the MEP direction, include the **direction** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]** hierarchy level.



**NOTE:** For all the configured L2VPNs with CFM UP MEPs, you should configure `no-control-word` under the `[edit routing-instances routing-instance-name protocols l2vpn]` or `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn]` hierarchy level. Otherwise, the CFM packets are not transmitted, and the `show oam ethernet connectivity-fault-management mep-database` will not show any remote MEPs.

## Configuring the Maintenance Endpoint Interface

You must specify the interface to which the MEP is attached. It can be a physical interface, logical interface, or trunk interface.

On MX Series routers, you can enable the MEP on a specific VLAN of a trunk interface.

To configure the interface, include the `interface interface-name` statement at the `[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]` hierarchy level.

### MEP Interface Configuration

This example shows the MEP interface configuration statements:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  domain-name maintenance-association ma-name]
mep mep-id {
  direction (up | down);
  interface (ge | xe)-(fpc/pic/port | fpc/pic/port.domain | fpc/pic/port.domain vlan vlan-id);
  auto-discovery;
  priority number;
}
```

## Configuring the Maintenance Endpoint Priority

You can specify the IEEE 802.1 priority bits that are used by continuity check and link trace messages.

To configure the priority, include the `priority` statement at the `[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]` hierarchy level.

## Configuring the Maintenance Endpoint Lowest Priority Defect

You can specify the lowest priority defect that is allowed to generate a fault alarm. This configuration determines whether to generate a fault alarm whenever it detects a defect. This configuration is done at the MEP level.

To configure the lowest priority defect, include the `lowest-priority-defect options` statement at the `[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]` hierarchy level.

Table 15 on page 168 describes the available lowest priority defect options.

Table 15: Lowest Priority Defect Options

Option	Description
<b>all-defects</b>	Allows all defects.
<b>err-xcon</b>	Allows only erroneous CCM and cross-connect CCM defects.
<b>mac-rem-err-xcon</b>	Allows only MAC, not receiving CCM, erroneous CCM, and cross-connect defects.
<b>no-defect</b>	Allows no defect.
<b>rem-err-xcon</b>	Allows only not receiving CCM, erroneous CCM, and cross-connect CCM defects.
<b>xcon</b>	Allows only cross-connect CCM defects.

The following configuration example shows **mac-rem-err-xcon** as the lowest priority defect:

```
[edit protocols]
oam {
  ethernet {
    connectivity-fault-management {
      maintenance-domain md6 {
        level 6;
        maintenance-association ma6 {
          mep 200 {
            interface ge-5/0/0.0;
            direction down;
            lowest-priority-defect mac-rem-err-xcon;
          }
        }
      }
    }
  }
}
```

## Configuring a Remote Maintenance Endpoint

You can configure a remote MEP from which CCM messages are expected. If autodiscovery is not enabled, the remote MEP must be configured under the **mep** statement. If the remote MEP is not configured under the **mep** statement, the CCMs from the remote MEP are treated as errors.

To configure the remote MEP, include the **remote-mep** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id*]** hierarchy level.

## Configuring a Remote Maintenance Endpoint Action Profile

You can specify the name of the action profile to use for the remote MEP.

To configure the action profile, include the **action-profile *profile-name*** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain**

***domain-name maintenance-association ma-name mep mep-id remote-mep mep-id*** hierarchy level. The profile must already be defined at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

## Configuring Maintenance Endpoint Service Protection

You can enable service protection for a VPWS (Virtual Private Wire Service) over MPLS by specifying a working path or protect path on the MEP. Service protection provides end-to-end connection protection of the working path in the event of a failure.

To configure service protection, you must create two separate transport paths a working path and a protect path. You can specify the working path and protect path by creating two maintenance associations. To associate the maintenance association with a path, you must configure the MEP **interface** statement within the maintenance association and specify the path as working or protect.

To configure the MEP interface, include the **interface** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *domain-name* maintenance-association *ma-name* mep *mep-id*** hierarchy level. On the **interface** statement, specify the path as (**working | protect**). The direction must also be configured as direction down for both sessions.



**NOTE:** If the path is not specified, the session monitors the active path.

Table 16 on page 169 describes the available service protection options.

**Table 16: Service Protection Options**

Option	Description
<b>working</b>	Specifies the working path.
<b>protect</b>	Specifies the protect path.

The following configuration example shows service protection is enabled for the VPWS service. The CCM session is configured for the working path and references the CCM session configured for the protect path in the **protect-maintenance-association** statement. The APS profile is configured and associated with the maintenance-association for the working path:

```
[edit protocols]
oam {
  ethernet {
    connectivity-fault-management {
      maintenance-domain vpws-service-1 {
        name-format none;
        level 5;
        maintenance-association W {
          short-name-format character-string;
          protect-maintenance-association P {
            aps-profile aps-profile-1;
```

```
    }
    continuity-check {
        interval 1s;
    }
    mep 1 {
        interface ge-1/3/5.0 working;
        direction down;
        auto-discovery;
    }
}
maintenance-association P {
    short-name-format character-string;
    continuity-check {
        interval 1s;
    }
    mep 1 {
        interface ge-1/3/5.0 protect;
        direction down;
        auto-discovery;
    }
}
}
}
}
```

---

## Configuring a Connectivity Fault Management Action Profile

You can configure an action profile and specify the action to be taken when any of the configured events occur. Alternately, you can configure an action profile and specify default actions when connectivity to a remote MEP fails.

To configure the action profile name, include the **action-profile** statement at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

- Configuring the Action of a CFM Action Profile on page 170
- Configuring the Default Actions of a CFM Action Profile on page 171
- Configuring a CFM Action Profile Event on page 172

### Configuring the Action of a CFM Action Profile

You can configure the action to be taken when any of the configured events occur.

To configure the action profile's action, include the **action** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name*]** hierarchy level.

```
[edit protocols oam]
ethernet {
    connectivity-fault-management {
        action-profile bring-down {
            event {
                interface-status-tlv down;
            }
            action {
```

```

        interface-down;
    }
}
}

```

## Configuring the Default Actions of a CFM Action Profile

You can configure the default actions to be taken when connectivity to a remote MEP fails.

To enable the **interface-down** as the default action for an action profile, include the **interface-down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* default-actions]** hierarchy level.

```

[edit]
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        action-profile bring-down {
          default-actions {
            interface-down;
          }
        }
      }
      maintenance-domain md1 {
        level 0;
        maintenance-association ma1 {
          continuity-check {
            interval 100 ms;
          }
          mep 4001 {
            interface ge-4/1/0;
            direction down;
            remote-mep 1 {
              action-profile bring-down;
            }
          }
        }
      }
    }
  }
}
}

```



**NOTE:** Associating an action-profile with the action of interface-down on an up MEP CFM session running over a CCC interface (l2circuit/l2vpn) is not advisable and could result in a deadlock situation.

## Configuring a CFM Action Profile Event

You can configure one or more events under the action profile, the occurrence of which will trigger the corresponding action to be taken.

To configure the interface-status-tlv lower-layer-down event, include the **interface-status-tlv lower-layer-down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure the interface-status-tlv down event, include the **interface-status-tlv down** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure the port-status-tlv blocked event, include the **port-status-tlv blocked** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure the adjacency-loss event, include the **adjacency-loss** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

To configure an RDI event to bring an interface down on reception of an RDI bit from a MEP, include the **rdi** statement at the **[edit protocols oam ethernet connectivity-fault-management action-profile *profile-name* event]** hierarchy level.

```
[edit protocols oam]
ethernet {
  connectivity-fault-management {
    action-profile bring-down {
      event {
        interface-status-tlv [lower-layer-down down];
        port-status-tlv blocked;
        adjacency-loss;
        rdi;
      }
      action {
        interface-down;
      }
    }
  }
}
```

**Related Documentation**

- [event \(CFM\)](#)



## Configuring Linktrace Protocol in CFM

---

The linktrace protocol is used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the **traceroute** command to verify the path between a pair of MEPs under the same maintenance association. Linktrace messages can also be used to verify the path between an MEP and an MIP under the same maintenance domain. The operation of IEEE 802.1ag linktrace request and response messages is similar to the operation of Layer 3 **traceroute** commands. For more information about the **traceroute** command, see the *Junos OS System Basics Configuration Guide*.

### Configuring the Linktrace Path Age Timer

If no response to a **linktrace** request is received, the request and response entries are deleted after the age timer expires. To configure the linktrace age timer, use the **linktrace** statement with the **age time** option at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level. The age is configured in minutes or seconds.

### Configuring the Linktrace Database Size

Configure the number of linktrace reply entries to be stored per linktrace request. To configure the linktrace database size, use the **linktrace** statement with the **path-database-size path-database-size** option at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

Display the linktrace database using the **show oam ethernet connectivity-fault-management path-database** command.

## Configuring Ethernet Local Management Interface

---

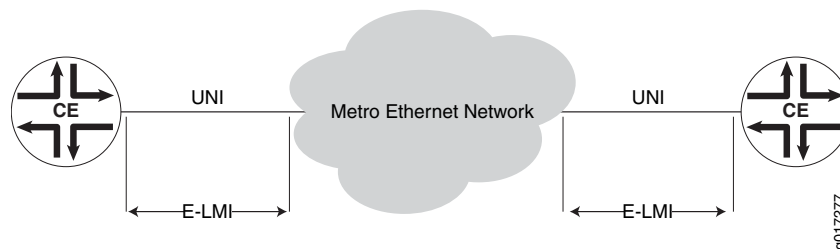
- Ethernet Local Management Interface Overview on page 173
- Configuring the Ethernet Local Management Interface on page 175
- Example E-LMI Configuration on page 177

### Ethernet Local Management Interface Overview

MX Series routers with Gigabit Ethernet (**ge**), 10-Gigabit Ethernet (**xe**), or Aggregated Ethernet (**ae**) interfaces support the Ethernet Local Management Interface (E-LMI). The E-LMI specification is available at the Metro Ethernet Forum. E-LMI procedures and protocols are used for enabling automatic configuration of the customer edge (CE) to support Metro Ethernet services. The E-LMI protocol also provides user-to-network interface (UNI) and Ethernet virtual connection (EVC) status information to the CE. The UNI and EVC information enables automatic configuration of CE operation based on the Metro Ethernet configuration.

The E-LMI protocol operates between the CE device and the provider edge (PE) device. It runs only on the PE-CE link and notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port. The scope of the E-LMI protocol is shown in Figure 20 on page 174.

Figure 20: Scope of the E-LMI Protocol



The E-LMI implementation on MX Series routers includes only the PE side of the E-LMI protocol.

E-LMI interoperates with an OAM protocol, such as Connectivity Fault Management (CFM), that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level (UNI-N to UNI-N with up MEPs at the UNI). E-LMI relies on the CFM for end-to-end status of EVCs across CFM domains (SVLAN domain or VPLS).

The E-LMI protocol relays the following information:

- Notification to the CE of the addition/deletion of an EVC (active, not active, or partially active)
- Notification to the CE of the availability state of a configured EVC
- Communication of UNI and EVC attributes to the CE:
  - UNI attributes:
    - UNI identifier (a user-configured name for UNI)
    - CE-VLAN ID/EVC map type (all-to-one bundling, service multiplexing with bundling, or no bundling)
    - Bandwidth profile is not supported (including the following features):
      - CM (coupling mode)
      - CF (color flag)
      - CIR (committed Information rate)
      - CBR (committed burst size)
      - EIR (excess information rate)
      - EBS (excess burst size)
  - EVC attributes:
    - EVC reference ID
    - EVC status type (active, not active, or partially active)
    - EVC type (point-to-point or multipoint-to-multipoint)

- EVC ID (a user-configured name for EVC)
- Bandwidth profile (not supported)
- CE-VLAN ID/EVC map

E-LMI on MX Series routers supports the following EVC types:

- Q-in-Q SVLAN (point-to-point or multipoint-to-multipoint)—Requires an end-to-end CFM session between UNI-Ns to monitor the EVS status.
- VPLS (BGP or LDP) (point-to-point or multipoint-to-multipoint)—Either VPLS pseudowire status or end-to-end CFM sessions between UNI-Ns can be used to monitor EVC status.
- L2 circuit/L2VPN (point-to-point)—Either VPLS pseudowire status or end-to-end CFM sessions between UNI-Ns can be used to monitor EVC status.



**NOTE:** l2-circuit and l2vpn are not supported.

## Configuring the Ethernet Local Management Interface

To configure E-LMI, perform the following steps:

- Configuring an OAM Protocol (CFM) on page 175
- Assigning the OAM Protocol to an EVC on page 175
- Enabling E-LMI on an Interface and Mapping CE VLAN IDs to an EVC on page 176

### Configuring an OAM Protocol (CFM)

For information on configuring the OAM protocol (CFM), see “IEEE 802.1ag OAM Connectivity Fault Management Overview” on page 159.

### Assigning the OAM Protocol to an EVC

To configure an EVC, you must specify a name for the EVC using the **evcsevc-id** statement at the **[edit protocols oam ethernet]** hierarchy level. You can set the EVC protocol for monitoring EVC statistics to **cfm** or **vpls** using the **evc-protocol** statement and its options at the **[edit protocols oam ethernet evcs]** hierarchy level.

You can set the number of remote UNIs in the EVC using the **remote-uni-count number** statement at the **[edit protocols oam ethernet evcs evcs-protocol]** hierarchy level. The **remote-uni-count** defaults to 1. Configuring a value greater than 1 makes the EVC multipoint-to-multipoint. If you enter a value greater than the actual number of endpoints, the EVC status will display as partially active even if all endpoints are up. If you enter a **remote-uni-count** less than the actual number of endpoints, the status will display as active, even if all endpoints are not up.

You can configure an EVC by including the **evcs** statement at the **[edit protocols oam ethernet]** hierarchy level:

```
[edit protocols oam ethernet]
```

```
evcs evc-id {  
    evc-protocol (cfm (management-domain name management-association name) | vpls  
        (routing-instance name)) {  
        remote-uni-count <number>; # Optional, defaults to 1  
        multipoint-to-multipoint;  
        # Optional, defaults to point-to-point if remote-uni-count is 1  
    }  
}
```

---

### Enabling E-LMI on an Interface and Mapping CE VLAN IDs to an EVC

---

To configure E-LMI, include the `lmi` statement at the `[edit protocols oam ethernet]` hierarchy level:

```
[edit protocols oam ethernet]  
lmi {  
    polling-verification-timer value;  
    # Polling verification timer (T392), defaults to 15 seconds  
    status-counter count; # Status counter (N393), defaults to 4  
    interface name {  
        evc evc-id {  
            default-evc;  
            vlan-list [ vlan-ids ];  
        }  
        evc-map-type (all-to-one-bundling | bundling | service-multiplexing);  
        polling-verification-time value; # Optional, defaults to global value  
        status-counter count; # Optional, defaults to global value  
        uni-id value; # Optional, defaults to interface-name  
    }  
}
```

You can set the status counter to count consecutive errors using the `status-counter count` statement at the `[edit protocols oam ethernet lmi]` hierarchy level. The status counter is used to determine if E-LMI is operational or not. The default value is 4.

You can set the `polling-verification-timer value` statement at the `[edit protocols oam ethernet lmi]` hierarchy level. The default value is 15 seconds.

You can enable an interface and set its options for use with E-LMI using the `interface name` statement at the `[edit protocols oam ethernet lmi]` hierarchy level. Only `ge`, `xe`, and `ae` interfaces are supported. You can use the interface `uni-id` option to specify a name for the UNI. If `uni-id` is not configured, it defaults to the name variable of `interface name`.

You can specify the CE-VLAN ID/EVC map type using the `evc-map-type type` interface option. The options are `all-to-one-bundling`, `bundling`, or `service-multiplexing`. Service multiplexing is with no bundling. The default type is `all-to-one-bundling`.

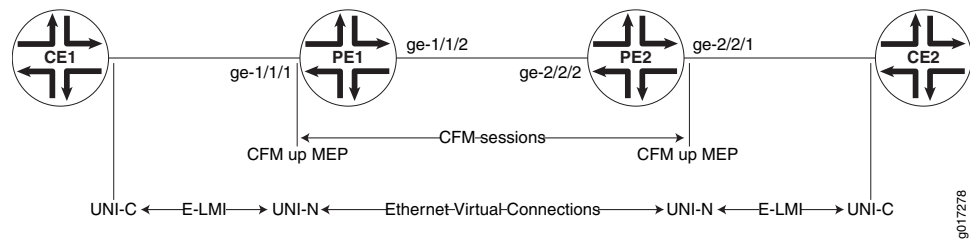
To specify the EVC that an interface uses, use the `evc evc-id` statement at the `[edit protocols oam ethernet lmi interface name]` hierarchy level. You can specify an interface as the default EVC interface using the `default-evc` statement at the `[edit protocols oam ethernet lmi interface name evc evc-id]` hierarchy level. All VLANs that are not mapped to any other EVCs are mapped to this EVC. Only one EVC can be configured as the default.

You can map a list of VLANs to an EVC using the `vlan-list vlan-id-list` statement at the `[edit protocols oam ethernet lmi interface name evc evc-id]` hierarchy level.

## Example E-LMI Configuration

Figure 21 on page 177 illustrates the E-LMI configuration for a point-to-point EVC (SVLAN) monitored by CFM. In this example, VLANs 1 through 2048 are mapped to **evc1** (SVLAN 100) and 2049 through 4096 are mapped to **evc2** (SVLAN 200). Two CFM sessions are created to monitor these EVCs.

**Figure 21: E-LMI Configuration for a Point-to-Point EVC (SVLAN) Monitored by CFM**



g017278

## Configuring PE1

```
[edit]
interfaces {
  ge-1/1/1 {
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list 1-2048;
      }
    }
    unit 1 {
      family bridge {
        interface-mode trunk;
        vlan-id-list 2049-4096;
      }
    }
  }
  ge-1/1/2 {
    unit 0 {
      vlan-id 100;
      family bridge {
        interface-mode trunk;
        inner-vlan-id-list 1-2048;
      }
    }
    unit 1 {
      vlan-id 200;
      family bridge {
        interface-mode trunk;
        inner-vlan-id-list 2049-4096;
      }
    }
  }
}
protocols {
  oam {
```

```
ethernet {
  connectivity-fault-management {
    maintenance-domain md {
      level 0;
      maintenance-association 1 {
        name-format vlan;
        mep 1 {
          direction up;
          interface ge-1/1/1.0 vlan 1;
        }
      }
      maintenance-association 2049 {
        name-format vlan;
        mep 1 {
          direction up;
          interface ge-1/1/1.1 vlan 2049;
        }
      }
    }
  }
}
evcs {
  evc1 {
    evc-protocol cfm management-domain md management-association 1;
    remote-uni-count 1;
  }
  evc2 {
    evc-protocol cfm management-domain md management-association 2049;
    remote-uni-count 1;
  }
}
lmi {
  interface ge-1/1/1 {
    evc evc1 {
      vlan-list 1-2048;
    }
    evc evc2 {
      vlan-list 2049-4096;
    }
    evc-map-type bundling;
    uni-id uni-ce1;
  }
}
}
```

---

## Configuring PE2

```
[edit]
interfaces {
  ge-2/2/1 {
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list 1-2048;
      }
    }
  }
}
```

```

    }
    unit 1 {
        family bridge {
            interface-mode trunk;
            vlan-id-list 2049-4096;
        }
    }
}
ge-2/2/2 {
    unit 0 {
        vlan-id 100;
        family bridge {
            interface-mode trunk;
            inner-vlan-id-list 1-2048;
        }
    }
    unit 1 {
        vlan-id 200;
        family bridge {
            interface-mode trunk;
            inner-vlan-id-list 2049-4095;
        }
    }
}
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 0;
                    maintenance-association 1 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.0 vlan 1;
                        }
                    }
                    maintenance-association 2049 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.1 vlan 2049;
                        }
                    }
                }
            }
        }
    }
    evcs {
        evc1 {
            evc-protocol cfm management-domain md management-association 1;
            remote-uni-count 1;
        }
        evc2 {
            evc-protocol cfm management-domain md management-association 2049;
            uni-count 2;
        }
    }
}

```

```
}
lmi {
  interface ge-2/2/1 {
    evc evc1 {
      vlan-list 1-2048;
    }
    evc evc2 {
      vlan-list 2049-4095;
    }
    evc-map-type bundling;
    uni-id uni-ce2;
  }
}
}
```

---

### Configuring Two UNIs Sharing the Same EVC

---

```
[edit protocols]
oam {
  ethernet {
    connectivity-fault-management { ...}
    evcs {
      evc1 {
        evc-protocol cfm management-domain md management-association 1;
        remote-uni-count 1;
      }
    }
  }
  lmi {
    interface ge-2/2/1 {
      evc evc1 {
        vlan-list 0-4095;
      }
      evc-map-type all-to-one-bundling;
      uni-id uni-ce1;
    }
    interface ge-2/3/1 {
      evc evc1 {
        vlan-list 0-4095;
      }
      evc-map-type all-to-one-bundling;
      uni-id uni-ce2;
    }
  }
}
```

---

### Configuring Port Status TLV and Interface Status TLV

---

- TLVs Overview on page 181
- Various TLVs for CFM PDUs on page 181
- Support for Additional Optional TLVs on page 183



- MAC Status Defects on page 189
- Configuring Remote MEP Action Profile Support on page 190

## TLVs Overview

Type, Length, and Value (TLVs) are described in the IEEE 802.1ag standard for CFM as a method of encoding variable-length and/or optional information in a PDU. TLVs are not aligned to any particular word or octet boundary. TLVs follow each other with no padding between them.

Table 17 on page 181 shows the TLV format and indicates if it is required or optional.

**Table 17: Format of TLVs**

Parameter	Octet (sequence)	Description
Type	1	Required. If 0, no Length or Value fields follow. If not 0, at least the Length field follows the Type field.
Length	2–3	Required if the Type field is not 0. Not present if the Type field is 0. The 16 bits of the Length field indicate the size, in octets, of the Value field. 0 in the Length field indicates that there is no Value field.
Value	4	Length specified by the Length field. Optional. Not present if the Type field is 0 or if the Length field is 0.

## Various TLVs for CFM PDUs

Table 18 on page 181 shows a set of TLVs defined by IEEE 802.1ag for various CFM PDU types. Each TLV can be identified by the unique value assigned to its type field. Some type field values are reserved.

**Table 18: Type Field Values for Various TLVs for CFM PDUs**

TLV or Organization	Type Field
End TLV	0
Sender ID TLV	1
Port Status TLV	2
Data TLV	3
Interface Status TLV	4
Reply Ingress TLV	5
Reply Egress TLV	6
LTM Egress Identifier TLV	7
LTR Egress Identifier TLV	8

Table 18: Type Field Values for Various TLVs for CFM PDUs (*continued*)

TLV or Organization	Type Field
Reserved for IEEE 802.1	9 to 30
Organization-Specific TLV	31
Defined by ITU-T Y.1731	32 to 63
Reserved for IEEE 802.1	64 to 255

Not every TLV is applicable for all types of CFM PDUs.

- TLVs applicable for continuity check message (CCM):
  - End TLV
  - Sender ID TLV
  - Port Status TLV
  - Interface Status TLV
  - Organization-Specific TLV
- TLVs applicable for loopback message (LBM):
  - End TLV
  - Sender ID TLV
  - Data TLV
  - Organization-Specific TLV
- TLVs applicable for loopback reply (LBR):
  - End TLV
  - Sender ID TLV
  - Data TLV
  - Organization-Specific TLV
- TLVs applicable for linktrace message (LTM):
  - End TLV
  - LTM Egress Identifier TLV
  - Sender ID TLV
  - Organization-Specific TLV
- TLVs applicable for linktrace reply (LTR):

- End TLV
- LTR Egress Identifier TLV
- Reply Ingress TLV
- Reply Egress TLV
- Sender ID TLV
- Organization-Specific TLV

The following TLVs are currently supported in the applicable CFM PDUs:

- End TLV
- Reply Ingress TLV
- Reply Egress TLV
- LTR Egress Identifier TLV
- LTM Egress Identifier TLV
- Data TLV

## Support for Additional Optional TLVs

The following additional optional TLVs are supported:

- Port Status TLV
- Interface Status TLV

MX Series routers support configuration of port status TLV and interface status TLV. Configuring the Port Status TLV allows the operator to control the transmission of the Port Status TLV in CFM PDUs.



**NOTE:** Although Port Status TLV configuration statements are visible in the CLI on M120 and M320 routers, Port Status TLV cannot be configured on these systems. Port Status TLV can be enabled on a MEP interface only if it is a bridge logical interface, which is not possible on these systems.

For configuration information, see the following sections:

- Port Status TLV on page 183
- Interface Status TLV on page 186

---

### Port Status TLV

The Port Status TLV indicates the ability of the bridge port on which the transmitting MEP resides to pass ordinary data, regardless of the status of the MAC. The value of this TLV is driven by the MEP variable **enableRmepDefect**, as shown in Table 20 on page 184. The format of this TLV is shown in Table 19 on page 184.

Any change in the Port Status TLVs value triggers one extra transmission of that bridge ports MEP CCMs.

**Table 19: Port Status TLV Format**

Parameter	Octet ( Sequence)
Type = 2	1
Length	2–3
Value (See Table 20 on page 184)	4

**Table 20: Port Status TLV Values**

Mnemonic	Ordinary Data Passing Freely Through the Port	Value
psBlocked	No: <code>enableRmepDefect</code> = false	1
psUp	Yes: <code>enableRmepDefect</code> = true	2

The MEP variable `enableRmepDefect` is a boolean variable indicating whether frames on the service instance monitored by the maintenance associations if this MEP are enabled to pass through this bridge port by the Spanning Tree Protocol and VLAN topology management. It is set to TRUE if:

- The bridge port is set in a state where the traffic can pass through it.
- The bridge port is running multiple instances of the spanning tree.
- The MEP interface is not associated with a bridging domain.

#### **Configuring Port Status TLV**

Junos OS provides configuration support for the Port Status TLV, allowing you to control the transmission of this TLV in CCM PDUs. The Junos OS provides this configuration at the continuity-check level. By default, the CCM does not include the Port Status TLV. To configure the Port Status TLV, use the `port-status-tlv` statement at the `[edit protocols oam ethernet connectivity-fault-management maintenance-domain identifier maintenance-association identifier continuity-check]` hierarchy level.



**NOTE:** Port Status TLV configuration is not mandated by IEEE 802.1ag. The Junos OS provides it in order to give more flexibility to the operator; however it receives and processes CCMs with a Port Status TLV, regardless of this configuration.

An example of the configuration statements follows:

```
protocols {
  oam {
    ethernet {
```

```

connectivity-fault-management {
  maintenance-domain identifier {
    level number;
    maintenance-association identifier {
      continuity-check {
        interval number,
        loss-threshold number;
        hold-interval number;
        port-status-tlv; # Sets Port Status TLV
      }
    }
  }
}

```

You cannot enable Port Status TLV transmission in the following two cases:

- If the MEP interface under the maintenance-association is not of type bridge.
- If the MEP is configured on a physical interface.

### ***Displaying the Received Port Status TLV***

The Junos OS saves the last received Port Status TLV from a remote MEP. If the received Port Status value does not correspond to one of the standard values listed in Table 20 on page 184, then the **show** command displays it as "unknown." You can display the last saved received Port Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

```

user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up
Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

Remote MEP identifier: 1001, State: ok
MAC address: 00:19:e2:b0:74:00, Type: Learned
Interface: ge-2/0/0.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none # RX PORT STATUS
Interface status TLV: none

```

### ***Displaying the Transmitted Port Status TLV***

The Junos OS saves the last transmitted Port Status TLV from a local MEP. If the transmission of the Port Status TLV has not been enabled, then the **show** command displays "none." You can display the last saved transmitted Port Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain**

*identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*  
command, as in the following example:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up # TX PORT STATUS
Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

Remote MEP identifier: 1001, State: ok
MAC address: 00:19:e2:b0:74:00, Type: Learned
Interface: ge-2/0/0.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: none
```

### Interface Status TLV

The Interface Status TLV indicates the status of the interface on which the MEP transmitting the CCM is configured, or the next-lower interface in the IETF RFC 2863 IF-MIB. The format of this TLV is shown in Table 21 on page 186. The enumerated values are shown in Table 22 on page 186.

Table 21: Interface Status TLV Format

Parameter	Octet (Sequence)
Type = 4	1
Length	2–3
Value (See Table 22 on page 186)	4

Table 22: Interface Status TLV Values

Mnemonic	Interface Status	Value
isUp	up	1
isDown	down	2
isTesting	testing	3
isUnknown	unknown	4
isDormant	dormant	5
isNotPresent	notPresent	6

Table 22: Interface Status TLV Values (*continued*)

Mnemonic	Interface Status	Value
isLowerLayerDown	lowerLayerDown	7

**Configuring Interface Status TLV**

The Junos OS provides configuration support for the Interface Status TLV, thereby allowing operators to control the transmission of this TLV in CCM PDUs through configuration at the continuity-check level.



**NOTE:** This configuration is not mandated by IEEE 802.1ag; rather it is provided to give more flexibility to the operator. The Junos OS receives and processes CCMs with the Interface Status TLV, regardless of this configuration.

The interface status TLV configuration is shown below:

```
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain identifier {
          level number;
          maintenance-association identifier {
            continuity-check {
              interval number;
              loss-threshold number;
              hold-interval number;
              interface-status-tlv; # Sets the interface status TLV
            }
          }
        }
      }
    }
  }
}
```



**NOTE:** The Junos OS supports transmission of only three out of seven possible values for the Interface Status TLV. The supported values are 1, 2, and 7. However, the Junos OS is capable of receiving any value for the Interface Status TLV.

**Displaying the Received Interface Status TLV**

The Junos OS saves the last received Interface Status TLV from the remote MEP. If the received Interface Status value does not correspond to one of the standard values listed in Table 21 on page 186, then the **show** command displays "unknown."

You can display this last saved Interface Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001
```

```
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up
Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

Remote MEP identifier: 1001, State: ok
MAC address: 00:19:e2:b0:74:00, Type: Learned
Interface: ge-2/0/0.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: none # displays the Interface Status TLV state
```

#### ***Displaying the Transmitted Interface Status TLV***

The Junos OS saves the last transmitted Interface Status TLV from a local MEP. If the transmission of Interface Status TLV has not been enabled, then the **show** command displays "none."

You can display the last transmitted Interface Status TLV using the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *identifier* maintenance-association *identifier* local-mep *identifier* remote-mep *identifier*** command, as in the following example:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001
```

```
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up
Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

Remote MEP identifier: 1001, State: ok
MAC address: 00:19:e2:b0:74:00, Type: Learned
Interface: ge-2/0/0.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: none
```



## MAC Status Defects

The Junos OS provides MAC status defect information, indicating that one or more of the remote MEPs is reporting a failure in its Port Status TLV or Interface Status TLV. It indicates “yes” if either some remote MEP is reporting that its interface is not isUp (for example, at least one remote MEPs interface is unavailable), or if all remote MEPs are reporting a Port Status TLV that contains some value other than psUp (for example, all remote MEPs Bridge Ports are not forwarding data). There are two **show** commands you can use to view the MAC Status Defects indication.

Use the **mep-database** command to display MAC status defects:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md6 maintenance-association ma6
Maintenance domain name: md6, Format: string, Level: 6
Maintenance association name: ma6, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
Auto-discovery: enabled, Priority: 0
Interface status TLV: up, Port status TLV: up
Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
Defects:
  Remote MEP not receiving CCM          : no
  Erroneous CCM received                 : no
  Cross-connect CCM received            : no
  RDI sent by some MEP                  : no
  Some remote MEP's MAC in error state  : yes # MAC Status Defects yes/no
Statistics:
  CCMs sent                             : 1658
  CCMs received out of sequence          : 0
  LBMs sent                             : 0
  Valid in-order LBRs received           : 0
  Valid out-of-order LBRs received       : 0
  LBRs received with corrupted data      : 0
  LBRs sent                             : 0
  LTMs sent                             : 0
  LTMs received                         : 0
  LTRs sent                             : 0
  LTRs received                         : 0
  Sequence number of next LTM request    : 0
  1DMs sent                             : 0
  Valid 1DMs received                   : 0
  Invalid 1DMs received                  : 0
  DMMs sent                             : 0
  DMRs sent                             : 0
  Valid DMRs received                   : 0
  Invalid DMRs received                  : 0
Remote MEP count: 1
  Identifier  MAC address  State  Interface
    200      00:05:85:73:39:4a    ok    xe-5/0/0.0
```

Use the **interfaces** command to display MAC status defects:

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
Maintenance domain name: md6, Format: string, Level: 6
Maintenance association name: ma6, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
```

```

Interface status TLV: up, Port status TLV: up
MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
MEP status: running
Defects:
  Remote MEP not receiving CCM                : no
  Erroneous CCM received                      : no
  Cross-connect CCM received                  : no
  RDI sent by some MEP                       : no
  Some remote MEP's MAC in error state        : yes # MAC Status Defects
yes/no
Statistics:
  CCMs sent                                  : 1328
  CCMs received out of sequence              : 0
  LBMs sent                                  : 0
  Valid in-order LBRs received                : 0
  Valid out-of-order LBRs received            : 0
  LBRs received with corrupted data           : 0
  LBRs sent                                  : 0
  LTMs sent                                  : 0
  LTMs received                              : 0
  LTRs sent                                  : 0
  LTRs received                              : 0
  Sequence number of next LTM request         : 0
  1DMs sent                                  : 0
  Valid 1DMs received                        : 0
  Invalid 1DMs received                      : 0
  DMMs sent                                  : 0
  DMRs sent                                  : 0
  Valid DMRs received                        : 0
  Invalid DMRs received                      : 0
Remote MEP count: 1
  Identifier  MAC address  State  Interface
    200      00:05:85:73:39:4a  ok    xe-5/0/0.0

```

## Configuring Remote MEP Action Profile Support

Based on values of **interface-status-tlv** and **port-status-tlv** in the received CCM packets, a specific action, such as **interface-down**, can be taken using the **action-profile** options. Multiple action profiles can be configured on the router, but only one action profile can be assigned to a remote MEP.

The action profile can be configured with at least one event to trigger the action; but the action will be triggered if any one of these events occurs. It is not necessary for all of the configured events to occur to trigger **action**.

An action-profile can be applied only at the remote MEP level.

The following example shows an action profile configuration with explanatory comments added:

```

[edit protocols oam ethernet connectivity-fault-management]
action-profile tlv-action {
  event {
    # If interface status tlv with value specified in the config is received
    interface-status-tlv down|lower-layer-down;
    # If port status tlv with value specified in the config is received
    port-status-tlv blocked;
    # If connectivity is lost to the peer */
  }
}

```

```

        adjacency-loss;
    }
    action {
        # Bring the interface down */
        interface-down;
    }
    default-actions interface-down;
}
# domains
maintenance-domain identifier {
    # maintenance domain level (0-7)
    level number;
    # association
    maintenance-association identifier {
        mep identifier {
            interface ge-x/y/z.w;
            remote-mep identifier {
                # Apply the action-profile for the remote MEP
                action-profile tlv-action;
            }
        }
    }
}

```

### Monitoring a Remote MEP Action Profile

You can use the **show oam ethernet connectivity-fault-management mep-database** command to view the action profile status of a remote MEP, as in the following example:

```

show oam ethernet connectivity-fault-management mep-database remote-mep
(Action Profile Event)
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 remote-mep 200
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
Auto-discovery: enabled, Priority: 0
Interface status TLV: none, Port status TLV: none # last status TLVs transmitted
by the router
Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

Remote MEP identifier: 200, State: ok # displays the remote MEP name and state

MAC address: 00:05:85:73:96:1f, Type: Configured
Interface: ge-1/0/8.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: lower-layer-down
Action profile: juniper # displays remote MEP's action profile identifier
Last event: Interface-status-tlv lower-layer-down # last remote MEP event

# to trigger action
Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
# action occurrence time

```

## Configuring MAC Flush Message Processing in CET Mode

---

In carrier Ethernet transport (CET) mode, MX series routers are used as provider edge (PE) routers, and Nokia Siemens Networks A2200 Carrier Ethernet Switches (referred to as E-domain devices) that run standard based protocols are used in the access side. On the MX series routers, VPLS pseudo wires are configured dynamically through label distribution protocol (LDP). On the E-domain devices, topology changes are detected through connectivity fault management (CFM) sessions running between the E-domain devices and the MX series PE routers. The MX series PE routers can bring the carrier Ethernet interface down if there is CFM connectivity loss. This will trigger a local MAC flush as well as a targeted label distribution protocol (T-LDP) MAC flush notification that gets sent towards the remote MX series PEs to trigger MAC flush on them.

In CET inter-op mode, MX series routers need to interoperate with the Nokia Siemens Networks Ax100 Carrier Ethernet access devices (referred to as A-domain devices) that run legacy protocols. Nokia Siemens Networks A4100 and A8100 devices act as an intermediate between the MX series PE routers and A-domain devices. These intermediate devices perform interworking function (IWF) procedures so that operations administration management (OAM) sessions can be run between MX series routers and A-domain devices. There are no VPLS pseudo wires between the MX series PE routers and the Nokia Siemens Networks A4100 and A8100 intermediate devices, so there is no LDP protocol running between the PE routers to send topology change notifications. In order to communicate topology changes, MX series routers can trigger a MAC flush and propagate it in the core. MX series routers can use action profiles based upon the connection protection type length value (TLV) event. The action profile brings down the carrier edge logical interface in MX series PE routers which will trigger a local MAC flush and also propagate the topology change to the core using LDP notification.

For VPLS there is no end to end connectivity monitored. The access rings are independently monitored by running CFM down multiple end points (MEPs) on the working and protection paths for each of the services between the E-domain devices and the MX series PE routers, and between the A-domain devices and the MX series PE routers via the IWF hosted by the Nokia Siemens Networks A-4100 devices. When there is a connectivity failure on the working path, the Nokia Siemens Networks Ax200 devices will perform a switchover to the protection path, triggering a topology change notification (in the form of TLVs carried in CCM) to be sent on the active path.

Figure 22: CET inter-op dual homed topology

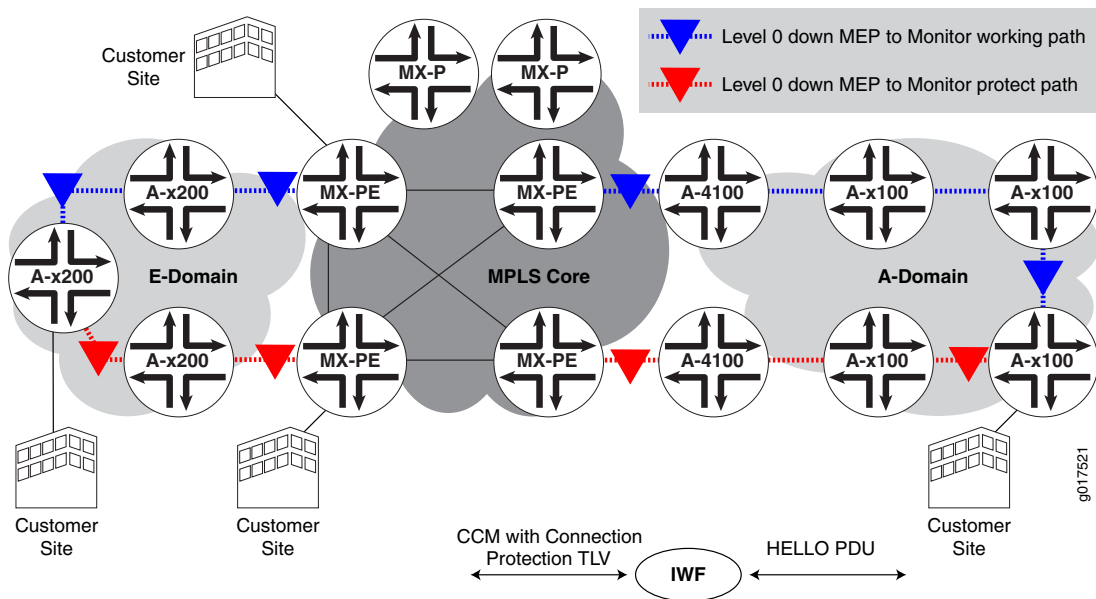


Figure 22 on page 193 describes the dual homed topology on MX series PE routers connected to the A-domain. When an A-domain device triggers a switchover, it starts switching the service traffic to the new active path. This change is communicated in the HELLO protocol data units (PDUs) sent by that A-domain device on the working and protection paths. When the IWF in A4100 receives these HELLO PDUs, it converts them to standard CCM messages and also inserts a connection protection TLV. The "Protection-in-use" field of the connection protection TLV is encoded with the currently active path, and is included in the CCM message. CCM messages are received by the MX series PE routers via the VLAN spoke in A4100. In the above dual homed scenario, one MX series PE router monitors the working path, and the other MX series PE router monitors the protection path.

A MAC flush occurs when the CFM session that is monitoring the working path detects that the service traffic has moved to the protection path or when the CFM session that is monitoring the protection path detects that the service traffic has moved to the working path.

Figure 23: CET inter-op dual attached topology

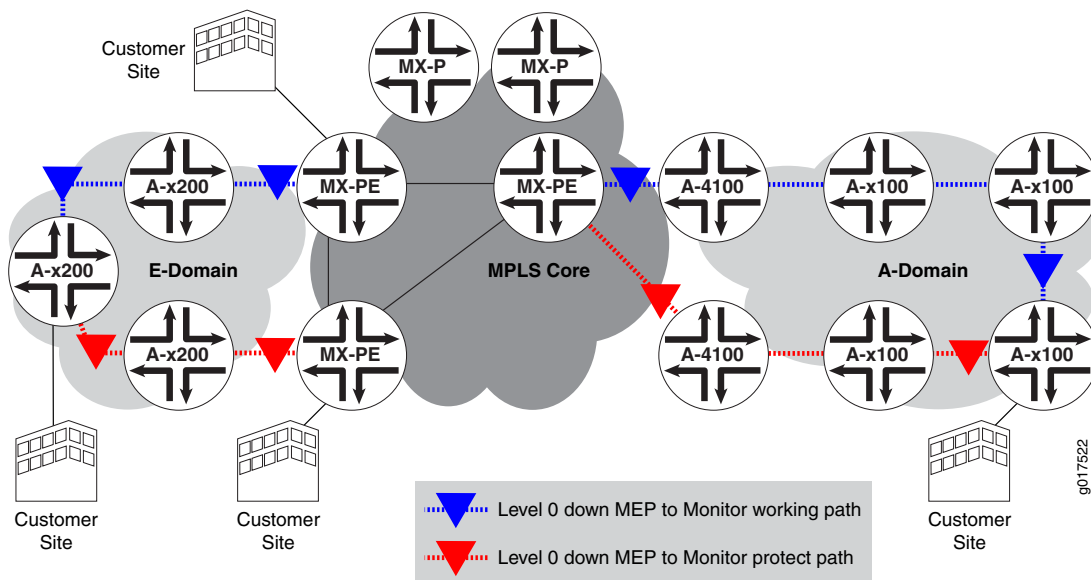


Figure 23 on page 194 describes the dual attached topology on MX series PE routers connected to the A-domain. The MAC flush mechanism used in this case is also the same as the one used for the A-domain in the dual homed scenario (Figure 1). However in this case both the CFM sessions are hosted by only one MX series PE router. When Ax100 in the A-domain detects topology changes, the MX series PE router receives the connection protection TLV in the CCM message for the working and protection paths with the value of “Protection-in-use” indicating which path is the active one. Based upon the event that is generated for the CFM session, the MX series PE router will bring down the appropriate interface which will trigger a local MAC flush.

## Configuring a Connection Protection TLV Action Profile

An action profile can be configured to perform the **interface-down** action based on the values of **connection-protection-tlv** in the received CCM packets.

The following example shows an action profile configuration with explanatory comments added:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
  event {
    # If a connection protection TLV with a "Protection-in-use" value of SET is received */
    connection-protection-tlv <using-protection-path>;
    # If a connection protection TLV with a "Protection-in-use" value of RESET is received
    */
    connection-protection-tlv <using-working-path>;
  }
  action {
    # Bring the interface down */
    interface-down;
  }
}
```

**Related Documentation**

- connection-protection-tlv

## Configuring M120 and MX Series Routers for CCC Encapsulated Packets

- IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview on page 195
- CFM Features Supported on Layer 2 VPN Circuits on page 195
- Configuring CFM for CCC Encapsulated Packets on page 196

### IEEE 802.1ag CFM OAM Support for CCC Encapsulated Packets Overview

Layer 2 virtual private network (L2VPN) is a type of virtual private network service used to transport customer's private Layer 2 traffic (for example, Ethernet, ATM or Frame Relay) over the service provider's shared IP/MPLS infrastructure. The service provider edge (PE) router must have an interface with circuit cross-connect (CCC) encapsulation to switch the customer edge (CE) traffic to the public network.

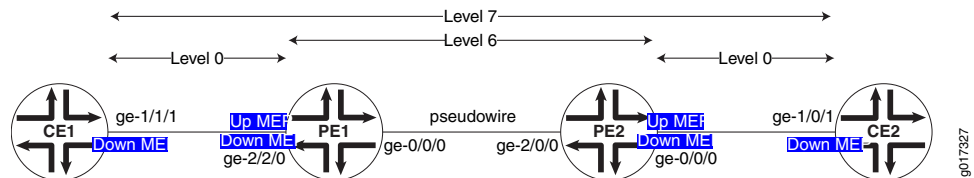
The IEEE 802.1ag Ethernet Connectivity Fault Management (CFM) is an OAM standard used to perform fault detection, isolation, and verification on virtual bridge LANs. M120 and MX Series routers provide CFM support for bridge/VPLS/routed interfaces and support 802.1ag Ethernet OAM for CCC encapsulated packets.

### CFM Features Supported on Layer 2 VPN Circuits

CFM features supported on L2VPN circuits are as follows:

- Creation of up/down MEPs at any level on the CE-facing logical interfaces.
- Creation of MIPs at any level on the CE-facing logical interfaces.
- Support for continuity check, loopback, and linktrace protocol.
- Support for the Y1731 Ethernet Delay measurement protocol.
- Support for action profiles to bring the CE-facing logical interfaces down when loss of connectivity is detected.

**Figure 24: Layer 2 VPN Topology**



To monitor the L2VPN circuit, a CFM up MEP (Level 6 in Figure 24 on page 195) can be configured on the CE-facing logical interfaces of provider edge routers PE1 and PE2. To monitor the CE-PE attachment circuit, a CFM down MEP can be configured on the customer logical interfaces of CE1-PE1 and CE2-PE2 (Level 0 in Figure 24 on page 195).

## Configuring CFM for CCC Encapsulated Packets

The only change from the existing CLI configuration is the introduction of a new command to create a MIP on the CE-facing interface of the PE router.

```
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        # Define a maintenance domains for each default level.
        #; These names are specified as DEFAULT_level_number
        maintenance-domain DEFAULT_x {
          # L2VPN CE interface
          interface (ge | xe)-fpc/pic/port.domain;
        }
        {
          level number;
          maintenance-association identifier {
            mep mep-id {
              direction (up | down);
              # L2 VPN CE interface on which encapsulation family CCC is configured.
              interface (ge | xe)-fpc/pic/port.domain;
              auto-discovery;
              priority number;
            }
          }
        }
      }
    }
  }
}
```

## Configuring Rate Limiting of Ethernet OAM Messages

---

M Series, M320 with Enhanced III FPC, M120, M7i and M10 with CFEB, and MX Series routers support rate limiting of Ethernet OAM messages. Depending on the connectivity fault management (CFM) configuration, CFM packets are discarded, sent to the CPU for processing, or flooded to other bridge interfaces. This feature allows the router to intercept incoming CFM packets for prevention of DoS attacks.

You can apply rate limiting of Ethernet OAM messages at either of two CFM policing levels, as follows:

- Global-level CFM policing—uses a policer at the global level to police the CFM traffic belonging to all the sessions.
- Session-level CFM policing—uses a policer created to police the CFM traffic belonging to one session.

To configure global-level CFM policing, include the **policer** statement and its options at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.



To configure session-level CFM policing, include the **policer** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *name* level *number* maintenance-association *name*]** hierarchy level.

The following example shows a CFM policer used for rate-limiting CFM:

```
[edit]
firewall {
  policer cfm-policer {
    if-exceeding {
      bandwidth-limit 8k;
      burst-size-limit 2k;
    }
    then discard;
  }
}
```

#### Case 1: Global-Level CFM Policing

This example shows a global level policer, at the CFM level, for rate-limiting CFM. The **continuity-check *cfm-policer*** statement at the global **connectivity-fault-management policer** hierarchy level specifies the policer to use for policing all continuity check packets of the CFM traffic belonging to all sessions. The **other *cfm-policer1*** statement at the **connectivity-fault-management policer** hierarchy level specifies the policer to use for policing all non-continuity check packets of the CFM traffic belonging to all sessions. The **all *cfm-policer2*** statement specifies to police all CFM packets with the specified policer *cfm-policer2*. If the **all *policer-name*** option is used, then the user cannot specify the previous **continuity-check** and **other** options.

```
[edit protocols oam ethernet]
connectivity-fault-management {
  policer {
    continuity-check cfm-policer;
    other cfm-policer1;
    # all cfm-policer2;
  }
}
```

#### Case 2: Session-Level CFM Policing

This example shows a session-level CFM policer used for rate-limiting CFM. The **policer** statement at the session **connectivity-fault-management maintenance-domain *md* maintenance-association *ma*** hierarchy level specifies the policer to use for policing only continuity check packets of the CFM traffic belonging to the specified session. The **other *cfm-policer1*** statement at the **connectivity-fault-management maintenance-domain *md* maintenance-association *ma*** hierarchy level specifies the policer to use for policing all non-continuity check packets of the CFM traffic belonging to this session only. The **all *cfm-policer2*** statement specifies to police all CFM packets with the specified policer *cfm-policer2*. If the **all *policer-name*** option is used, then the user cannot specify the previous **continuity-check** and **other** options.

```
[edit protocols oam ethernet]
connectivity-fault-management {
  maintenance-domain md {
    level number;
    maintenance-association ma {
      continuity-check {
        interval 1s;
      }
      policer {
```

```
continuity-check cfm-policer;  
other cfm-policer1;  
# all cfm-policer2;  
}  
mep 1 {  
    interface ge-3/3/0.0;  
    direction up;  
    auto-discovery;  
}  
}  
}
```

In the case of global CFM policing, the same policer is shared across multiple CFM sessions. In per-session CFM policing, a separate policer must be created to rate-limit packets specific to that session.



NOTE:

Service-level policer configuration for any two CFM sessions on the same interface at different levels must satisfy the following constraints if the direction of the sessions is the same:

- If one session is configured with `policer all`, then the other session cannot have a `policer all` or `policer other` configuration.
- If one session is configured with `policer other`, then the other session cannot have a `policer all` or `policer other` configuration.

A commit error will occur if such a configuration is committed.



NOTE: Policers with PBB and MIPs are not supported.

---

## Configuring 802.1ag Ethernet OAM for VPLS

---



**BEST PRACTICE:** The logical interfaces in a VPLS routing instance may have the same or different VLAN configurations. VLAN normalization is required to switch packets correctly among these interfaces. VLAN normalization is effectively VLAN translation wherein the VLAN tags of the received packet need to be translated if they are different than the normalized VLAN tags. Configuration is described starting in “IEEE 802.1ag OAM Connectivity Fault Management Overview” on page 159 and you should further observe the additional requirements described in this section.

For MX Series routers, the normalized VLAN is specified using one of the following configuration statements in the VPLS routing instance:

- `vlan-id vlan-number`

- `vlan-id none`
- `vlan-tags outer outer-vlan-number inner inner-vlan-number`

You must configure `vlan-maps` explicitly on all interfaces belonging to the routing instance.

The following forwarding path considerations must be observed:

- Packet receive path:
  - This is the forwarding path for packets received on the interfaces.
  - 802.1ag Ethernet OAM for VPLS uses implicit interface filters and forwarding table filters to flood, accept, and drop the CFM packets.
- Packet transmit path:
  - The JUNOS Software uses the router's hardware-based forwarding for CPU-generated packets.
  - For Down MEPs, the packets are transmitted on the interface on which the MEP is configured.
  - For Up MEPs, the packet must be flooded to other interfaces in the VPLS routing instance. The router creates a flood route tied to a flood next hop (with all interfaces to flood) and then sources the packet to be forwarded with this flood route.
  - The router also uses implicit-based forwarding for CPU generated packets. The result is for the flood next hop tied to the flood route to be tied to the filter term. The filter term uses match criteria to correctly identify the host-generated packets.

---

**Related  
Documentation**

- Example: Configuring Ethernet CFM over VPLS
- IEEE 802.1ag OAM Connectivity Fault Management Overview on page 159



## CHAPTER 13

# Configuring ITU-T Y.1731 Ethernet Service OAM

- Service-Level Agreement Measurement on page 202
- Ethernet Frame Delay Measurements Overview on page 202
- Ethernet Frame Loss Measurement Overview on page 208
- On-Demand Mode on page 209
- Proactive Mode on page 210
- Configuring an Iterator Profile on page 211
- Configuring a Remote MEP with an Iterator Profile on page 213
- Configuring Statistical Frame Loss Measurement for VPLS Connections on page 214
- Guidelines for Configuring Routers to Support an ETH-DM Session on page 215
- Guidelines for Starting an ETH-DM Session on page 216
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts on page 218
- Configuring Routers to Support an ETH-DM Session on page 223
- Starting an ETH-DM Session on page 226
- Managing ETH-DM Statistics and ETH-DM Frame Counts on page 228
- Managing ETH-LM Statistics on page 231
- Managing Iterator Statistics on page 233
- Managing Continuity Measurement Statistics on page 238
- Example: One-Way Ethernet Frame Delay Measurement on page 238
- Example: Configuring an Iterator on page 246

## Service-Level Agreement Measurement

---

Service-level agreement (SLA) measurement is the process of monitoring the bandwidth, delay, delay variation (jitter), continuity, and availability of a service (E-Line or E-LAN). It enables you to identify network problems before customers are impacted by network defects.



---

**NOTE:**

The Ethernet VPN services can be classified into:

- Peer-to-peer-services (E-Line services)—The E-Line services are offered using MPLS-based Layer 2 VPN virtual private wire service (VPWS).
- Multipoint-to-multipoint services (E-LAN services)—The E-LAN services are offered using MPLS-based virtual private LAN service (VPLS).

For more information, see the *Junos VPNs Configuration Guide*.

---

In Junos OS, SLA measurements are classified into:

- On-demand mode—In on-demand mode, the measurements are triggered through the CLI. For more information, see “On-Demand Mode” on page 209.
- Proactive mode—In proactive mode, the measurements are triggered by an iterator application. For more information, see “Proactive Mode” on page 210.

For more information about frame delay measurement, see “Ethernet Frame Delay Measurements Overview” on page 202. For more information about frame loss measurement, see “Ethernet Frame Loss Measurement Overview” on page 208. Note that Ethernet frame delay measurement and Ethernet frame loss measurement are not supported on the **ae** interface.

**Related  
Documentation**

- Proactive Mode on page 210.
- On-Demand Mode on page 209.

## Ethernet Frame Delay Measurements Overview

---

- ITU-T Y.1731 Frame Delay Measurement Feature on page 203
- One-Way Ethernet Frame Delay Measurement on page 204
- Two-Way Ethernet Frame Delay Measurement on page 205
- Choosing Between One-Way and Two-Way ETH-DM on page 207
- Restrictions for Ethernet Frame Delay Measurement on page 207

## ITU-T Y.1731 Frame Delay Measurement Feature

The IEEE 802.3-2005 standard for Ethernet Operations, Administration, and Maintenance (OAM) defines a set of link fault management mechanisms to detect and report link faults on a single point-to-point Ethernet LAN.

Junos OS supports key OAM standards that provide for automated end-to-end management and monitoring of Ethernet service by service providers:

- *IEEE Standard 802.1ag*, also known as “Connectivity Fault Management (CFM).”
- *ITU-T Recommendation Y.1731*, which uses different terminology than IEEE 802.1ag and defines Ethernet service OAM features for fault monitoring, diagnostics, and performance monitoring.

These capabilities allow operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are tailored to the specific needs of their customers.

---

### Ethernet CFM

The IEEE 802.1ag standard for connectivity fault management (CFM) defines mechanisms to provide for end-to-end Ethernet service assurance over any path, whether a single link or multiple links spanning networks composed of multiple LANs.

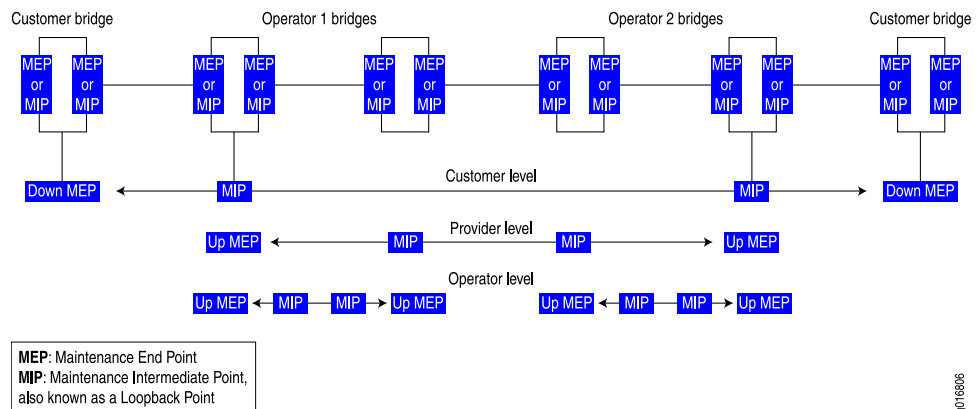
For Ethernet interfaces on M320, MX Series, and T Series routers, Junos OS supports the following key elements of the Ethernet CFM standard:

- Fault monitoring using the IEEE 802.1ag Ethernet OAM Continuity Check protocol
- Path discovery and fault verification using the IEEE 802.1ag Ethernet OAM Linktrace protocol
- Fault isolation using the IEEE 802.1ag Ethernet OAM Loopback protocol

In a CFM environment, network entities such as network operators, service providers, and customers may be part of different administrative domains. Each administrative domain is mapped into one maintenance domain. Maintenance domains are configured with different level values to keep them separate. Each domain provides enough information for the entities to perform their own management and end-to-end monitoring, and still avoid security breaches.

Figure 25 on page 204 shows the relationships among the customer, provider, and operator Ethernet bridges, maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs).

Figure 25: Relationship of MEPs, MIPs, and Maintenance Domain Levels



## Ethernet Frame Delay Measurement

Two key objectives of OAM functionality are to measure quality-of-service attributes such as frame delay and frame delay variation (also known as “frame jitter”). Such measurements can enable you to identify network problems before customers are impacted by network defects.

Junos OS supports Ethernet frame delay measurement between MEPs configured on Ethernet physical or logical interfaces on Dense Port Concentrators (DPCs) in MX Series routers. Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor SLAs. Ethernet frame delay measurement also collects other useful information, such as worst and best case delays, average delay, and average delay variation. The Junos OS implementation of Ethernet frame delay measurement (ETH-DM) is fully compliant with the ITU-T Recommendation Y.1731, *OAM Functions and Mechanisms for Ethernet-based Networks*. The recommendation defines OAM mechanisms for operating and maintaining the network at the Ethernet service layer, which is called the “ETH layer” in ITU-T terminology.

## One-Way Ethernet Frame Delay Measurement

In one-way ETH-DM mode, a series of frame delay and frame delay variation values are calculated based on the time elapsed between the time a measurement frame is sent from the initiator MEP at one router and the time when the frame is received at the receiver MEP at the other router.

### 1DM Transmission

When you start a one-way frame delay measurement, the router sends 1DM frames—frames that carry the protocol data unit (PDU) for a one-way delay measurement—from the initiator MEP to the receiver MEP at the rate and for the number of frames you specify. The router marks each 1DM frame as drop-ineligible and inserts a timestamp of the transmission time into the frame.

### 1DM Reception

When an MEP receives a 1DM frame, the router that contains the receiver MEP measures the one-way delay for that frame (the difference between the time the frame was received



and the timestamp contained in the frame itself) and the delay variation (the difference between the current and previous delay values).

---

### One-Way ETH-DM Statistics

The router that contains the receiver MEP stores each set of one-way delay statistics in the ETH-DM database. The ETH-DM database collects up to 100 sets of statistics for any given CFM session (pair of peer MEPs). You can access these statistics at any time by displaying the ETH-DM database contents.

---

### One-Way ETH-DM Frame Counts

Each router counts the number of one-way ETH-DM frames sent and received:

- For an initiator MEP, the router counts the number of 1DM frames sent.
- For a receiver MEP, the router counts the number of valid 1DM frames received and the number of invalid 1DM frames received.

Each router stores ETH-DM frame counts in the CFM database. The CFM database stores CFM session statistics and, for interfaces that support ETH-DM, any ETH-DM frame counts. You can access the frame counts at any time by displaying CFM database information for Ethernet interfaces assigned to MEPs or for MEPs in CFM sessions.

---

### Synchronization of System Clocks

The accuracy of one-way delay calculations depends on close synchronization of the system clocks at the initiator MEP and receiver MEP.

The accuracy of one-way delay variation is not dependent on system clock synchronization. Because delay variation is simply the difference between consecutive one-way delay values, the out-of-phase period is eliminated from the frame jitter values.



**NOTE:** For a given one-way Ethernet frame delay measurement, frame delay and frame delay variation values are available only on the router that contains the receiver MEP.

---

## Two-Way Ethernet Frame Delay Measurement

In two-way ETH-DM mode, frame delay and frame delay variation values are based on the time difference between when the initiator MEP transmits a request frame and receives a reply frame from the responder MEP, subtracting the time elapsed at the responder MEP.

---

### DMM Transmission

When you start a two-way frame delay measurement, the router sends delay measurement message (DMM) frames—frames that carry the PDU for a two-way ETH-DM request—from the initiator MEP to the responder MEP at the rate and for the number of frames you specify. The router marks each DMM frame as drop-ineligible and inserts a timestamp of the transmission time into the frame.

### DMR Transmission

---

When an MEP receives a DMM frame, the responder MEP responds with a delay measurement reply (DMR) frame, which carries ETH-DM reply information and a copy of the timestamp contained in the DMM frame.

### DMR Reception

---

When an MEP receives a valid DMR, the router that contains the MEP measures the two-way delay for that frame based on the following sequence of timestamps:

1.  $TI_{TxDMM}$
2.  $TR_{RxDMM}$
3.  $TR_{TxDMR}$
4.  $TI_{RxDMR}$

A two-way frame delay is calculated as follows:

$$[TI_{RxDMR} - TI_{TxDMM}] - [TR_{TxDMR} - TR_{RxDMM}]$$

In other words, frame delay is the difference between the time at which the initiator MEP sends a DMM frame and the time at which the initiator MEP receives the associated DMR frame from the responder MEP, minus the time elapsed at the responder MEP.

The delay variation is the difference between the current and previous delay values.

### Two-Way ETH-DM Statistics

---

The router that contains the initiator MEP stores each set of two-way delay statistics in the ETH-DM database. The ETH-DM database collects up to 100 sets of statistics for any given CFM session (pair of peer MEPs). You can access these statistics at any time by displaying the ETH-DM database contents.

### Two-Way ETH-DM Frame Counts

---

Each router counts the number of two-way ETH-DM frames sent and received:

- For an initiator MEP, the router counts the number DMM frames transmitted, the number of valid DMR frames received, and the number of invalid DMR frames received.
- For a responder MEP, the router counts the number of DMR frames sent.

Each router stores ETH-DM frame counts in the CFM database. The CFM database stores CFM session statistics and, for interfaces that support ETH-DM, any ETH-DM frame counts. You can access the frame counts at any time by displaying CFM database information for Ethernet interfaces assigned to MEPs or for MEPs in CFM sessions.



**NOTE:** For a given two-way Ethernet frame delay measurement, frame delay and frame delay variation values are available only at the router that contains the initiator MEP.

---

## Choosing Between One-Way and Two-Way ETH-DM

One-way frame delay measurement requires that the system clocks at the initiator MEP and receiver MEP are closely synchronized. Two-way frame delay measurement does not require synchronization of the two systems. If it is not practical for the clocks to be synchronized, two-way frame delay measurements are more accurate.

When two systems are close to each other, their one-way delay values are very high compared to their two-way delay values. This is because one-way delay measurement requires that the timing for the two systems be synchronized at a very granular level, and MX Series routers currently do not support this granular synchronization.

## Restrictions for Ethernet Frame Delay Measurement

The following restrictions apply to the Ethernet frame delay measurement feature:

- The Ethernet frame delay measurement feature is supported only for MEPs configured on Ethernet physical or logical interfaces on DPCs in MX Series routers. The ETH-DM feature is not supported on aggregated Ethernet interfaces or label-switched interface (LSI) pseudowires.
- Hardware-assisted timestamping for ETH-DM frames in the reception path is only supported for MEP interfaces on Enhanced DPCs and Enhanced Queuing DPCs in MX Series routers. For information about hardware-assisted timestamping, see “Guidelines for Configuring Routers to Support an ETH-DM Session” on page 215 and “Enabling the Hardware-Assisted Timestamping Option” on page 225.
- Ethernet frame delay measurements can be triggered only when the distributed periodic packet management daemon (**ppm**) is enabled. For more information about this limitation, see “Guidelines for Configuring Routers to Support an ETH-DM Session” on page 215 and “Ensuring that Distributed ppm Is Not Disabled” on page 224.
- You can monitor only one session at a time to the same remote MEP or MAC address. For more information about starting an ETH-DM session, see “Starting an ETH-DM Session” on page 226.
- ETH-DM statistics are collected at only one of the two peer routers in the ETH-DM session. For a one-way ETH-DM session, you can display frame ETH-DM statistics at the receiver MEP only, using ETH-DM-specific **show** commands. For a two-way ETH-DM session, you can display frame delay statistics at the initiator MEP only, using the same ETH-DM-specific **show** commands. For more information, see “Managing ETH-DM Statistics and ETH-DM Frame Counts” on page 228.
- ETH-DM frame counts are collected at both MEPs and are stored in the respective CFM databases.
- If graceful Routing Engine switchover (GRES) occurs, any collected ETH-DM statistics are lost, and ETH-DM frame counts are reset to zeroes. Therefore, the collection of ETH-DM statistics and ETH-DM frame counters has to be restarted, after the switchover is complete. GRES enables a router with dual Routing Engines to switch from a master

Routing Engine to a backup Routing Engine without interruption to packet forwarding. For more information, see the [Junos OS High Availability Configuration Guide](#).

- Accuracy of frame delay statistics is compromised when the system is changing (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

**Related  
Documentation**

- Guidelines for Configuring Routers to Support an ETH-DM Session on page 215
- Guidelines for Starting an ETH-DM Session on page 216
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts on page 218
- Example: One-Way Ethernet Frame Delay Measurement on page 238

---

## Ethernet Frame Loss Measurement Overview

---

The key objectives of the OAM functionality are to measure quality-of-service attributes such as frame delay, frame delay variation (also known as “frame jitter”), and frame loss. Such measurements enable you to identify network problems before customers are impacted by network defects. For more information about Ethernet frame delay measurement, see “Ethernet Frame Delay Measurements Overview” on page 202.

Junos OS supports Ethernet frame loss measurement (ETH-LM) between maintenance association end points (MEPs) configured on Ethernet physical or logical interfaces on Rev-B Dense Port Concentrators (DPCs) in MX Series routers and is presently supported only for VPWS service. ETH-LM is used by operators to collect counter values applicable for ingress and egress service frames. These counters maintain a count of transmitted and received data frames between a pair of MEPs. Ethernet frame loss measurement is performed by sending frames with ETH-LM information to a peer MEP and similarly receiving frames with ETH-LM information from the peer MEP. This type of frame loss measurement is also known as single-ended Ethernet loss measurement.

ETH-LM supports the following frame loss measurements:

- Near-end frame loss measurement—Measurement of frame loss associated with ingress data frames.
- Far-end frame loss measurement—Measurement of frame loss associated with egress data frames.

The Junos OS implementation of Ethernet frame delay measurement (ETH-DM) is fully compliant with the ITU-T Recommendation Y.1731, as described in *OAM Functions and Mechanisms for Ethernet-Based Networks*. The recommendation defines OAM mechanisms for operating and maintaining the network at the Ethernet service layer, which is called the “ETH layer” in ITU-T terminology.

**Related  
Documentation**

- Proactive Mode on page 210.
- On-Demand Mode on page 209.
- Managing Continuity Measurement Statistics on page 238

## On-Demand Mode

---

In on-demand mode, the measurements are triggered by the user through the CLI.

When the user triggers the delay measurement through the CLI, the delay measurement request that is generated is as per the frame formats specified by the ITU-T Y.1731 standard. For two-way delay measurement, the server-side processing can be delegated to the Packet Forwarding Engine to prevent overloading on the Routing Engine. For more information, see “Configuring Routers to Support an ETH-DM Session” on page 223. When the server-side processing is delegated to the Packet Forwarding Engine, the delay measurement message (DMM) frame **receive** counters and delay measurement reply (DMR) frame **transmit** counters are not displayed by the **show** command.

When the user triggers the loss measurement through the CLI, the router sends the packets in standard format along with the loss measurement TLV. By default, the **session-id-tlv** argument is included in the packet to allow concurrent loss measurement sessions from same local MEP. You can also disable the session ID TLV by using the **no-session-id-tlv** argument.

Single-ended ETH-LM is used for on-demand operation, administration, and maintenance purposes. An MEP sends frames with ETH-LM request information to its peer MEP and receives frames with ETH-LM reply information from its peer MEP to carry out loss measurements. The protocol data unit (PDU) used for a single-ended ETH-LM request is referred to as a loss measurement message (LMM) and the PDU used for a single-ended ETH-LM reply is referred to as a loss measurement reply (LMR).

### Related Documentation

- Configuring Routers to Support an ETH-DM Session on page 223.

## Proactive Mode

---

In proactive mode, SLA measurements are triggered by an iterator application. An iterator is designed to periodically transmit SLA measurement packets in form of ITU-Y.1731-compliant frames for two-way delay measurement or loss measurement and is supported on Rev-B DPCs on MX Series routers. This mode differs from on-demand SLA measurement, which is user initiated. The iterator sends periodic delay or loss measurement request packets for each of the connections registered to it. Iterators make sure that measurement cycles do not occur at the same time for the same connection to avoid CPU overload. Junos OS supports proactive mode for VPWS. For an iterator to form a remote adjacency and to become functionally operational, the continuity check message (CCM) must be active between the local and remote MEP configurations of the connectivity fault management (CFM). Any change in the iterator adjacency parameters resets the existing iterator statistics and restarts the iterator. Here, the term adjacency refers to a pairing of two endpoints (either connected directly or virtually) with relevant information for mutual understanding, which is used for subsequent processing. For example, the iterator adjacency refers to the iterator association between the two endpoints of the MEPs.

For every DPC, only 30 iterator instances for a cycle time value of 10 milliseconds (ms) are supported. In Junos OS, 255 iterator profile configurations and 2000 remote MEP associations are supported.

Iterators with cycle time value less than 100 ms are supported only for infinite iterators, whereas the iterators with cycle time value greater than 100 ms are supported for both finite and infinite iterators. Infinite iterators are iterators that run infinitely until the iterator is disabled or deactivated manually.

A VPWS service configured on a router is monitored for SLA measurements by registering the connection (here, the connection is a pair of remote and local MEPs) on an iterator and then initiating periodic SLA measurement frame transmission on those connections. The end-to-end service is identified through a maintenance association end point (MEP) configured at both ends.

For two-way delay measurement and loss measurement, an iterator sends a request message for the connection in the list (if any) and then sends a request message for the connection that was polled in the former iteration cycle. The back-to-back request messages for the SLA measurement frames and their responses help in computing delay variation and loss measurement.

The Y.1731 frame transmission for a service attached to an iterator continues endlessly unless intervened and stopped by an operator or until the iteration-count condition is met. To stop the iterator from sending out any more proactive SLA measurement frames, the operator must perform one of the following tasks:

- Enable the **deactivate sla-iterator-profile** statement at the **[edit protocols oam ethernet connectivity-fault-management maintenance-domain *md-name* maintenance association *ma-name* mep *mep-id* remote-mep *mep-id*]** hierarchy level. For more information, see “Example: Configuring an Iterator” on page 246.

- Provision a **disable** statement under the corresponding iterator profile at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles *profile-name*]** hierarchy level. For more information, see “Configuring an Iterator Profile” on page 211.

## Ethernet Delay Measurements and Loss Measurement by Proactive Mode

In two-way delay measurement, the delay measurement message (DMM) frame is triggered through an iterator application. The DMM frame carries an iterator type, length, and value (TLV) in addition to the fields described in standard frame format and the server copies the iterator TLV from the DMM frame to the delay measurement reply (DMR) frame.

In one-way delay variation computation using the two-way delay measurement method, the delay variation computation is based on the timestamps that are present in the DMR frame (and not the IDM frame). Therefore, there is no need for client-side and server-side clocks to be in sync. Assuming that the difference in their clocks remains constant, the one-way delay variation results are expected to be fairly accurate. This method also eliminates the need to send separate IDM frames just for the one-way delay variation measurement purpose.

In proactive mode for loss measurement, the router sends packets in standard format along with loss measurement TLV and iterator TLV.

### Related Documentation

- Clearing Iterator Statistics on page 237
- Configuring an Iterator Profile on page 211
- Configuring a Remote MEP with an Iterator Profile on page 213
- Example: Configuring an Iterator on page 246
- Displaying Iterator Statistics on page 233
- Managing Iterator Statistics on page 233

## Configuring an Iterator Profile

You can create an iterator profile with its parameters to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for delay measurement or loss measurement.

To create an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
performance-monitoring
```

2. Configure the SLA measurement monitoring iterator:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# edit sla-iterator-profiles
```

3. Configure an iterator profile—for example, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles]
user@host# set i1
```

4. (Optional) Configure the cycle time, which is the amount of time (in milliseconds) between back-to-back transmission of SLA frames for one connection, with values from 10 through 3,600,000. The default value is 1000 ms.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set cycle-time cycle-time-value
```

5. (Optional) Configure the iteration period, which indicates the maximum number of cycles per iteration (the number of connections registered to an iterator cannot exceed this value), with values from 1 through 2000. The default value is 2000.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set iteration-period iteration-period-value
```

6. Configure the measurement type as loss measurement, statistical frame-loss measurement, or two-way delay measurement.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set measurement-type (loss | statistical-frame-loss | two-way-delay)
```

7. (Optional) Configure the calculation weight for delay with values from 1 through 65,535. The default value is 1 (applicable only for two-way delay measurement).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set calculation-weight delay delay-value
```

8. (Optional) Configure the calculation weight for delay variation with values from 1 through 65,535. The default value is 1 (applicable only for two-way delay measurement).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set calculation-weight delay-variation delay-variation-value
```

9. Configure the **disable** statement to stop the iterator (that is, disable the iterator profile).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles i1]
user@host# set disable
```

10. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles]
user@host# show i1
  cycle-time cycle-time-value;
  iteration-period iteration-period-value;
  measurement-type (loss | two-way-delay);
  calculation-weight {
    delay delay-weight;
```



```

        delay-variation delay-variation-weight;
    }

```

#### Related Documentation

- Proactive Mode on page 210
- Clearing Iterator Statistics on page 237
- Configuring a Remote MEP with an Iterator Profile on page 213
- Example: Configuring an Iterator on page 246
- Displaying Iterator Statistics on page 233
- Managing Iterator Statistics on page 233

## Configuring a Remote MEP with an Iterator Profile

You can associate a remote maintenance association end point (MEP) with more than one iterator profile.

To configure a remote MEP with an iterator profile:

1. In configuration mode, go to the following hierarchy level:

```

user@host# edit protocols oam ethernet connectivity-fault-management
maintenance-domain md-name maintenance-association ma-name mep mep-id

```

2. Configure the remote MEP with values from 1 through 8191.

```

[edit protocols oam ethernet connectivity-fault-management maintenance-domain
md-name maintenance-association ma-name mep mep-id]
user@host# set remote-mep remote-mep-id

```

3. Set the iterator profile.

```

[edit protocols oam ethernet connectivity-fault-management maintenance-domain
md-name maintenance-association ma-name mep mep-id remote-mep
remote-mep-id]
user@host# set sla-iterator-profile profile-name

```

4. (Optional) Set the size of the data TLV portion of the Y.1731 data frame with values from 1 through 1400 bytes. The default value is 1.

```

[edit protocols oam ethernet connectivity-fault-management maintenance-domain
md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id
sla-iterator-profile profile-name]
user@host# set data-tlv-size size

```

5. (Optional) Set the iteration count, which indicates the number of iterations for which this connection should partake in the iterator for acquiring SLA measurements, with values from 1 through 65,535. The default value is 0 (that is, infinite iterations).

```

[edit protocols oam ethernet connectivity-fault-management maintenance-domain
md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id
sla-iterator-profile profile-name]
user@host# set iteration-count count-value

```

6. (Optional) Set the priority, which is the **vlan-pcp** value that is sent in the Y.1731 data frames, with values from 0 through 7. The default value is 0.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id
  sla-iterator-profile profile-name]
user@host# set priority priority-value
```

7. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  md-name maintenance-association ma-name mep mep-id remote-mep
  remote-mep-id]
user@host# show
sla-iterator-profile profile-name {
  data-tlv-size size;
  iteration-count count-value;
  priority priority-value;
}
```

**Related  
Documentation**

- Proactive Mode on page 210
- Clearing Iterator Statistics on page 237
- Configuring an Iterator Profile on page 211
- Example: Configuring an Iterator on page 246
- Displaying Iterator Statistics on page 233
- Managing Iterator Statistics on page 233

---

## Configuring Statistical Frame Loss Measurement for VPLS Connections

Using proactive statistical frame loss measurement, you can monitor VPLS connections on MX Series routers with Rev-B DPCs. Statistical frame loss measurement allows you to monitor the quality of Ethernet connections for service level agreements (SLAs). Point-to-point and multipoint-to-multipoint connections configured on MX Series routers can be monitored by registering the connection on an iterator and initiating periodic SLA measurement of frame transmissions on the connections.

Iterators periodically transmit SLA measurement packets using ITU-Y.1731 compliant frames. The iterator sends periodic measurement packets for each of the connections registered to it. These measurement cycles are transmitted in such a way as to not overlap, reducing the processing demands placed on the CPU. The measurement packets are exchanged between the source user network interface (UNI) port and the destination UNI port, providing a sequence of timed performance measurements for each UNI pair. The Frame Loss Ratio (FLR) and connection availability can be computed from these measurements using statistics.

The following steps outline how to configure statistical frame loss measurement for VPLS connections:

1. To configure proactive ETH-DM measurement for a VPLS connection, see “Guidelines for Configuring Routers to Support an ETH-DM Session” on page 215.
2. To enable statistical loss measurement for a VPLS connection, configure an iterator for the VPLS connection using the `sla-iterator-profiles` statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level. For detailed instructions, see “Configuring an Iterator Profile” on page 211.
3. As part of the iterator configuration, include the **statistical-frame-loss** option for the `measurement-type` statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]** hierarchy level.
4. Once you have enabled the iterator, you can display the statistical frame loss for a VPLS connection by issuing the `show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator identifier maintenance-domain name maintenance-association name local-mep identifier remote-mep identifier` command.

#### Related Documentation

- Guidelines for Configuring Routers to Support an ETH-DM Session on page 215
- Configuring an Iterator Profile on page 211
- Example: Configuring an Iterator on page 246

## Guidelines for Configuring Routers to Support an ETH-DM Session

Keep the following guidelines in mind when configuring routers to support an Ethernet frame delay measurement (ETH-DM) session:

- Configuration Requirements for ETH-DM on page 215
- Configuration Options for ETH-DM on page 216

### Configuration Requirements for ETH-DM

You can obtain ETH-DM information for a link that meets the following requirements:

- The measurements can be performed between peer maintenance association endpoints (MEPs) on two routers.
- The two MEPs must be configured on two Ethernet physical interfaces or on two Ethernet logical interfaces. For more information, see “Configuring a Maintenance Endpoint” on page 166.
- The two MEPs must be configured—on their respective routers—under the same maintenance association (MA) identifier. For more information, see “Creating a Maintenance Association” on page 163.
- On both routers, the MA must be associated with the same maintenance domain (MD) name. For more information, see “Creating the Maintenance Domain” on page 161.

- On both routers, periodic packet management (PPM) must be running on the Routing Engine and Packet Forwarding Engine, which is the default configuration. You can disable PPM on the Packet Forwarding Engine only. However, the Ethernet frame delay measurement feature requires that distributed PPM remain enabled on the Packet Forwarding Engine of both routers. For more information about **ppm**, see the *Junos OS Routing Protocols Configuration Guide*.
- If the PPM process (**ppm**) is disabled on the Packet Forwarding Engine, you must re-enable it. Re-enabling distributed **ppm** entails restarting the **ethernet-connectivity-fault-management** process, which causes all connectivity fault management (CFM) sessions to re-establish. For more information about CFM sessions, see “Configuring Ethernet Local Management Interface” on page 173.



**NOTE:** The Ethernet frame delay measurement feature is supported only for MEPs configured on Ethernet physical or logical interfaces on DPCs in MX Series routers. The ETH-DM feature is not supported on aggregated Ethernet interfaces or LSI pseudowires.

---

## Configuration Options for ETH-DM

By default, the ETH-DM feature calculates frame delays using software-based timestamping of the ETH-DM PDU frames sent and received by the MEPs in the session. As an option that can increase the accuracy of ETH-DM calculations when the DPC is loaded with heavy traffic in the receive direction, you can enable hardware-assisted timestamping of session frames in the receive direction.



**NOTE:** Hardware-assisted timestamping for ETH-DM frames is only supported for MEP interfaces on Enhanced DPCs and Enhanced Queuing DPCs in MX Series routers.

### Related Documentation

- Ethernet Frame Delay Measurements Overview on page 202
- Configuring Routers to Support an ETH-DM Session on page 223

---

## Guidelines for Starting an ETH-DM Session

Keep the following guidelines in mind when preparing to start an Ethernet frame delay measurement (ETH-DM) session:

- ETH-DM Session Prerequisites on page 216
- ETH-DM Session Parameters on page 217
- Restrictions for an ETH-DM Session on page 218

### ETH-DM Session Prerequisites

Before you can start an ETH-DM session, you must configure two MX Series routers to support ETH-DM by defining the two CFM-enabled physical or logical Ethernet interfaces

on each router. This entails creating and configuring CFM maintenance domains, maintenance associations, and maintenance association end points on each router. For more information about enabling CFM on an Ethernet interface, see “Creating the Maintenance Domain” on page 161.



**NOTE:** The Ethernet frame delay measurement feature is supported only for maintenance association end points configured on Ethernet physical or logical interfaces on DPCs in MX Series routers. The ETH-DM feature is not supported on aggregated Ethernet interfaces or LSI pseudowires.

For specific information about configuring routers to support ETH-DM, see “Guidelines for Configuring Routers to Support an ETH-DM Session” on page 215 and “Configuring Routers to Support an ETH-DM Session” on page 223.

## ETH-DM Session Parameters

You can initiate a one-way or two-way ETH-DM session by entering the **monitor ethernet delay-measurement** operational command at a router that contains one end of the service for which you want to measure frame delay. The command options specify the ETH-DM session in terms of the CFM elements:

- The type of ETH-DM measurement (one-way or two-way) to be performed.
- The Ethernet service for which the ETH-DM measurement is to be performed:
  - CFM maintenance domain—Name of the existing maintenance domain (MD) for which you want to measure Ethernet frame delays. For more information, see “Creating the Maintenance Domain” on page 161.
  - CFM maintenance association—Name of an existing maintenance association (MA) within the maintenance domain. For more information, see “Creating a Maintenance Association” on page 163.
  - Remote CFM maintenance association end point—The unicast MAC address or the numeric identifier of the remote maintenance association end point (MEP)—the physical or logical interface on the remote router that resides in the specified MD and is named in the specified MA—with which to perform the ETH-DM session. For more information, see “Configuring a Maintenance Endpoint” on page 166.
- Optional specifications:
  - Count—You can specify the number of ETH-DM requests to send for this frame delay measurement session. The range is from 1 through 65,535 frames. The default value is 10 frames.

**NOTE:** Although you can trigger frame delay collection for up to 65,535 ETH-DM requests at a time, a router stores only the last 100 frame delay statistics per CFM session (pair of peer MEPs).

- Frame interval—You can specify the number of seconds to elapse between ETH-DM frame transmittals. The default value is 1 second.

For more detailed information about the parameters you can specify to start an ETH-DM session, see the **monitor ethernet delay-measurement** operational command description in the *Junos OS System Basics and Services Command Reference*.

## Restrictions for an ETH-DM Session

The following restrictions apply to an ETH-DM session:

- You cannot run multiple simultaneous ETH-DM sessions with the same remote MEP or MAC address.
- For a given ETH-DM session, you can collect frame delay information for a maximum of 65,535 frames.
- For a given CFM session (pair of peer MEPs), the ETH-DM database stores a maximum of 100 statistics, with the older statistics being “aged out” as newer statistics are collected for that pair of MEPs.
  - For one-way delay measurements collected within the same CFM session, the 100 most recent ETH-DM statistics can be retrieved at any point of time at the router on which the receiver MEP is defined.
  - For two-way delay measurements collected within the same CFM session, the 100 most recent ETH-DM statistics can be retrieved at any point of time at the router on which the initiator MEP is defined.

Depending on the number of frames exchanged in the individual ETH-DM sessions, the ETH-DM database can contain statistics collected through multiple ETH-DM sessions.

- If graceful Routing Engine switchover (GRES) occurs, any collected ETH-DM statistics are lost, and ETH-DM frame counts are reset to zeroes. GRES enables a router with dual Routing Engines to switch from a master Routing Engine to a backup Routing Engine without interruption to packet forwarding. For more information, see the *Junos OS High Availability Configuration Guide*.
- Accuracy of frame delay data is compromised when the system is changing (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

### Related Documentation

- Ethernet Frame Delay Measurements Overview on page 202
- Starting an ETH-DM Session on page 226
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts on page 218
- **monitor ethernet delay-measurement** operational command

---

## Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts

- ETH-DM Statistics on page 219
- ETH-DM Statistics Retrieval on page 220

- ETH-DM Frame Counts on page 221
- ETH-DM Frame Count Retrieval on page 221

## ETH-DM Statistics

Ethernet frame delay statistics are the frame delay and frame delay variation values determined by the exchange of frames containing ETH-DM protocol data units (PDUs).

- For a one-way ETH-DM session, statistics are collected in an ETH-DM database at the router that contains the receiver MEP. For a detailed description of one-way Ethernet frame delay measurement, including the exchange of one-way delay PDU frames, see “Ethernet Frame Delay Measurements Overview” on page 202.
- For a two-way ETH-DM session, statistics are collected in an ETH-DM database at the router that contains the initiator MEP. For a detailed description of two-way Ethernet frame delay measurement, including the exchange of two-way delay PDU frames, see “Ethernet Frame Delay Measurements Overview” on page 202.

A CFM database stores CFM-related statistics and—for Ethernet interfaces that support ETH-DM—the 100 most recently collected ETH-DM statistics for that pair of MEPs. You can view ETH-DM statistics by using the **delay-statistics** or **mep-statistics** form of the **show oam ethernet connectivity-fault-management** command to display the CFM statistics for the MEP that collects the ETH-DM statistics you want to view.

Table 23 on page 219 describes the ETH-DM statistics calculated in an ETH-DM session.

**Table 23: ETH-DM Statistics**

Field Name	Field Description
<b>One-way delay (μsec)<sup>†</sup></b>	<p>For a one-way ETH-DM session, the frame delay, in microseconds, collected at the receiver MEP.</p> <p>To display frame delay statistics for a given one-way ETH-DM session, use the <b>delay-statistics</b> or <b>mep-statistics</b> form of the <b>show oam ethernet connectivity-fault-management</b> command at the receiver MEP for that session.</p>
<b>Two-way delay (μsec)</b>	<p>For a two-way ETH-DM session, the frame delay, in microseconds, collected at the initiator MEP.</p> <p>When you start a two-way frame delay measurement, the CLI output displays each DMR frame receipt timestamp and corresponding DMM frame delay and delay variation collected as the session progresses.</p> <p>To display frame delay statistics for a given two-way ETH-DM session, use the <b>delay-statistics</b> or <b>mep-statistics</b> form of the <b>show oam ethernet connectivity-fault-management</b> command at the initiator MEP for that session.</p>

Table 23: ETH-DM Statistics (*continued*)

Field Name	Field Description
<b>Average delay</b> <sup>†</sup>	<p>When you start a two-way frame delay measurement, the CLI output includes a runtime display of the average two-way frame delay among the statistics collected for the ETH-DM session only.</p> <p>When you display ETH-DM statistics using a <b>show</b> command, the <b>Average delay</b> field displays the average one-way and two- frame delays among all ETH-DM statistics collected at the CFM session level.</p> <p>For example, suppose you start two one-way ETH-DM sessions for 50 counts each, one after the other. If, after both measurement sessions complete, you use a <b>show</b> command to display 100 ETH-DM statistics for that CFM session, the <b>Average delay</b> field displays the average frame delay among all 100 statistics.</p>
<b>Average delay variation</b> <sup>†</sup>	<p>When you start a two-way frame delay measurement, the CLI output includes a runtime display of the average two-way frame delay variation among the statistics collected for the ETH-DM session only.</p> <p>When you display ETH-DM statistics using a <b>show</b> command, the <b>Average delay variation</b> field displays the average one-way and two- frame delay variations among all ETH-DM statistics collected at the CFM session level.</p>
<b>Best-case delay</b> <sup>†</sup>	<p>When you start a two-way frame delay measurement, the CLI output includes a runtime display of the lowest two-way frame delay value among the statistics collected for the ETH-DM session only.</p> <p>When you display ETH-DM statistics using a <b>show</b> command, the <b>Best case delay</b> field displays the lowest one-way and two-way frame delays among all ETH-DM statistics collected at the CFM session level.</p>
<b>Worst-case delay</b> <sup>†</sup>	<p>When you start a two-way frame delay measurement, the CLI output includes a runtime display of the highest two-way frame delay value among the statistics collected for the ETH-DM session only.</p> <p>When you display ETH-DM statistics using a <b>show</b> command, the <b>Worst case delay</b> field displays the highest one-way and two-way frame delays among all statistics collected at the CFM session level.</p>

<sup>†</sup>When you start a one-way frame delay measurement, the CLI output displays **NA** ("not available") for this field. One-way ETH-DM statistics are collected at the remote (receiver) MEP. Statistics for a given one-way ETH-DM session are available only by displaying CFM statistics for the receiver MEP.

## ETH-DM Statistics Retrieval

At the receiver MEP for a one-way session, or at the initiator MEP for a two-way session, you can display all ETH-DM statistics collected at a CFM session level by using the following operational commands:

- **show oam ethernet connectivity-fault-management delay-statistics**  
**maintenance-domain** *md-name* **maintenance-association** *ma-name* <local-mep *mep-id*>  
<remote-mep *mep-id*> <count *count*>



- **show oam ethernet connectivity-fault-management mep-statistics**  
**maintenance-domain** *md-name* **maintenance-association** *ma-name* **<local-mep** *mep-id* **<remote-mep** *mep-id* **<count** *count* **>**

## ETH-DM Frame Counts

The number of ETH-DM PDU frames exchanged in a ETH-DM session are stored in the CFM database on each router.

Table 24 on page 221 describes the ETH-DM frame counts collected in an ETH-DM session.

**Table 24: ETH-DM Frame Counts**

Field Name	Field Description
<b>1DMs sent</b>	Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session.  Stored in the CFM database of the MEP initiating a one-way frame delay measurement.
<b>Valid 1DMs received</b>	Number of valid 1DM frames received.  Stored in the CFM database of the MEP receiving a one-way frame delay measurement.
<b>Invalid 1DMs received</b>	Number of invalid 1DM frames received.  Stored in the CFM database of the MEP receiving a one-way frame delay measurement.
<b>DMMs sent</b>	Number of delay measurement message (DMM) PDU frames sent to the peer MEP in this session.  Stored in the CFM database of the MEP initiating a two-way frame delay measurement.
<b>DMRs sent</b>	Number of delay measurement reply (DMR) frames sent (in response to a received DMM).  Stored in the CFM database of the MEP responding to a two-way frame delay measurement.
<b>Valid DMRs received</b>	Number of valid DMR frames received.  Stored in the CFM database of the MEP initiating a two-way frame delay measurement.
<b>Invalid DMRs received</b>	Number of invalid DMR frames received.  Stored in the CFM database of the MEP initiating a two-way frame delay measurement.

## ETH-DM Frame Count Retrieval

Each router counts the number of ETH-DM frames sent or received and stores the counts in a CFM database.

### Frame Counts Stored in CFM Databases

You can display ETH-DM frame counts for MEPs assigned to specified Ethernet interfaces or for specified MEPs in CFM sessions by using the following operational commands:

- **show oam ethernet connectivity-fault-management interfaces** (**detail** | **extensive**)

- **show oam ethernet connectivity-fault-management mep-database**  
**maintenance-domain** *md-name* **maintenance-association** *ma-name* <local-mep *mep-id*>  
<remote-mep *mep-id*>

---

### One-Way ETH-DM Frame Counts

For a one-way ETH-DM session, delay statistics are collected at the receiver MEP only, but frame counts are collected at both MEPs. As indicated in Table 24 on page 221, one-way ETH-DM frame counts are tallied from the perspective of each router in the session:

- At the initiator MEP, the router counts the number of 1DM frames sent.
- At the receiver MEP, the router counts the number of valid 1DM frames received and the number of invalid 1DM frames received.

You can also view one-way ETH-DM frame counts—for a receiver MEP—by using the **show oam ethernet connectivity-fault-management mep-statistics** command to display one-way statistics and frame counts together.

---

### Two-Way ETH-DM Frame Counts

For a two-way ETH-DM session, delay statistics are collected at the initiator MEP only, but frame counts are collected at both MEPs. As indicated in Table 24 on page 221, two-way ETH-DM frame counts are tallied from the perspective of each router in the session:

- At the initiator MEP, the router counts the number of DMM frames sent, valid DMR frames received, and invalid DMR frames received.
- At the responder MEP, the router counts the number of DMR frames sent.

You can also view two-way ETH-DM frame counts—for an initiator MEP—by using the **show oam ethernet connectivity-fault-management mep-statistics** command to display two-way statistics and frame counts together.

#### Related Documentation

- Ethernet Frame Delay Measurements Overview on page 202
- Managing ETH-DM Statistics and ETH-DM Frame Counts on page 228
- Example: One-Way Ethernet Frame Delay Measurement on page 238
- **clear oam ethernet connectivity-fault-management statistics** command
- **show oam ethernet connectivity-fault-management mep-statistics** command
- **show oam ethernet connectivity-fault-management delay-statistics** command
- **show oam ethernet connectivity-fault-management interfaces (detail | extensive)** command
- **show oam ethernet connectivity-fault-management mep-database** command

## Configuring Routers to Support an ETH-DM Session

- Configuring MEP Interfaces on page 223
- Ensuring that Distributed ppm Is Not Disabled on page 224
- Enabling the Hardware-Assisted Timestamping Option on page 225
- Configuring the Server-Side Processing Option on page 226

### Configuring MEP Interfaces

Before you can start an Ethernet frame delay measurement session across an Ethernet service, you must configure two MX Series routers to support ETH-DM.

To configure an Ethernet interface on a DPC in MX Series router to support ETH-DM:

1. On each router, configure two physical or logical Ethernet interfaces connected by a VLAN. The following configuration is typical for single-tagged logical interfaces:

```
[edit interfaces]
interface {
  ethernet-interface-name {
    vlan-tagging;
    unit logical-unit-number {
      vlan-id vlan-id; # Both interfaces on this VLAN
    }
  }
}
```

Both interfaces will use the same VLAN ID.

2. On each router, attach peer MEPs to the two interfaces. The following configuration is typical:

```
[edit protocols]
oam {
  ethernet {
    connectivity-fault-management {
      maintenance-domain md-name { # On both routers
        level number;
        maintenance-association ma-name { # On both routers
          continuity-check {
            interval 100ms;
            hold-interval 1;
          }
          mep mep-id { # Attach to VLAN interface
            auto-discovery;
            direction (up | down);
            interface interface-name;
            priority number;
          }
        }
      }
    }
  }
}
```

## Ensuring that Distributed ppm Is Not Disabled

By default, the router's period packet management process (**ppm**) runs sessions distributed to the Packet Forwarding Engine in addition to the Routing Engine. This process is responsible for periodic transmission of packets on behalf of its various client processes, such as Bidirectional Forwarding Detection (BFD), and it also receives packets on behalf of client processes.

In addition, **ppm** handles time-sensitive periodic processing and performs such processes as sending process-specific packets and gathering statistics. With **ppm** processes running distributed on both the Routing Engine and the Packet Forwarding Engine, you can run such processes as BFD on the Packet Forwarding Engine.

### Distributed ppm Required for ETH-DM

Ethernet frame delay measurement requires that **ppm** remains distributed to the Packet Forwarding Engine. If **ppm** is not distributed to the Packet Forwarding Engines of both routers, ETH-DM PDU frame timestamps and ETH-DM statistics are not valid.

Before you start ETH-DM, you must verify that the following configuration statement is *NOT* present:

```
[edit]
routing-options {
  ppm {
    no-delegate-processing;
  }
}
```

If distributed **ppm** processing is disabled (as shown in the stanza above) on either router, you must re-enable it in order to use the ETH-DM feature.

### Procedure to Ensure that Distributed ppm is Not Disabled

To ensure that distributed **ppm** is not disabled on a router:

1. Display the packet processing management (PPM) configuration to determine whether distributed **ppm** is disabled.

- In the following example, distributed **ppm** is enabled on the router. In this case, you do not need to modify the router configuration:

```
[edit]
user@host# show routing-options
ppm;
```

- In the following example, distributed **ppm** is disabled on the router. In this case, you must proceed to Step 2 to modify the router configuration:

```
[edit]
user@host show routing-options
ppm {
  no-delegate-processing;
}
```

2. Modify the router configuration to re-enable distributed **ppm** and restart the Ethernet OAM Connectivity Fault Management process *ONLY IF* distributed **ppm** is disabled (as determined in the previous step).

- a. Before continuing, make any necessary preparations for the possible loss of connectivity on the router.

Restarting the **ethernet-connectivity-fault-management** process has the following effect on your network:

- All connectivity fault management (CFM) sessions re-establish.
- All ETH-DM requests on the router terminate.
- All ETH-DM statistics and frame counts reset to 0.

- b. Modify the router configuration to re-enable distributed **ppm**. For example:

```
[edit]
user@host# delete routing-options ppm no-delegate-processing
```

- c. Commit the updated router configuration. For example:

```
[edit]
user@host# commit and-quit
commit complete
exiting configuration mode
```

- d. To restart the Ethernet OAM Connectivity-Fault-Management process, enter the **restart ethernet-connectivity-fault-management <gracefully | immediately | soft>** operational mode command. For example:

```
user@host> restart ethernet-connectivity-fault-management
Connectivity fault management process started, pid 9893
```

## Enabling the Hardware-Assisted Timestamping Option

By default, Ethernet frame delay measurement uses software for timestamping transmitted and received ETH-DM frames. For Ethernet interfaces on Enhanced Dense Port Concentrators (DPCs) and Enhanced Queuing DPCs only, you can optionally use hardware timing to assist in the timestamping of received ETH-DM frames to increase the accuracy of delay measurements.

Enabling hardware-assisted timestamping of received frames can increase the accuracy of ETH-DM calculations when the DPC is loaded with heavy traffic in the receive direction.

To enable Ethernet frame delay measurement hardware assistance on the reception path, include the **hardware-assisted-timestamping** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level:

```
[edit protocols]
oam {
  ethernet {
    connectivity-fault-management {
      performance-monitoring {
        hardware-assisted-timestamping;
```

```
    }  
  }  
}
```

## Configuring the Server-Side Processing Option

You can delegate the server-side processing (for both two-way delay measurement and loss measurement) to the Packet Forwarding Engine to prevent overloading on the Routing Engine. By default, the server-side processing is done by the Routing Engine.

To configure the server-side processing option:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit protocols oam ethernet connectivity-fault-management  
performance-monitoring
```

2. Configure the server-side processing option.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]  
user@host# set delegate-server-processing
```

3. Verify the configuration.

```
[edit protocols oam ethernet connectivity-fault-management]  
user@host# show  
performance-monitoring {  
  delegate-server-processing;  
}
```

---

## Starting an ETH-DM Session

- Using the monitor ethernet delay-measurement Command on page 226
- Starting a One-Way ETH-DM Session on page 227
- Starting a Two-Way ETH-DM Session on page 228

### Using the monitor ethernet delay-measurement Command

After you have configured two MX Series routers to support ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM), you can initiate a one-way or two-way Ethernet frame delay measurement session from the CFM maintenance association end point (MEP) on one of the routers to the peer MEP on the other router.

To start an ETH-DM session between the specified local MEP and the specified remote MEP, enter the **monitor ethernet delay-measurement** command at operational mode. The syntax of the command is as follows:

```
monitor ethernet delay-measurement  
(one-way | two-way)  
maintenance-domain md-name  
maintenance-association ma-name  
(remote-mac-address | mep remote-mep-id)  
<count frame-count>  
<wait interval-seconds>  
<priority 802.1p value>
```

```
<size>
<no-session-id-tlv>
<xml>
```

For a one-way frame delay measurement, the command displays a runtime display of the number of 1DM frames sent from the initiator MEP during that ETH-DM session. One-way frame delay and frame delay variation measurements from an ETH-DM session are collected in a CFM database at the router that contains the receiver MEP. You can retrieve ETH-DM statistics from a CFM database at a later time.

For a two-way frame delay measurement, the command displays two-way frame delay and frame delay variation values for each round-trip frame exchange during that ETH-DM session, as well as a runtime display of useful summary information about the session: average delay, average delay variation, best-case delay, and worst-case delay. Two-way frame delay and frame delay variation values measurements from an ETH-DM session are collected in a CFM database at the router that contains the initiator MEP. You can retrieve ETH-DM statistics from a CFM database at a later time.



**NOTE:** Although you can trigger frame delay collection for up to 65,535 ETH-DM requests at a time, a router stores only the last 100 frame delay statistics per CFM session (pair of peer MEPs).

For a complete description of the **monitor ethernet delay-measurement** operational command, see the [Junos OS System Basics and Services Command Reference](#).

## Starting a One-Way ETH-DM Session

To start a one-way Ethernet frame delay measurement session, enter the **monitor ethernet delay-measurement one-way** command from operational mode, and specify the peer MEP by its MAC address or by its MEP identifier.

For example:

```
user@host> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a
maintenance-domain md6 maintenance-association ma6 count 10
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```



**NOTE:** If you attempt to monitor delays to a nonexistent MAC address, you must type **Ctrl + C** to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

## Starting a Two-Way ETH-DM Session

To start a two-way Ethernet frame delay measurement session, enter the **monitor ethernet delay-measurement two-way** command from operational mode, and specify the peer MEP by its MAC address or by its MEP identifier.

For example:

```
user@host> monitor ethernet delay-measurement two-way 00:05:85:73:39:4a
maintenance-domain md6 maintenance-association ma6 count 10
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a Delay: 100 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 111 usec Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a Delay: 110 usec Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a Delay: 119 usec Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a Delay: 122 usec Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 108 usec Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```



**NOTE:** If you attempt to monitor delays to a nonexistent MAC address, you must type **Ctrl + C** to explicitly quit the **monitor ethernet delay-measurement** command and return to the CLI command prompt.

### Related Documentation

- Ethernet Frame Delay Measurements Overview on page 202
- Guidelines for Starting an ETH-DM Session on page 216
- **monitor ethernet delay-measurement** command
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts on page 218
- Managing ETH-DM Statistics and ETH-DM Frame Counts on page 228

---

## Managing ETH-DM Statistics and ETH-DM Frame Counts

- Displaying ETH-DM Statistics Only on page 228
- Displaying ETH-DM Statistics and Frame Counts on page 229
- Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity on page 229
- Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level on page 230
- Clearing ETH-DM Statistics and Frame Counts on page 231

## Displaying ETH-DM Statistics Only

**Purpose** Display ETH-DM statistics.



By default, the **show oam ethernet connectivity-fault-management delay-statistics** command displays ETH-DM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

- Action**
- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain ma1 maintenance-association ma1
```

- To display the ETH-DM statistics collected for ETH-DM sessions for the local MEP **201** belonging to MA **ma2** and within MD **md2**:

```
user@host> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md2 maintenance-association ma2 local-mep 201
```

- To display the ETH-DM statistics collected for ETH-DM sessions from local MEPs belonging to MA **ma3** and within MD **md3** to remote MEP **302**:

```
user@host> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md3 maintenance-association ma3 remote-mep 302
```

## Displaying ETH-DM Statistics and Frame Counts

**Purpose** Display ETH-DM statistics and ETH-DM frame counts.

By default, the **show oam ethernet connectivity-fault-management mep-statistics** command displays ETH-DM statistics and frame counts for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

- Action**
- To display the ETH-DM statistics and ETH-DM frame counts for MEPs in MA **ma1** and within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain md1 maintenance-association ma1
```

- To display the ETH-DM statistics and ETH-DM frame counts for the local MEP **201** in MA **ma2** and within MD **md2**:

```
user@host> show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain md2 maintenance-association ma2 local-mep 201
```

- To display the ETH-DM statistics and ETH-DM frame counts for the local MEP in MD **md3** and within MA **ma3** that participates in an ETH-DM session with the remote MEP **302**:

```
user@host> show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain ma3 maintenance-association ma3 remote-mep 302
```

## Displaying ETH-DM Frame Counts for MEPs by Enclosing CFM Entity

**Purpose** Display ETH-DM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management mep-database** command displays CFM database information for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).



**NOTE:** At the router attached to the initiator MEP for a one-way session, or at the router attached to the receiver MEP for a two-way session, you can only display ETH-DM frame counts.

- Action**
- To display CFM database information (including ETH-DM frame counts) for all MEPs in MA **ma1** within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain ma1 maintenance-association ma1
```

- To display CFM database information (including ETH-DM frame counts) only for local MEP **201** in MA **ma1** within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md2 maintenance-association ma2 local-mep 201
```

- To display CFM database information (including ETH-DM frame counts) only for remote MEP **302** in MD **md3** within MA **ma3**:

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain ma3 maintenance-association ma3 remote-mep 302
```

## Displaying ETH-DM Frame Counts for MEPs by Interface or Domain Level

- Purpose**
- Display ETH-DM frame counts for CFM maintenance association end points (MEPs).

By default, the **show oam ethernet connectivity-fault-management interfaces** command displays CFM database information for MEPs attached to CFM-enabled Ethernet interfaces on the router or at a maintenance domain level. For Ethernet interfaces that support ETH-DM, any frame counts are also displayed when you specify the **detail** or **extensive** command option.



**NOTE:** At the router attached to the initiator MEP for a one-way session, or at the router attached to the receiver MEP for a two-way session, you can only display ETH-DM frame counts.

- Action**
- To display CFM database information (including ETH-DM frame counts) for all MEPs attached to CFM-enabled Ethernet interfaces on the router:

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
```

- To display CFM database information (including ETH-DM frame counts) only for the MEPs attached to CFM-enabled router interface **ge-5/2/9.0**:

```
user@host> show oam ethernet connectivity-fault-management interfaces ge-5/2/9.0
detail
```

- To display CFM database information (including ETH-DM frame counts) only for MEPs enclosed within CFM maintenance domains (MDs) at level 6:

```
user@host> show oam ethernet connectivity-fault-management interfaces level 6
detail
```

## Clearing ETH-DM Statistics and Frame Counts

**Purpose** Clear the ETH-DM statistics and ETH-DM frame counts.

By default, statistics and frame counts are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

- Action**
- To clear the ETH-DM statistics and ETH-DM frame counts for all MEPs attached to CFM-enabled interfaces on the router:

```
user@host> clear oam ethernet connectivity-fault-management statistics
```

- To clear the ETH-DM statistics and ETH-DM frame counts only for MEPs attached to the logical interface **ge-0/5.9.0**:

```
user@host> clear oam ethernet connectivity-fault-management statistics ge-0/5/9.0
```

- Related Documentation**
- `clear oam ethernet connectivity-fault-management statistic` command
  - `show oam ethernet connectivity-fault-management delay-statistics` command
  - `show oam ethernet connectivity-fault-management interfaces (detail | extensive)` command
  - `show oam ethernet connectivity-fault-management mep-statistics` command
  - `show oam ethernet connectivity-fault-management mep-database` command

## Managing ETH-LM Statistics

- Displaying ETH-LM Statistics on page 231
- Clearing ETH-LM Statistics on page 232

### Displaying ETH-LM Statistics

**Purpose** Display the ETH-LM statistics.

By default, the `show oam ethernet connectivity-fault-management loss-statistics maintenance-domain md-name maintenance-association ma-name` command displays ETH-LM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

The following list consists of the CFM-related operational mode commands that have been enhanced to display ETH-LM statistics:

- The **show oam ethernet connectivity-fault-management interfaces detail** command is enhanced to display ETH-DM and ETH-LM statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).
- The **show oam ethernet connectivity-fault-management mep-statistics** command is enhanced to display ETH-DM and ETH-LM statistics and frame counts for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).
- The **show oam ethernet connectivity-fault-management mep-database** command is enhanced to display ETH-DM and ETH-LM frame counters for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

- Action**
- To display the ETH-LM statistics for all MEPs attached to CFM-enabled interfaces on the router:

```
user@host> show oam ethernet connectivity-fault-management loss-statistics
```

- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management delay-statistics  
maintenance-domain md1 maintenance-association ma1
```

- To display the ETH-DM statistics and ETH-DM frame counts for MEPs in MA **ma1** and within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management mep-statistics  
maintenance-domain md1 maintenance-association ma1
```

- To display CFM database information (including ETH-DM frame counts) for all MEPs in MA **ma1** within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management mep-database  
maintenance-domain md1 maintenance-association ma1
```

## Clearing ETH-LM Statistics

- Purpose**
- Clear the ETH-LM statistics.

By default, statistics are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

- Action**
- To clear the ETH-LM statistics for all MEPs attached to CFM-enabled interfaces on the router:

```
user@host> clear oam ethernet connectivity-fault-management loss-statistics
```

- Related Documentation**
- `clear oam ethernet connectivity-fault-management loss-statistics` command
  - `show oam ethernet connectivity-fault-management delay-statistics` command
  - `show oam ethernet connectivity-fault-management interfaces (detail | extensive)` command
  - `show oam ethernet connectivity-fault-management mep-statistics` command
  - `show oam ethernet connectivity-fault-management mep-database` command
  - `show oam ethernet connectivity-fault-management loss-statistics` command
  - Managing ETH-DM Statistics and ETH-DM Frame Counts on page 228

## Managing Iterator Statistics

- Displaying Iterator Statistics on page 233
- Clearing Iterator Statistics on page 237

### Displaying Iterator Statistics

**Purpose** Retrieve and display iterator statistics.

Multiple iterators can be associated with a remote MEP. However, by default, only one result pertaining to one iterator profile is displayed.

- Action**
- To display the iterator statistics for remote MEP 1 and iterator profile `il` with MEPs belonging to the maintenance association `ma1` and within the maintenance domain `default-1` (here, the iterator profile `il` is configured for two-way delay measurement):

```
user@host> show oam ethernet connectivity-fault-management sla-iterator-statistics
sla-iterator il maintenance-domain default-1 maintenance-association ma1 local-mep
1 remote-mep 1
```

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: il, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap
```

```
Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent : 23898520
DMM skipped for threshold hit : 11000
DMM skipped for threshold hit window : 0
DMR received : 23851165
DMR out of sequence : 1142
DMR received with invalid time stamps : 36540
Average two-way delay : 129 usec
Average two-way delay variation : 15 usec
Average one-way forward delay variation : 22 usec
Average one-way backward delay variation : 22 usec
Weighted average two-way delay : 134 usec
```

```

Weighted average two-way delay variation      : 8 usec
Weighted average one-way forward delay variation : 6 usec
Weighted average one-way backward delay variation : 2 usec

```

Output fields are listed in the approximate order in which they appear.

**Table 25: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields**

Output Field Name	Output Field Description
<b>Maintenance domain</b>	Maintenance domain name.
<b>Level</b>	Maintenance domain level configured.
<b>Maintenance association</b>	Maintenance association name.
<b>Local MEP id</b>	Numeric identifier of the local MEP.
<b>Remote MEP id</b>	Numeric identifier of the remote MEP.
<b>Remote MAC address</b>	Unicast MAC address of the remote MEP.
<b>Iterator name</b>	Name of iterator.
<b>Iterator Id</b>	Numeric identifier of the iterator.
<b>Iterator cycle time</b>	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
<b>Iteration period</b>	Maximum number of cycles per iteration
<b>Iterator status</b>	Current status of iterator whether running or stopped.
<b>Infinite iterations</b>	Status of iteration as infinite or finite.
<b>Counter reset time</b>	Date and time when the counter was reset.
<b>Reset reason</b>	Reason to reset counter.
<b>Delay weight</b>	Calculation weight of delay.
<b>Delay variation weight</b>	Calculation weight of delay variation.
<b>DMM sent</b>	Delay measurement message (DMM) PDU frames sent to the peer MEP in this session.
<b>DMM skipped for threshold hit</b>	Number of DMM frames sent to the peer MEP in this session skipped during threshold hit.
<b>DMM skipped for threshold hit window</b>	Number of DMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
<b>DMR received</b>	Number of delay measurement reply (DMR) frames received.

Table 25: Displaying Iterator Statistics for Ethernet Delay Measurement Output Fields (*continued*)

Output Field Name	Output Field Description
DMR out of sequence	Total number of DMR out of sequence packets received.
DMR received with invalid time stamps	Total number of DMR frames received with invalid timestamps.
Average two-way delay	Average two-way frame delay for the statistics displayed.
Average two-way delay variation	Average two-way "frame jitter" for the statistics displayed.
Average one-way forward delay variation	Average one-way forward delay variation for the statistics displayed in microseconds.
Average one-way backward delay variation	Average one-way backward delay variation for the statistics displayed in microseconds.
Weighted average two-way delay	Weighted average two-way delay for the statistics displayed in microseconds.
Weighted average two-way delay variation	Weighted average two-way delay variation for the statistics displayed in microseconds.
Weighted average one-way forward delay variation	Weighted average one-way forward delay variation for the statistics displayed in microseconds.
Weighted average one-way backward delay variation	Weighted average one-way backward delay variation for the statistics displayed in microseconds.

- To display the iterator statistics for remote MEP 1 and iterator profile i2 with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1** (here, the iterator profile **i1** is configured for loss measurement):

```
user@host> show oam ethernet connectivity-fault-management sla-iterator-statistics
sla-iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep
1 remote-mep 1
```

```
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i2, Iterator Id: 2
Iterator cycle time: 1000ms, Iteration period: 2000 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:25 ago)
Reset reason: Adjacency flap
```

```
Iterator loss measurement statistics:
LMM sent : 238970
LMM skipped for threshold hit : 60
LMM skipped for threshold hit window : 0
LMR received : 238766
LMR out of sequence : 43
```

```

Accumulated transmit statistics:
Near-end (CIR)                : 0
Far-end (CIR)                 : 0
Near-end (EIR)                : 0
Far-end (EIR)                 : 0

Accumulated loss statistics:
Near-end (CIR)                : 0 (0.00%)
Far-end (CIR)                 : 0 (0.00%)
Near-end (EIR)                : 0 (0.00%)
Far-end (EIR)                 : 0 (0.00%)

Last loss measurement statistics:
Near-end (CIR)                : 0
Far-end (CIR)                 : 0
Near-end (EIR)                : 0
Far-end (EIR)                 : 0

```

Output fields are listed in the approximate order in which they appear.

**Table 26: Displaying Iterator Statistics for Ethernet Loss Measurement Output Fields**

Output Field Name	Output Field Description
<b>Maintenance domain</b>	Maintenance domain name.
<b>Level</b>	Maintenance domain level configured.
<b>Maintenance association</b>	Maintenance association name.
<b>Local MEP id</b>	Numeric identifier of the local MEP.
<b>RemoteMEP identifier</b>	Numeric identifier of the remote MEP.
<b>Remote MAC address</b>	Unicast MAC address of the remote MEP.
<b>Iterator name</b>	Name of iterator.
<b>Iterator Id</b>	Numeric identifier of the iterator.
<b>Iterator cycle time</b>	Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection
<b>Iteration period</b>	Maximum number of cycles per iteration
<b>Iterator status</b>	Current status of iterator whether running or stopped.
<b>Infinite iterations</b>	Status of iteration as infinite or finite.
<b>Counter reset time</b>	Date and time when the counter was reset.
<b>Reset reason</b>	Reason to reset counter.
<b>LMM sent</b>	Number of loss measurement message (LMM) PDU frames sent to the peer MEP in this session.



Table 26: Displaying Iterator Statistics for Ethernet Loss Measurement Output Fields (*continued*)

Output Field Name	Output Field Description
LMM skipped for threshold hit	Number of LMM frames sent to the peer MEP in this session skipped during threshold hit.
LMM skipped for threshold hit window	Number of LMM frames sent to the peer MEP in this session skipped during the last threshold hit window.
LMR received	Number of LMRs frames received.
LMR out of sequence	Total number of LMR out of sequence packets received.
Near-end (CIR)	Frame loss associated with ingress data frames for the statistics displayed.
Far-end (CIR)	Frame loss associated with egress data frames for the statistics displayed.
Near-end (EIR)	Frame loss associated with ingress data frames for the statistics displayed.
Far-end (EIR)	Frame loss associated with egress data frames for the statistics displayed.

## Clearing Iterator Statistics

**Purpose** Clear iterator statistics.

Multiple iterators can be associated with remote MEP. However, by default, only one result pertaining to one iterator profile can be cleared.

- Action**
- To clear the iterator statistics for remote MEP 1 and iterator profile i1 with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1**:

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics
sla-iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep
1 remote-mep 1
```

- To clear the iterator statistics for remote MEP 1 and iterator profile i2 with MEPs belonging to the maintenance association **ma1** and within the maintenance domain **default-1**:

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics
sla-iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep
1 remote-mep 1
```

- Related Documentation**
- Configuring an Iterator Profile on page 211
  - Configuring a Remote MEP with an Iterator Profile on page 213
  - Example: Configuring an Iterator on page 246
  - Proactive Mode on page 210

## Managing Continuity Measurement Statistics

---

- Displaying Continuity Measurement Statistics on page 238
- Clearing Continuity Measurement Statistics on page 238

### Displaying Continuity Measurement Statistics

**Purpose** Display continuity measurement.

The **show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1** command is enhanced to display continuity measurement statistics for MEPs in the specified CFM maintenance association (MA) within the specified CFM maintenance domain (MD).

- Action**
- To display the ETH-DM statistics collected for MEPs belonging to MA **ma1** and within MD **md1**:

```
user@host> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md1 maintenance-association ma1
```

### Clearing Continuity Measurement Statistics

**Purpose** Clear the continuity measurement statistics

By default, statistics are deleted for all MEPs attached to CFM-enabled interfaces on the router. However, you can filter the scope of the command by specifying an interface name.

- Action**
- To clear the continuity measurement statistics for all MEPs attached to CFM-enabled interfaces on the router:

```
user@host> clear oam ethernet connectivity-fault-management continuity-measurement
maintenance-domain md-name maintenance-association ma-name local-mep
local-mep-id remote-mep remote-mep-id
```

## Example: One-Way Ethernet Frame Delay Measurement

---

- Description of the One-Way Frame Delay Measurement Example on page 238
- Steps for the One-Way Frame Delay Measurement Example on page 240

### Description of the One-Way Frame Delay Measurement Example

This example shows how you can configure two MX Series routers (**MX-PE1** and **MX-PE2**) to support an ETH-DM session between two peer MEPs (MEP **201** and MEP **101**), initiate a one-way ETH-DM session (from MEP **101** to MEP **201**), and then display the ETH-DM statistics and frame counts collected. To increase the accuracy of the ETH-DM statistics, enable optional hardware-assisted timestamping of received ETH-DM frames on the router that contains the receiver MEP.

### Routers Used in This Example

---

To support one-way ETH-DM with optional hardware timestamping of frames on the reception path, the routers used in this example are configured as follows:

- Routers **MX-PE1** and **MX-PE2** are MX Series routers.
- The system clocks of routers **MX-PE1** and **MX-PE2** are closely synchronized.
- On router **MX-PE1**, interface **ge-5/2/9** is an Ethernet port on an Enhanced or Enhanced Queuing Dense Port Concentrator (DPC). The traffic load received on this DPC is heavy.
- On router **MX-PE2**, interface **ge-0/2/5** is an Ethernet port on a DPC.

### ETH-DM Frame Counts for this Example

---

Both routers count the number of ETH-DM frames sent and received by the peer MEPs in the session and store the frame counts in the CFM databases as follows:

- At router **MX-PE2**, which contains the initiator MEP **101**, the CFM database stores the ETH-DM frame counts for a one-way ETH-DM initiator (the count of 1DM frames sent).
- At router **MX-PE1**, which contains the receiver MEP **201**, the CFM database stores the ETH-DM frame counts for a one-way ETH-DM receiver (the count of valid 1DM frames received and the count of invalid 1DM frames received).

### ETH-DM Statistics for this Example

---

For a one-way frame delay measurement, only the router that contains the receiver MEP measures and stores frame delay statistics. In this example, ETH-DM statistics collected for the session are available only at router **MX-PE1**.

## Steps for the One-Way Frame Delay Measurement Example

The following steps describe an example one-way Ethernet frame delay measurement:

1. At router **MX-PE1**, configure MEP **201** as a CFM maintenance association endpoint in CFM maintenance domain **md6** as follows:
  - a. Define the maintenance domain **md6** by associating it with maintenance domain level **6** and maintenance association identifier **ma6**.
  - b. Configure the maintenance association by specifying continuity protocol options and specifying MEP identifier **201**.
  - c. Configure MEP **201** by attaching it to logical interface **ge-5/2/9.0**, which is a single-tag interface on VLAN **512**.

The following configuration is only a partial example of a complete and functional router configuration:

```
[edit]
interfaces { # Configure a single-tag logical interface on VLAN 512
  ge-5/2/9 { # Interface must be on a DPC
    vlan-tagging;
    unit 0 {
      vlan-id 512;
    }
  }
}
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        traceoptions {
          file eoam_cfm.log size 1g files 2 world-readable;
          flag all;
        }
        maintenance-domain md6 { # Define MD 'md6' on router MX-PE1
          level 6;
          maintenance-association ma6 { # Configure MA 'ma6' on router MX-PE1
            continuity-check {
              interval 100ms;
              hold-interval 1;
            }
            mep 201 { # Configure MEP 201 on router MX-PE1
              interface ge-5/2/9.0; # Attach to logical interface on VLAN 512
              direction down;
              auto-discovery;
            }
          }
        }
      }
    }
  }
}
```

2. At router **MX-PE2**, configure MEP **101** as a CFM maintenance association endpoint in CFM maintenance domain **md6** as follows:
  - a. Define the maintenance domain **md6** by associating it with maintenance domain level **6** and maintenance association identifier **ma6**.
  - b. Configure the maintenance association by specifying continuity protocol options and specifying MEP identifier **101**.
  - c. Configure MEP **101** by attaching it to logical interface **ge-0/2/5.0**, which is a single-tag interface on VLAN **512**.

The following configuration is only a partial example of a complete and functional configuration for router **MX-PE2**:

```
[edit]
interfaces { # Configure a single-tag logical interface on VLAN 512
  ge-0/2/5 { # Interface must be on a DPC
    vlan-tagging;
    unit 0 {
      vlan-id 512;
    }
  }
}
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        traceoptions {
          file eoam_cfm.log size 1g files 2 world-readable;
          flag all;
        }
      }
      maintenance-domain md6 { # Define MD 'md6' on router MX-PE2
        level 6;
        maintenance-association ma6 { # Configure MA 'ma6' on router MX-PE2
          continuity-check {
            interval 100ms;
            hold-interval 1;
          }
        }
        mep 101 { # Configure MEP 101 on router MX-PE2
          interface ge-0/2/5.0; # Attach to logical interface on VLAN 512
          direction down;
          auto-discovery;
        }
      }
    }
  }
}
```

3. (Optional) To increase the accuracy of the ETH-DM statistics, modify the configuration of router **MX-PE1**, which contains the receiver MEP, by enabling hardware-assisted timestamping of **IDM** frames received on the router.

```
[edit protocols]
oam {
```

```

ethernet {
  connectivity-fault-management {
    performance-monitoring {
      hardware-assisted-timestamping;
    }
  }
}

```



**NOTE:** The hardware-assisted timestamping option for ETH-DM is available for Ethernet interfaces on Enhanced or Enhanced Queuing DPCs only.

4. At router **MX-PE2**, start a one-way frame delay measurement session from local MEP 101 to remote MEP 201 on router **MX-PE1**:

```

user@MX-PE2> monitor ethernet delay-measurement one-way mep 201
maintenance-domain md6 maintenance-association ma6 count 10

One-way ETH-DM request to 00:90:69:0a:43:94, Interface ge-0/2/5.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA

```

5. At router **MX-PE2**, which contains the initiator MEP, only the ETH-DM frame counts are available. Furthermore, the only frame count tallied for the initiator of a one-way frame delay measurement is the count of 1DM frames transmitted.

ETH-DM frame counts (the number of 1DM, DMM, and DMR frames exchanged during an ETH-DM session) are stored in the CFM database of both the initiator and receiver MEPs. When you display CFM database information, you can also display the ETH-DM frame counts. You can display CFM database information for all interfaces on the router, or you can limit the output to MEPs associated with certain CFM MDs and MAs.

- To display CFM database information for MEPs specified by enclosing CFM entities, use the **mep-database** form of the **show oam ethernet connectivity-fault-management** command. A CFM database also stores any ETH-DM frame counts.

In the example configuration for router **MX-PE2**, MEP 101 is the only MEP defined in MA **ma6** within MD **md6**. Therefore, the **show oam ethernet connectivity-fault-management mep-database** command output displays CFM database information for MEP 101 only, even though you do not filter the command output by including the **local-mep** or **remote-mep** command options.

```

user@MX-PE2> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md6 maintenance-association ma6

Maintenance domain name: md6, Format: string, Level: 6
Maintenance association name: ma6, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3
frames
MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
Auto-discovery: enabled, Priority: 0
Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up

```

```

Defects:
  Remote MEP not receiving CCM           : no
  Erroneous CCM received                 : no
  Cross-connect CCM received            : no
  RDI sent by some MEP                  : no
Statistics:
  CCMs sent                             : 1590
  CCMs received out of sequence         : 0
  LBMs sent                             : 0
  Valid in-order LBRs received          : 0
  Valid out-of-order LBRs received      : 0
  LBRs received with corrupted data     : 0
  LBRs sent                             : 0
  LTMs sent                             : 0
  LTMs received                         : 0
  LTRs sent                             : 0
  LTRs received                         : 0
  Sequence number of next LTM request   : 0
  1DMs sent                             : 10
  Valid 1DMs received                   : 0
  Invalid 1DMs received                 : 0
  DMMS sent                             : 0
  DMRs sent                             : 0
  Valid DMRs received                  : 0
  Invalid DMRs received                 : 0
Remote MEP count: 1
  Identifier  MAC address  State  Interface
    201      00:90:69:0a:43:94  ok    ge-0/2/5.0

```

- To display CFM database information for MEPs specified by interface name, use the **interfaces detail** form of the **show oam ethernet connectivity-fault-management** command. A CFM database also stores any ETH-DM frame counts.

In the example configuration for router **MX-PE2**, MEP 101 is the only MEP assigned to an interface on the router. Therefore, the **show oam ethernet connectivity-fault-management interfaces (detail | extensive)** command output displays CFM database information for MEP 101 only, even though you do not filter the command output by including the *ethernet-interface-name* or *level md-level* command options.

```

user@MX-PE2> show oam ethernet connectivity-fault-management interfaces detail

Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up
Maintenance domain name: md6, Format: string, Level: 6
Maintenance association name: ma6, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3
frames
MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
MEP status: running
Defects:
  Remote MEP not receiving CCM           : no
  Erroneous CCM received                 : no
  Cross-connect CCM received            : no
  RDI sent by some MEP                  : no
Statistics:
  CCMs sent                             : 1590
  CCMs received out of sequence         : 0
  LBMs sent                             : 0
  Valid in-order LBRs received          : 0
  Valid out-of-order LBRs received      : 0

```

```

LBRs received with corrupted data      : 0
LBRs sent                              : 0
LTMs sent                              : 0
LTMs received                          : 0
LTRs sent                              : 0
LTRs received                          : 0
Sequence number of next LTM request    : 0
1DMs sent                              : 10
Valid 1DMs received                    : 0
Invalid 1DMs received                  : 0
DMMs sent                              : 0
DMRs sent                              : 0
Valid DMRs received                   : 0
Invalid DMRs received                  : 0
Remote MEP count: 1
Identifier  MAC address      State   Interface
  201      00:90:69:0a:43:94   ok    ge-0/2/5.0

```



**NOTE:** You can use these same commands—`show oam ethernet connectivity-fault-management mep-database` and `show oam ethernet connectivity-fault-management interfaces (detail | extensive)`—at router **MX-PE1** to display the CFM database information (which includes any ETH-DM frame counts) for receiver MEP 201.

6. At router **MX-PE1**, which contains the receiver MEP, you can use two different **show oam ethernet connectivity-fault-management** commands to display ETH-DM statistics and ETH-DM frame counts.

- To display only the delay statistics, use the **delay-statistics** form of the **show oam ethernet connectivity-fault-management** command:

```
user@MX-PE1> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md6
```

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
```

```

Remote MAC address: 00:90:69:0a:48:57
Delay measurement statistics:
Index  One-way delay  Two-way delay
      (usec)         (usec)
  1      370
  2      357
  3      344
  4      332
  5      319
  6      306
  7      294
  8      281
  9      269
 10      255
Average one-way delay      : 312 usec
Average one-way delay variation: 11 usec
Best case one-way delay    : 255 usec
Worst case one-way delay   : 370 usec

```



- To display both the ETH-DM statistics and the CFM database information (which includes any ETH-DM frame counts), use the **mep-statistics** form of the **show oam ethernet connectivity-fault-management** command:

```
user@MX-PE1> show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain md6
```

```
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
  CCMs sent : 3240
  CCMs received out of sequence : 0
  LBMs sent : 0
  Valid in-order LBRs received : 0
  Valid out-of-order LBRs received : 0
  LBRs received with corrupted data : 0
  LBRs sent : 0
  LTMs sent : 0
  LTMs received : 0
  LTRs sent : 0
  LTRs received : 0
  Sequence number of next LTM request : 0
  1DMs sent : 0
  Valid 1DMs received : 10
  Invalid 1DMs received : 0
  DMMs sent : 0
  DMRs sent : 0
  Valid DMRs received : 0
  Invalid DMRs received : 0
```

```
Remote MEP identifier: 101
Remote MAC address: 00:90:69:0a:48:57
Delay measurement statistics:
  Index One-way delay Two-way delay
        (usec)         (usec)
    1      370
    2      357
    3      344
    4      332
    5      319
    6      306
    7      294
    8      281
    9      269
   10      255
Average one-way delay : 312 usec
Average one-way delay variation: 11 usec
Best case one-way delay : 255 usec
Worst case one-way delay : 370 usec
```

#### Related Documentation

- Guidelines for Configuring Routers to Support an ETH-DM Session on page 215
- Guidelines for Starting an ETH-DM Session on page 216
- Guidelines for Managing ETH-DM Statistics and ETH-DM Frame Counts on page 218
- On-Demand Mode on page 209

## Example: Configuring an Iterator

---

The following examples illustrate the configuration of an iterator for two-way delay measurement and loss measurement and the configuration of a remote MEP with an iterator profile. The examples also illustrate disabling an iterator profile with the **disable** statement and deactivating an iterator profile with the **deactivate** command.

- Example: Configuring an Iterator Profile for Two-way Delay Measurement on page 246
- Example: Configuring an Iterator Profile for Loss Measurement on page 246
- Example: Configuring a Remote MEP with an Iterator Profile on page 246
- Example: Disabling an Iterator Profile with the **disable** Statement on page 247
- Example: Disabling an Iterator Profile by Deactivating the Profile on page 247

### Example: Configuring an Iterator Profile for Two-way Delay Measurement

Configuring an iterator profile **i1** for two-way delay measurement, where the cycle time value is **1000 ms**, iteration period is **2000** cycles per second, delay value is **1**, and delay variation value is **1**:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles]
i1 {
  cycle-time 1000;
  iteration-period 2000;
  measurement-type two-way-delay;
  calculation-weight {
    delay 1;
    delay-variation 1;
  }
}
```

### Example: Configuring an Iterator Profile for Loss Measurement

Configuring an iterator profile **i2** for loss measurement, where the cycle time value is **1000 ms** and iteration period is **2000** cycles per second:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
sla-iterator-profiles]
i2 {
  cycle-time 1000;
  iteration-period 2000;
  measurement-type loss;
}
```

### Example: Configuring a Remote MEP with an Iterator Profile

Configuring a remote MEP with an iterator profile **i3** for two-way delay measurement, where the data TLV size is **1**, iteration count is **1**, and the priority value is **1** for the remote MEP whose value is **1**:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
default-1 maintenance association ma1 mep 1 remote-mep 1]
user@host# show
```

```
sla-iterator-profile i3 {
  data-tlv-size 1;
  iteration-count 1;
  priority 1;
}
```

### Example: Disabling an Iterator Profile with the `disable` Statement

Disabling an iterator profile `i1` for two-way delay measurement with the **`disable`** statement, where the cycle time value is **1000 ms**, iteration period is **2000** cycles per second, delay value is 1, delay variation value is 1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
 sla-iterator-profiles i1]
disable;
cycle-time 1000;
iteration-period 2000;
measurement-type two-way-delay;
calculation-weight {
  delay 1;
  delay-variation 1;
}
```

### Example: Disabling an Iterator Profile by Deactivating the Profile

Disabling an iterator profile `i2` with the **`deactivate`** command for a remote MEP whose value is 1:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
 default-1 maintenance association ma1 mep 1]
remote-mep 1 {
  deactivate sla-iterator-profile i2;
}
```

#### Related Documentation

- Proactive Mode on page 210
- Clearing Iterator Statistics on page 237
- Configuring an Iterator Profile on page 211
- Configuring a Remote MEP with an Iterator Profile on page 213
- Displaying Iterator Statistics on page 233
- Managing Iterator Statistics on page 233



# Configuring IEEE 802.1x Port-Based Network Access Control

- IEEE 802.1x Port-Based Network Access Control Overview on page 249
- Understanding the Administrative State of the Authenticator Port on page 250
- Understanding the Administrative Mode of the Authenticator Port on page 250
- Configuring the Authenticator on page 250
- Viewing the dot1x Configuration on page 251

## IEEE 802.1x Port-Based Network Access Control Overview

---

MX Series routers support the IEEE 802.1x Port-Based Network Access Control (dot1x) protocol on Ethernet interfaces for validation of client and user credentials to prevent unauthorized access to a specified router port. Before authentication is complete, only 802.1x control packets are allowed and forwarded to the router control plane for processing. All other packets are dropped.

Authentication methods used must be 802.1x compliant. Authentication using RADIUS and Microsoft Active Directory servers is supported. The following user/client authentication methods are allowed:

- EAP-MD5 (RFC 3748)
- EAP-TTLS requires a server certificate (RFC 2716)
- EAP-TLS requires a client and server certificate
- PEAP requires only a server certificate

You can use both client and server certificates in all types of authentication except EAP-MD5.



**NOTE:** On the MX Series router, 802.1x can be enabled on bridged ports only and not on routed ports.

Dynamic changes to a user session are supported to allow the router administrator to terminate an already authenticated session by using the “RADIUS disconnect” message defined in RFC 3576.

## Understanding the Administrative State of the Authenticator Port

---

The administrative state of an authenticator port can take any of the following three states:

- Force authorized—Allows network access to all users of the port without requiring them to be authenticated. This is equivalent to not having any authentication enabled on the port.
- Force unauthorized—Denies network access to all users of the port. This is equivalent to disabling the port.
- Automatic—This is the default mode where the authentication server response determines if the port is opened for traffic or not. Only the successfully authenticated clients are allowed access, all others are denied.

In Junos OS, the default mode is “automatic.” The “force authorized” and “force unauthorized” admin modes are not supported. You can achieve the functionality of “force authorized” mode by disabling **dot1x** on the required port. You can achieve the functionality of “force unauthorized” mode by disabling the port itself.

## Understanding the Administrative Mode of the Authenticator Port

---

Junos OS supports the supplicant mode “single” and not the “single secure” nor “multiple” modes. The “Single” mode option authenticates only the first client that connects to a port. All other clients that connect later (802.1x compliant or noncompliant) are allowed free access on that port without any further authentication. If the first authenticated client logs out, all other users are locked out until a client authenticates again.

## Configuring the Authenticator

---

To configure the IEEE 802.1x Port-Based Network Access Control protocol on Ethernet interfaces you must configure the **authenticator** statement at the **[edit protocols dot1x]** hierarchy level. Use the **authentication-profile-name access-profile-name** statement to specify the authenticating RADIUS server, and use the **interface** statement to specify and configure the Gigabit Ethernet or Fast Ethernet interface on the router specifically for IEEE 802.1x protocol use; both at the **[edit protocols dot1x authenticator]** hierarchy level.

```
[edit protocols dot1x]
authenticator {
  authentication-profile-name access-profile-name;
  interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) {
    maximum-requests seconds;
    quiet-period seconds;
    reauthentication (disable | interval seconds);
    retries integer;
    server-timeout seconds;
```

```
    supplicant (single);  
    supplicant-timeout seconds;  
    transmit-period seconds;  
  }  
}
```

---

## Viewing the dot1x Configuration

**Purpose** To review and verify the dot1x configuration.

**Action** To view all **dot1x** configurations, use the **show dot1x interface** operational mode command. To view a **dot1x** configuration for a specific interface, use the **show dot1x interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) detail** operational mode command. See the *Network Interfaces Command Reference* for more information about this command.





# Configuring IEEE 802.3ah OAM Link-Fault Management

- IEEE 802.3ah OAM Link-Fault Management Overview on page 253
- Configuring IEEE 802.3ah OAM Link-Fault Management on page 254
- Enabling IEEE 802.3ah OAM Support on page 254
- Configuring Link Discovery on page 255
- Configuring the OAM PDU Interval on page 255
- Configuring the OAM PDU Threshold on page 255
- Configuring Threshold Values for Local Fault Events on an Interface on page 255
- Disabling the Sending of Link Event TLVs on page 256
- Detecting Remote Faults on page 256
- Configuring an OAM Action Profile on page 256
- Specifying the Actions to Be Taken for Link-Fault Management Events on page 257
- Monitoring the Loss of Link Adjacency on page 258
- Monitoring Protocol Status on page 258
- Configuring Threshold Values for Fault Events in an Action Profile on page 258
- Applying an Action Profile on page 259
- Setting a Remote Interface into Loopback Mode on page 259
- Enabling Remote Loopback Support on the Local Interface on page 259
- Example: Configuring IEEE 802.3ah OAM Support on an Interface on page 260

## IEEE 802.3ah OAM Link-Fault Management Overview

---

Ethernet interfaces capable of running at 100 Mbps or faster on MX Series, M Series (except M5 and M10 routers), and T Series routers support the IEEE 802.3ah standard for Operation, Administration, and Management (OAM). You can configure IEEE 802.3ah OAM on Ethernet point-to-point direct links or links across Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities as Ethernet moves from being solely an enterprise technology to being a WAN and access technology, as well as being backward-compatible with existing Ethernet technology. Junos OS supports IEEE 802.3ah link-fault management.

The features of link-fault management are:

- Discovery
- Link monitoring
- Remote fault detection
- Remote loopback



**NOTE:** Ethernet running on top of a Layer 2 protocol, such as Ethernet over ATM, is not supported in OAM configurations.

---

## Configuring IEEE 802.3ah OAM Link-Fault Management

---

You can configure threshold values for fault events that trigger the sending of link event TLVs when the values exceed the threshold. To set threshold values for fault events on an interface, include the **event-thresholds** statement at the **[edit protocols oam ethernet link-fault-management interface]** hierarchy level.

You can also configure OAM threshold values within an action profile and apply the action profile to multiple interfaces. To create an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level.

You can configure Ethernet OAM either on an aggregate interface or on each of its member links. However, we recommend that you configure Ethernet OAM on the aggregate interface, and this will internally enable Ethernet OAM on the member links.

To view OAM statistics, use the **show oam ethernet link-fault-management** operational mode command. To clear OAM statistics, use the **clear oam ethernet link-fault-management statistics** operational mode command. To clear link-fault management state information and restart the link discovery process on Ethernet interfaces, use the **clear oam ethernet link-fault-management state** operational mode command. For more information about these commands, see the *Junos OS Interfaces Command Reference*.

## Enabling IEEE 802.3ah OAM Support

---

To enable IEEE 802.3ah OAM support, include the **interface** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level:

**[edit protocols oam ethernet link-fault-management interface *interface-name*]**

When you enable IEEE 802.3ah OAM on a physical interface, the discovery process is automatically triggered.

## Configuring Link Discovery

---

When the IEEE 802.3ah OAM protocol is enabled on a physical interface, the discovery process is automatically triggered. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard.

You can specify the discovery mode used for IEEE 802.3ah OAM support. The discovery process is triggered automatically when OAM IEEE 802.3ah functionality is enabled on a port. Link monitoring is done when the interface sends periodic OAM PDUs.

To configure the discovery mode, include the **link-discovery** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
link-discovery (active | passive);
```

In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. In passive mode, the peer initiates the discovery process. After the discovery process has been initiated, both sides participate in discovery.

## Configuring the OAM PDU Interval

---

Periodic OAM PDUs are sent to perform link monitoring.

You can specify the periodic OAM PDU sending interval for fault detection.

To configure the sending interval, include the **pdu-interval** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
pdu-interval interval;
```

The periodic OAM PDU interval range is from 100 through 1000 milliseconds. The default sending interval is 1000 milliseconds.

## Configuring the OAM PDU Threshold

---

You can specify the number of OAM PDUs that an interface can miss before the link between peers is considered down.

To configure the number of PDUs that can be missed from the peer, include the **pdu-threshold** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
pdu-threshold threshold-value;
```

The threshold value range is from 3 through 10. The default is three PDUs.

## Configuring Threshold Values for Local Fault Events on an Interface

---

You can configure threshold values on an interface for the local errors that trigger the sending of link event TLVs.

To set the error threshold values for sending event TLVs, include the **frame-error**, **frame-period**, **frame-period-summary**, and **symbol-period** statements at the **[edit protocols oam ethernet link-fault-management interface *interface-name* event-thresholds]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
event-thresholds {  
    frame-error count;  
    frame-period count;  
    frame-period-summary count;  
    symbol-period count;  
}
```

---

## Disabling the Sending of Link Event TLVs

You can disable the sending of link event TLVs.

To disable the monitoring and sending of PDUs containing link event TLVs in periodic PDUs, include the **no-allow-link-events** statement at the **[edit protocols oam ethernet link-fault-management interface *interface-name* negotiation-options]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name  
negotiation-options]  
no-allow-link-events;
```

---

## Detecting Remote Faults

Fault detection is either based on flags or fault event type, length, and values (TLVs) received in OAM protocol data units (PDUs). Flags that trigger a link fault are:

- Critical Event
- Dying Gasp
- Link Fault

The link event TLVs are sent by the remote DTE by means of event notification PDUs. Link event TLVs are:

- Errored Symbol Period Event
- Errored Frame Event
- Errored Frame Period Event
- Errored Frame Seconds Summary Event

---

## Configuring an OAM Action Profile

You can create an action profile to define event fault flags and thresholds and the action to be taken. You can then apply the action profile to one or more interfaces.

To configure an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level:

```

action-profile profile-name {
  action {
    syslog;
    link-down;
    send-critical-event;
  }
  event {
    link-adjacency-loss;
    link-event-rate {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    protocol-down;
  }
}

```

## Specifying the Actions to Be Taken for Link-Fault Management Events

You can specify the action to be taken by the system when the configured link-fault event occurs. Multiple action profiles can be applied to a single interface. For each action-profile, at least one event and one action must be specified. The actions are taken only when all of the events in the action profile are true. If more than one action is specified, all the actions are executed.

You might want to set a lower threshold for a specific action such as logging the error and set a higher threshold for another action such as sending a critical event TLV.

To specify the action, include the **action** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name*]** hierarchy level:

```

[edit protocol oam ethernet link-fault-management action-profile profile-name]
event {
  link-adjacency-loss;
  protocol-down;
}
action {
  syslog;
  link-down;
  send-critical-event;
}

```

To create a system log entry when the link-fault event occurs, include the **syslog** statement.

To administratively disable the link when the link-fault event occurs, include the **link-down** statement.

To send IEEE 802.3ah link event TLVs in the OAM PDU when a link-fault event occurs, include the **send-critical-event** statement.



**NOTE:** If multiple actions are specified in the action profile, all of the actions are executed in no particular order.

---

## Monitoring the Loss of Link Adjacency

You can specify actions be taken when link adjacency is lost. When link adjacency is lost, the system takes the action defined in the **action** statement of the action profile.

To configure the system to take action when link adjacency is lost, include the **link-adjacency-loss** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]  
link-adjacency-loss;
```

---

## Monitoring Protocol Status

The CCC-DOWN flag is associated with a circuit cross-connect (CCC) connection, Layer 2 circuit, and Layer 2 VPN, which send the CCC-DOWN status to the kernel. The CCC-DOWN flag indicates that the CCC is down. The CCC-DOWN status is sent to the kernel when the CCC connection, Layer 2 circuit, or Layer 2 VPN is down. This in turn, brings down the CE-facing PE router interface associated with the CCC connection, Layer 2 circuit, or Layer 2 VPN.

When the CCC-DOWN flag is signaled to the IEEE 802.3ah protocol, the system takes the action defined in the **action** statement of the action profile. For additional information about Layer 2 circuits, see the Junos OS Layer 2 Circuits Feature Guide, Junos OS VPNs Configuration Guide.

To monitor the IEEE 802.3ah protocol, on the CE-facing PE router, include the **protocol-down** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]  
protocol-down;
```



**NOTE:** If multiple events are specified in the action profile, all the events must occur before the specified action is taken.

---

## Configuring Threshold Values for Fault Events in an Action Profile

You can configure link event thresholds for received error events that trigger the action specified in the **action** statement. You can then apply the action profile to one or more interfaces.

To configure link event thresholds, include the **link-event-rate** statement at the **[edit protocols oam ethernet link-fault-management action-profile *profile-name* event]** hierarchy level:

```
link-event-rate {  
  frame-error count;  
  frame-period count;  
  frame-period-summary count;  
  symbol-period count;  
}
```

---

## Applying an Action Profile

You can apply an action profile to one or more interfaces.

To apply an action profile to an interface, include the **apply-action-profile** statement at the **[edit protocols oam ethernet link-fault-management action-profile interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
  apply-action-profile profile-name;
```

---

## Setting a Remote Interface into Loopback Mode

You can configure the software to set the remote DTE into loopback mode on the following interfaces:

- IQ2 and IQ2-E Gigabit Ethernet interfaces
- Ethernet interfaces on the MX Series routers

Junos OS can place a remote DTE into loopback mode (if remote-loopback mode is supported by the remote DTE). When you place a remote DTE into loopback mode, the interface receives the remote-loopback request and puts the interface into remote-loopback mode. When the interface is in remote-loopback mode, all frames except OAM PDUs are looped back without any changes made to the frames. OAM PDUs continue to be sent to the management plane and processed.

To configure remote loopback, include the **remote-loopback** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name*]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name]  
  remote-loopback;
```

To take the remote DTE out of loopback mode, remove the **remote-loopback** statement from the configuration.

---

## Enabling Remote Loopback Support on the Local Interface

You can allow a remote DTE to set a local interface into remote loopback mode on IQ2 and IQ2-E Gigabit Ethernet interfaces and all Ethernet interfaces on the MX Series routers. When a remote-loopback request is sent by a remote DTE, the Junos OS places the local interface into loopback mode. When an interface is in loopback mode, all frames except

OAM PDUs are looped back without any changes to the frames. OAM PDUs continue to be sent to the management plane and processed. By default, the remote loopback feature is not enabled.

To enable remote loopback, include the **allow-remote-loopback** statement at the **[edit protocol oam ethernet link-fault-management interface *interface-name* negotiation-options]** hierarchy level:

```
[edit protocol oam ethernet link-fault-management interface interface-name
 negotiation-options]
allow-remote-loopback;
```



**NOTE:** Activation of OAM remote loopback may result in data frame loss.

---

## Example: Configuring IEEE 802.3ah OAM Support on an Interface

---

Configure 802.3ah OAM support on an MX Series 10-Gigabit Ethernet interface:

```
[edit]
protocols {
  oam {
    ethernet {
      link-fault-management {
        interface xe-0/0/0 {
          link-discovery active;
          pdu-interval 800;
          pdu-threshold 4;
          remote-loopback;
          negotiation-options {
            allow-remote-loopback;
          }
          event-thresholds {
            frame-error 30;
            frame-period 50;
            frame-period summary 40;
            symbol-period 20;
          }
        }
      }
    }
  }
}
```



# Configuring VRRP and VRRP for IPv6

- VRRP and VRRP for IPv6 Overview on page 261
- Configuring VRRP and VRRP for IPv6 on page 261

## VRRP and VRRP for IPv6 Overview

---

You can configure the Virtual Router Redundancy Protocol (VRRP) and VRRP for IPv6 for the following interfaces:

- Ethernet
- Fast Ethernet
- Tri-Rate Ethernet copper
- Gigabit Ethernet
- 10-Gigabit Ethernet LAN/WAN PIC
- Ethernet logical interfaces

VRRP and VRRP for IPv6 allow hosts on a LAN to make use of redundant routers on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routers share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routers is the master (active) and the others are backups. If the master fails, one of the backup routers becomes the new master router, thus always providing a virtual default router and allowing traffic on the LAN to be routed without relying on a single router.

VRRP is defined in RFC 3768, *Virtual Router Redundancy Protocol*.

For VRRP and VRRP for IPv6 overview information, configuration guidelines, and statement summaries, see the *Junos OS High Availability Configuration Guide*.

## Configuring VRRP and VRRP for IPv6

---

To configure VRRP or VRRP for IPv6, include the **vrrp-group** or **vrrp-inet6-group** statement, respectively. These statements are available at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*]**

- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address*]

The VRRP and VRRP IPv6 configuration statements are as follows:

```
(vrrp-group | vrrp-inet-group) group-number {  
  (accept-data | no-accept-data);  
  advertise-interval seconds;  
  authentication-key key;  
  authentication-type authentication;  
  fast-interval milliseconds;  
  (preempt | no-preempt) {  
    hold-time seconds;  
  }  
  priority-number number;  
  track {  
    priority-hold-time;  
    interface interface-name {  
      priority-cost priority;  
      bandwidth-threshold bits-per-second {  
        priority-cost;  
      }  
    }  
  }  
  virtual-address [ addresses ];  
}
```

To trace VRRP and VRRP for IPv6 operations, include the **traceoptions** statement at the [edit protocols vrrp] hierarchy level:

```
[edit protocols vrrp]  
traceoptions {  
  file <filename> <files number <match regular-expression <microsecond-stamp>  
    <size size> <world-readable | no-world-readable>;  
  flag flag;  
  no-remote-trace;  
}
```

When there are multiple VRRP groups, there is a few seconds delay between the time the first gratuitous ARP is sent out and the rest of the gratuitous ARP are sent. Configuring failover-delay compensates for this delay. To configure the failover delay from 500 to 2000 milliseconds for VRRP and VRRP for IPv6 operations, include the **failover-delay** *milliseconds* statement at the [edit protocols vrrp] hierarchy level:

```
[edit protocols vrrp]  
failover-delay milliseconds;
```

To configure the startup period for VRRP and VRRP for IPv6 operations, include the **startup-silent-period** statement at the [edit protocols vrrp] hierarchy level:

```
[edit protocols vrrp]  
startup-silent-period seconds;
```

# Configuring Gigabit Ethernet Accounting and Policing

- Gigabit Ethernet Accounting and Policing Overview on page 263
- Configuring Gigabit Ethernet Policers on page 265
- Configuring Gigabit Ethernet Two-Color and Tricolor Policers on page 271
- Configuring MAC Address Accounting on page 274

## Gigabit Ethernet Accounting and Policing Overview

---

For Gigabit Ethernet IQ PICs and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can configure granular per-VLAN class-of-service (CoS) capabilities and extensive instrumentation and diagnostics on a per-VLAN and per-MAC address basis.

VLAN rewrite, tagging, and deleting enables you to use VLAN address space to support more customers and services.

VPLS allows you to provide a point-to-multipoint LAN between a set of sites in a VPN. Ethernet IQ PICs and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router) are combined with VPLS to deliver metro Ethernet service.

For Gigabit Ethernet IQ2 and IQ2-E and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, you can apply Layer 2 policing to logical interfaces in the egress or ingress direction. Layer 2 policers are configured at the **[edit firewall]** hierarchy level. You can also control the rate of traffic sent or received on an interface by configuring a policer overhead at the **[edit chassis fpc slot-number pic slot-number]** hierarchy level.

Table 27 on page 264 lists the capabilities of Gigabit Ethernet IQ PICs and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router).

**Table 27: Capabilities of Gigabit Ethernet IQ and Gigabit Ethernet with SFPs**

Capability	Gigabit Ethernet IQ (SFP)	Gigabit Ethernet (SFP)
<b>Layer 2</b>		
802.3ad link aggregation	Yes	Yes
Maximum VLANs per port	384	1023
Maximum transmission unit (MTU) size	9192	9192
MAC learning	Yes	Yes
MAC accounting	Yes	Yes
MAC filtering	Yes	Yes
Destinations per port	960	960
Sources per port	64	64
Hierarchical MAC policers	Yes, premium and aggregate	No, aggregate only
Multiple TPID support and IP service for nonstandard TPIDs	Yes	Yes
Multiple Ethernet encapsulations	Yes	Yes
Dual VLAN tags	Yes	No
VLAN rewrite	Yes	No
<b>Layer 2 VPNs</b>		
VLAN CCC	Yes	Yes
Port-based CCC	Yes	Yes
Extended VLAN CCC Virtual Metropolitan Area Network (VMAN) Tag Protocol	Yes	Yes
<b>CoS</b>		
PIC-based egress queues	Yes	Yes
Queued VLANs	Yes	No
VPLS	Yes	Yes

For more information about configuring VPLS, see the [Junos OS VPNs Configuration Guide](#) and the [Junos OS Feature Guides](#).

You can also configure CoS on logical IQ interfaces. For more information, see the [Junos OS Class of Service Configuration Guide](#).

**Related  
Documentation**

- [Configuring a Policer Overhead](#)

## Configuring Gigabit Ethernet Policers

On Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can define rate limits for premium and aggregate traffic received on the interface. These policers allow you to perform simple traffic policing without configuring a firewall filter. First you configure the Ethernet policer profile, next you classify ingress and egress traffic, then you can apply the policer to a logical interface.

For Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), the policer rates you configure can be different than the rates on the Packet Forward Engine. The difference results from Layer 2 overhead. The PIC accounts for this difference.



**NOTE:**

On MX Series routers with Gigabit Ethernet or Fast Ethernet PICs, the following considerations apply:

- Interface counters do not count the 7-byte preamble and 1-byte frame delimiter in Ethernet frames.
- In MAC statistics, the frame size includes MAC header and CRC before any VLAN rewrite/imposition rules are applied.
- In traffic statistics, the frame size encompasses the L2 header without CRC after any VLAN rewrite/imposition rule.

For information on understanding Ethernet frame statistics, see the [MX Series Layer 2 Configuration Guide](#).

This section contains the following topics:

- [Configuring a Policer on page 266](#)
- [Specifying an Input Priority Map on page 266](#)
- [Specifying an Output Priority Map on page 267](#)
- [Applying a Policer on page 268](#)
- [Configuring MAC Address Filtering on page 269](#)
- [Example: Configuring Gigabit Ethernet Policers on page 270](#)

## Configuring a Policer

To configure an Ethernet policer profile, include the **ethernet-policer-profile** statement at the **[edit interfaces *interface-name* gigether-options ethernet-switch-profile]** hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
ethernet-policer-profile {
  policer cos-policer-name {
    aggregate {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    premium {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
  }
}
```

In the Ethernet policer profile, the aggregate-priority policer is mandatory; the premium-priority policer is optional.

For aggregate and premium policers, you specify the bandwidth limit in bits per second. You can specify the value as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000). There is no absolute minimum value for bandwidth limit, but any value below 61,040 bps will result in an effective rate of 30,520 bps. The maximum bandwidth limit is 4.29 Gbps.

The maximum burst size controls the amount of traffic bursting allowed. To determine the burst-size limit, you can multiply the bandwidth of the interface on which you are applying the filter by the amount of time you allow a burst of traffic at that bandwidth to occur:

$$\text{burst size} = \text{bandwidth} \times \text{allowable time for burst traffic}$$

If you do not know the interface bandwidth, you can multiply the maximum MTU of the traffic on the interface by 10 to obtain a value. For example, the burst size for an MTU of 4700 would be 47,000 bytes. The burst size should be at least 10 interface MTUs. The maximum value for the burst-size limit is 100 MB.

## Specifying an Input Priority Map

An input priority map identifies ingress traffic with specified IEEE 802.1p priority values, and classifies that traffic as premium.

If you include a premium-priority policer, you can specify an input priority map by including the **ieee802.1p premium** statement at the **[edit interfaces *interface-name* gigether-options ethernet-policer-profile input-priority-map]** hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-policer-profile input-priority-map]
ieee802.1p premium [ values ];
```

The priority values can be from 0 through 7. The remaining traffic is classified as nonpremium (or aggregate). For a configuration example, see “Example: Configuring Gigabit Ethernet Policers” on page 270.



**NOTE:** On IQ2 and IQ2-E interfaces and MX Series interfaces, when a VLAN tag is pushed, the inner VLAN IEEE 802.1p bits are copied to the IEEE bits of the VLAN or VLANs being pushed. If the original packet is untagged, the IEEE bits of the VLAN or VLANs being pushed are set to 0.

## Specifying an Output Priority Map

An output priority map identifies egress traffic with specified queue classification and packet loss priority (PLP), and classifies that traffic as premium.

If you include a premium-priority policer, you can specify an output priority map by including the **classifier** statement at the **[edit interfaces *interface-name* gigether-options ethernet-policer-profile output-priority-map]** hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-policer-profile
 output-priority-map]
classifier {
  premium {
    forwarding-class class-name {
      loss-priority (high | low);
    }
  }
}
```

You can define a forwarding class, or you can use a predefined forwarding class. Table 28 on page 267 shows the predefined forwarding classes and their associated queue assignments.

**Table 28: Default Forwarding Classes**

Forwarding Class Name	Queue
best-effort	Queue 0
expedited-forwarding	Queue 1
assured-forwarding	Queue 2
network-control	Queue 3

For more information about CoS forwarding classes, see the [Junos OS Class of Service Configuration Guide](#). For a configuration example, see “Example: Configuring Gigabit Ethernet Policers” on page 270.

## Applying a Policer

On all MX Series Router interfaces, Gigabit Ethernet IQ, IQ2, and IQ2-E PICs, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can apply input and output policers that define rate limits for premium and aggregate traffic received on the logical interface. Aggregate policers are supported on Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router).

These policers allow you to perform simple traffic policing without configuring a firewall filter. For information about defining these policers, see “Configuring Gigabit Ethernet Policers” on page 265.

To apply policers to specific source MAC addresses, include the **accept-source-mac** statement:

```
accept-source-mac {  
  mac-address mac-address {  
    policer {  
      input cos-policer-name;  
      output cos-policer-name;  
    }  
  }  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* ]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* ]

You can specify the MAC address as *nn:nn:nn:nn:nn:nn* or *nnnn.nnnn.nnnn*, where *n* is a hexadecimal number. You can configure up to 64 source addresses. To specify more than one address, include multiple **mac-address** statements in the logical interface configuration.



**NOTE:** On untagged Gigabit Ethernet interfaces you should not configure the **source-address-filter** statement at the [edit interfaces *ge-fpc/pic/port* *gigether-options*] hierarchy level and the **accept-source-mac** statement at the [edit interfaces *ge-fpc/pic/port* *gigether-options* unit *logical-unit-number*] hierarchy level simultaneously. If these statements are configured for the same interfaces at the same time, an error message is displayed.

On tagged Gigabit Ethernet interfaces you should not configure the **source-address-filter** statement at the [edit interfaces *ge-fpc/pic/port* *gigether-options*] hierarchy level and the **accept-source-mac** statement at the [edit interfaces *ge-fpc/pic/port* *gigether-options* unit *logical-unit-number*] hierarchy level with an identical MAC address specified in both filters. If these statements are configured for the same interfaces with an identical MAC address specified, an error message is displayed.





**NOTE:** If the remote Ethernet card is changed, the interface does not accept traffic from the new card because the new card has a different MAC address.

The MAC addresses you include in the configuration are entered into the router's MAC database. To view the router's MAC database, enter the **show interfaces mac-database interface-name** command:

```
user@host> show interfaces mac-database interface-name
```

In the **input** statement, list the name of one policer template to be evaluated when packets are received on the interface.

In the **output** statement, list the name of one policer template to be evaluated when packets are transmitted on the interface.



**NOTE:** On IQ2 and IQ2-E PIC interfaces, the default value for maximum retention of entries in the MAC address table has changed, for cases in which the table is not full. The new holding time is 12 hours. The previous retention time of 3 minutes is still in effect when the table is full.

You can use the same policer one or more times.

If you apply both policers and firewall filters to an interface, input policers are evaluated before input firewall filters, and output policers are evaluated after output firewall filters.

## Configuring MAC Address Filtering

You cannot explicitly define traffic with specific source MAC addresses to be rejected; however, for Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and for Gigabit Ethernet DPCs on MX Series routers, you can block all incoming packets that do not have a source address specified in the **accept-source-mac** statement. For more information about the **accept-source-mac** statement, see “Applying a Policar” on page 268.

To enable this blocking, include the **source-filtering** statement at the **[edit interfaces interface-name gigeother-options]** hierarchy level:

```
[edit interfaces interface-name gigeother-options]
source-filtering;
```

For more information about the **source-filtering** statement, see “Enabling Ethernet MAC Address Filtering” on page 38.

To accept traffic even though it does not have a source address specified in the **accept-source-mac** statement, include the **no-source-filtering** statement at the **[edit interfaces interface-name gigeother-options]** hierarchy level:

```
[edit interfaces interface-name gigeother-options]
no-source-filtering;
```

For more information about the **accept-source-mac** statement, see “Applying a Policer” on page 268.

### Example: Configuring Gigabit Ethernet Policers

Configure interface **ge-6/0/0** to treat priority values 2 and 3 as premium. On ingress, this means that IEEE 802.1p priority values **2** and **3** are treated as premium. On egress, it means traffic that is classified into queue 0 or 1 with PLP of low and queue 2 or 3 with PLP of high, is treated as premium.

Define a policer that limits the premium bandwidth to 100 Mbps and burst size to 3 k, and the aggregate bandwidth to 200 Mbps and burst size to 3 k.

Specify that frames received from the MAC address **00:01:02:03:04:05** and the VLAN ID **600** are subject to the policer on input and output. On input, this means frames received with the source MAC address **00:01:02:03:04:05** and the VLAN ID 600 are subject to the policer. On output, this means frames transmitted from the router with the destination MAC address **00:01:02:03:04:05** and the VLAN ID **600** are subject to the policer.

```
[edit interfaces]
ge-6/0/0 {
  gigether-options {
    ether-switch-profile {
      ether-policer-profile {
        input-priority-map {
          ieee-802.1p {
            premium [ 2 3 ];
          }
        }
        output-priority-map {
          classifier {
            premium {
              forwarding-class best-effort {
                loss-priority low;
              }
              forwarding-class expedited-forwarding {
                loss-priority low;
              }
              forwarding-class assured-forwarding {
                loss-priority high;
              }
              forwarding-class network-control {
                loss-priority high;
              }
            }
          }
        }
      }
    }
    policer policer-1 {
      premium {
        bandwidth-limit 100m;
        burst-size-limit 3k;
      }
      aggregate {
        bandwidth-limit 200m;
      }
    }
  }
}
```

```

        burst-size-limit 3k;
    }
}
}
}
unit 0 {
    accept-source-mac {
        mac-address 00:01:02:03:04:05 {
            policer {
                input policer-1;
                output policer-1;
            }
        }
    }
}
}

```

**Related Documentation**

- [Configuring a Policer Overhead](#)

## Configuring Gigabit Ethernet Two-Color and Tricolor Policers

For Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series and T Series routers, you can configure two-color and tricolor marking policers and apply them to logical interfaces to prevent traffic on the interface from consuming bandwidth inappropriately.

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or classes of service.

Policers require you to apply a burst size and bandwidth limit to the traffic flow, and set a consequence for packets that exceed these limits—usually a higher loss priority, so that packets exceeding the policer limits are discarded first.

Juniper Networks router architectures support three types of policer:

- **Two-color policer**—A two-color policer (or “policer” when used without qualification) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit in some way, or simply discard them. A policer is most useful for metering traffic at the port (physical interface) level.
- **Single-rate tricolor marking (srTCM)**—A single-rate tricolor marking policer is defined in RFC 2697, *A Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets arriving are below the CBS (green), exceed the CBS (yellow) but

not the EBS, or exceed the EBS (red). Single-rate TCM is most useful when a service is structured according to packet length and not peak arrival rate.

- Two-rate Tricolor Marking (trTCM)—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and peak information rate (PIR), along with their associated burst sizes, the CBS and EBS. Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets arriving are below the CIR (green), exceed the CIR (yellow) but not the PIR, or exceed the PIR (red). Two-rate TCM is most useful when a service is structured according to arrival rates and not necessarily packet length.

Unlike policing (described in “Configuring Gigabit Ethernet Policers” on page 265), configuring two-color policers and tricolor marking policers requires that you configure a firewall filter.

This section contains the following topics:

- Configuring a Policer on page 272
- Applying a Policer on page 273
- Example: Configuring and Applying a Policer on page 273

## Configuring a Policer

Two-color and tricolor marking policers are configured at the **[edit firewall]** hierarchy level.

A tricolor marking policer polices traffic on the basis of metering rates, including the CIR, the PIR, their associated burst sizes, and any policing actions configured for the traffic.

To configure tricolor policer marking, include the **three-color-policer** statement with options at the **[edit firewall]** hierarchy level:

```
[edit firewall]
three-color-policer name {
  action {
    loss-priority high {
      then discard;
    }
  }
  single-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-information-rate bps;
    committed-burst-size bytes;
    peak-information-rate bps;
    peak-burst-size bytes;
```

```

    }
}

```

For more information about configuring tricolor policer markings, see the *Junos OS Routing Policy Configuration Guide* and the *Junos OS Class of Service Configuration Guide*.

## Applying a Policer

Apply a two-color policer or tricolor policer to a logical interface to prevent traffic on the interface from consuming bandwidth inappropriately. To apply two-color or tricolor policers, include the **layer2-policer** statement:

```

layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    policer-name;
}

```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Use the **input-policer** statement to apply a two-color policer to received packets on a logical interface and the **input-three-color** statement to apply a tricolor policer. Use the **output-policer** statement to apply a two-color policer to transmitted packets on a logical interface and the **output-three-color** statement to apply a tricolor policer. The specified policers must be configured at the [edit firewall] hierarchy level. For each interface, you can configure a three-color policer or two-color input policer or output policers—you cannot configure both a three-color policer and a two-color policer.

## Example: Configuring and Applying a Policer

Configure tricolor policers and apply them to an interface:

```

[edit firewall]
three-color-policer three-color-policer-color-blind {
    logical-interface-policer;
    two-rate {
        color-blind;
        committed-information-rate 1500000;
        committed-burst-size 150;
        peak-information-rate 3;
        peak-burst-size 300;
    }
}
three-color-policer three-color-policer-color-aware {
    logical-interface-policer;
    two-rate {
        color-aware;
        committed-information-rate 1500000;
        committed-burst-size 150;
        peak-information-rate 3;
    }
}

```

```
        peak-burst-size 300;
    }
}
[edit interfaces ge-1/1/0]
unit 1 {
    layer2-policer {
        input-three-color three-color-policer-color-blind;
        output-three-color three-color-policer-color-aware;
    }
}
```

Configure a two-color policer and apply it to an interface:

```
[edit firewall]
policer two-color-policer {
    logical-interface-policer;
    if-exceeding {
        bandwidth-percent 90;
        burst-size-limit 300;
    }
    then loss-priority-high;
}
[edit interfaces ge-1/1/0]
unit 2 {
    layer2-policer {
        input-policer two-color-policer;
        output-policer two-color-policer;
    }
}
```

**Related Documentation**

- [Configuring a Policer Overhead](#)

---

## Configuring MAC Address Accounting

For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and for Gigabit Ethernet DPCs on MX Series routers, you can configure whether source and destination MAC addresses are dynamically learned. To configure MAC address accounting, include the **mac-learn-enable** statement at the **[edit interfaces *interface-name* gether-options ethernet-switch-profile]** hierarchy level:

```
[edit interfaces interface-name gether-options ethernet-switch-profile]
mac-learn-enable;
```

To prohibit the interface from dynamically learning source and destination MAC addresses, include the **no-mac-learn-enable** statement at the **[edit interfaces *interface-name* gether-options ethernet-switch-profile]** hierarchy level:

```
[edit interfaces interface-name gether-options ethernet-switch-profile]
no-mac-learn-enable;
```

MAC address learning is based on source addresses. You can start accounting for traffic after it has been sent from the MAC address. Once the MAC address is learned, the frames and bytes transmitted to or received from the MAC address can be tracked.



NOTE: DPCs based on I-chips and Trio-based MPCs support MAC address accounting. DPCs based on I-chips support both source and destination MAC address accounting. Trio-based MPCs support only source MAC address accounting.





# Configuring Gigabit Ethernet Autonegotiation

- Gigabit Ethernet Autonegotiation Overview on page 277
- Configuring Gigabit Ethernet Autonegotiation on page 277

## Gigabit Ethernet Autonegotiation Overview

---

Autonegotiation is enabled by default on all Gigabit Ethernet and Tri-Rate Ethernet copper interfaces. However, you can explicitly enable autonegotiation to configure remote fault options manually.



**NOTE:** For Gigabit Ethernet interfaces installed in J4350 and J6350 Services Routers, when you manually configure either the link mode or speed settings, the system ignores the configuration and generates a system log message. When autonegotiation is enabled and you specify the link mode and speed, the link autonegotiates with the manually configured settings. When autonegotiation is disabled and you configure both the link mode and speed, the link operates with the manually configured settings. If you disable autonegotiation and do not manually configure the link mode and speed, the link operates at 1000 Mbps full duplex.



**NOTE:** When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled.

## Configuring Gigabit Ethernet Autonegotiation

---

- Configuring Gigabit Ethernet Autonegotiation with Remote Fault on page 278
- Configuring Flow Control on page 278
- Configuring Autonegotiation Speed on MX Series Routers on page 278
- Displaying Autonegotiation Status on page 278

## Configuring Gigabit Ethernet Autonegotiation with Remote Fault

To configure explicit autonegotiation and remote fault, include the **auto-negotiation** statement and the **remote-fault** option at the **[edit interfaces ge-fpc/pic/port gigerther-options]** hierarchy level.

```
[edit interfaces ge-fpc/pic/port gigerther-options]
(auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
local-interface-offline>
```

## Configuring Flow Control

To enable flow control, include the **flow-control** statement at the **[edit interfaces ge-fpc/pic>/port gigerther-options]** hierarchy level. For more information, see “Configuring Flow Control” on page 41.

## Configuring Autonegotiation Speed on MX Series Routers

MX Series routers with Combo Line Rate DPCs and Tri-Rate Copper SFPs support autonegotiation of speed. The autonegotiation specified interface speed is propagated to CoS, routing protocols, and other system components. Half-duplex mode is not supported.

MX Series routers with IQ2 PICs connected to other devices require matching auto-negotiation configurations for both the PIC and for the device in order to achieve link up.

To specify the autonegotiation speed, use the **speed (auto | 1Gbps | 100Mbps | 10Mbps)** statement at the **[edit interfaces ge-fpc/pic/port]** hierarchy level.

To set port speed negotiation to a specific rate, set the port speed to **1Gbps**, **100Mbps**, or **10Mbps**. If the negotiated speed and the interface speed do not match, the link will not be brought up.

If you set the autonegotiation speed **auto** option, then the port speed is negotiated.

You can disable auto MDI/MDIX using the **no-auto-mdix** statement at the **[edit interfaces ge-fpc/pic/port gigerther-options]** hierarchy level.

Use the **show interfaces ge-fpc/pic/port brief** command to display the auto negotiation of speed and auto MDI/MDIX states.

## Displaying Autonegotiation Status

To display Gigabit Ethernet interface details, including the autonegotiation status, use the operational mode command **show interfaces ge- fpc/pic/port extensive**.

Table 29 on page 279 and Table 30 on page 281 provide information about the autonegotiation status on local and remote routers with fiber interfaces. The status of the link and LED can vary depending on the level of autonegotiation set and the transmit and receive fiber status.

Table 29: Mode and Autonegotiation Status (Local)

Transmit	Receive	Mode	LED	Link	Autonegotiation Status
ON	ON	Default	Green	UP	Complete
ON	OFF	Default	Red	DOWN	
OFF	ON	Default	Red	DOWN	
OFF	OFF	Default	Red	DOWN	
ON	ON	Default	Red	DOWN	
ON	ON	Default	Green	UP	No-autonegotiation
ON	OFF	Default	Red	DOWN	
OFF	OFF	Default	Red	DOWN	
ON	ON	Default	Green	UP	
ON	ON	Default	Red	DOWN	
ON	ON	No-autonegotiation	Green	UP	Incomplete
ON	OFF	No-autonegotiation	Red	DOWN	
OFF	ON	No-autonegotiation	Green	UP	
OFF	OFF	No-autonegotiation	Red	DOWN	
ON	ON	No-autonegotiation	Red	DOWN	
ON	ON	Explicit	Green	UP	Complete
ON	OFF	Explicit	Red	DOWN	
OFF	ON	Explicit	Red	DOWN	
OFF	OFF	Explicit	Red	DOWN	
ON	ON	Explicit	Red	DOWN	
ON	ON	Explicit	Green	UP	No-autonegotiation
ON	OFF	Explicit	Red	DOWN	
OFF	ON	Explicit	Green	UP	
OFF	OFF	Explicit	Red	DOWN	

Table 29: Mode and Autonegotiation Status (Local) (*continued*)

Transmit	Receive	Mode	LED	Link	Autonegotiation Status
ON	ON	Explicit	Red	DOWN	
ON	ON	Explicit+RFI-Offline	Green	UP	Complete
OFF	ON	Explicit+RFI-Offline	Red	DOWN	
OFF	OFF	Explicit+RFI-Offline	Red	DOWN	
ON	ON	Explicit+RFI-Offline	Red	DOWN	
ON	ON	Explicit+RFI-Offline	Green	UP	No-autonegotiation
ON	OFF	Explicit+RFI-Offline	Red	DOWN	
OFF	ON	Explicit+RFI-Offline	Green	UP	
OFF	OFF	Explicit+RFI-Offline	Red	DOWN	
ON	ON	Explicit+RFI-Offline	Red	DOWN	
ON	ON	Explicit+RFI-Offline	Red	DOWN	Complete
ON	OFF	Explicit+RFI-Offline	Red	DOWN	
OFF	ON	Explicit+RFI-Online	Red	DOWN	
OFF	OFF	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Green	UP	No-autonegotiation*
ON	OFF	Explicit+RFI-Online	Red	DOWN	
OFF	ON	Explicit+RFI-Online	Green	UP	
OFF	OFF	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Green	UP	
ON	ON	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Red	DOWN	Complete
ON	OFF	Explicit+RFI-Online	Red	DOWN	
OFF	ON	Explicit+RFI-Online	Red	DOWN	

Table 29: Mode and Autonegotiation Status (Local) (*continued*)

Transmit	Receive	Mode	LED	Link	Autonegotiation Status
OFF	OFF	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Red	DOWN	
ON	ON	Explicit+RFI-Online	Green	UP	Complete

Table 30: Mode and Autonegotiation Status (Remote)

Transmit	Receive	Mode	LED	Link	Autonegotiation Status
ON	ON	Default	Green	UP	Complete
ON	ON	Default	Red	DOWN	
ON	OFF	Default	Red	DOWN	
OFF	ON	Default	Red	DOWN	
OFF	OFF	Default	Red	DOWN	
ON	ON	No-autonegotiation	Green	UP	Incomplete
ON	ON	No-autonegotiation	Red	DOWN	
ON	OFF	No-autonegotiation	Red	DOWN	
OFF	ON	No-autonegotiation	Green	UP	
OFF	OFF	No-autonegotiation	Red	DOWN	
ON	ON	Explicit	Green	UP	Complete
ON	ON	Explicit	Red	DOWN	
ON	OFF	Explicit	Red	DOWN	
OFF	ON	Explicit	Red	DOWN	
OFF	OFF	Explicit	Red	DOWN	
ON	ON	Explicit	Red	DOWN	Complete
ON	OFF	Explicit	Red	DOWN	
OFF	ON	Explicit	Red	DOWN	
OFF	OFF	Explicit	Red	DOWN	

Table 30: Mode and Autonegotiation Status (Remote) (*continued*)

Transmit	Receive	Mode	LED	Link	Autonegotiation Status
ON	ON	Explicit+RFI-Offline	Red	DOWN	Complete
ON	OFF	Explicit+RFI-Offline	Red	DOWN	
OFF	ON	Explicit+RFI-Offline	Red	DOWN	
OFF	OFF	Explicit+RFI-Offline	Red	DOWN	
ON	ON	Explicit+RFI-Online	Green	UP	Complete
ON	ON	Explicit+RFI-Online	Red	DOWN	
ON	OFF	Explicit+RFI-Online	Red	DOWN	
OFF	ON	Explicit+RFI-Online	Red	DOWN	
OFF	OFF	Explicit+RFI-Online	Red	DOWN	

# Configuring Gigabit Ethernet OTN Options

- Gigabit Ethernet OTN Options Configuration Overview on page 283
- Gigabit Ethernet OTN Options on page 283

## Gigabit Ethernet OTN Options Configuration Overview

M120, T320, T640, and T1600 routers support Optical Transport Network (OTN) interfaces, including the 10-Gigabit Ethernet DWDM OTN PIC, and provide ITU-G.709 support. Use the **set otn-options** statement at the **[edit interfaces if-*fpc/pic/port*]** hierarchy level to configure the OTN options.

## Gigabit Ethernet OTN Options

The following example shows the configuration settings for Gigabit Ethernet OTN options:

```
[edit interfaces ge-fpc/pic/port]
otn-options {
  fec (efec | gfec | none);
  (laser-enable | no-laser-enable);
  (line-loopback | no-line-loopback);
  pass-thru;
  rate (fixed-stuff-bytes | no-fixed-stuff-bytes | pass-thru);
  transmit-payload-type number;
  trigger (oc-lof | oc-lom | oc-los | oc-wavelength-lock | odu-ais | odu-bbe-th | odu-bdi |
    odu-es-th | odu-lck | odu-oci | odu-sd | odu-ses-th | odu-ttim | odu-uas-th | opu-ptm |
    otu-ais | otu-bbe-th | otu-bdi | otu-es-th | otu-fec-deg | otu-fec-exe | otu-iae | otu-sd |
    otu-ses-th | otu-ttim | otu-uas-th);
  tti;
}
```



**NOTE:** The Gigabit Ethernet interface and the XENPAK interface support the read/write overhead bytes only for the APS/PPC (bytes 0 through 3).

You can use the following show commands to view the OTN configuration:

- **show interfaces extensive**—See the *Junos OS Interfaces Command Reference* for command details.

- **show chassis hardware**—See the *Junos OS System Basics and Services Command Reference* for command details.
- **show chassis pic**—See the *Junos OS System Basics and Services Command Reference* for command details.



## CHAPTER 20

# Configuring the Management Ethernet Interface

- Management Ethernet Interface Overview on page 285
- Configuring a Consistent Management IP Address on page 285
- Configuring the MAC Address on the Management Ethernet Interface on page 286

### Management Ethernet Interface Overview

---

The router's management Ethernet interface, **fxp0** or **em0**, is an out-of-band management interface that needs to be configured only if you want to connect to the router through the management port on the front of the router. You can configure an IP address and prefix length for this interface, which you commonly do when you first install the Junos OS:

```
[edit]
user@host# set interfaces (fxp0 | em0) unit 0 family inet address/prefix-length
[edit]
user@host# show
interfaces {
  (fxp0 | em0) {
    unit 0 {
      family inet {
        address/prefix-length;
      }
    }
  }
}
```

### Configuring a Consistent Management IP Address

---

On routers with multiple Routing Engines, each Routing Engine is configured with a separate IP address for the management Ethernet interface. To access the master Routing Engine, you must know which Routing Engine is active and use the appropriate IP address.

Optionally, for consistent access to the master Routing Engine, you can configure an additional IP address and use this address for the management interface regardless of which Routing Engine is active. This additional IP address is active only on the

management Ethernet interface for the master Routing Engine. During switchover, the address moves to the new master Routing Engine.



**NOTE:** For M Series, MX Series, and most T Series routers, the management Ethernet interface is `fxp0`. For TX Matrix Plus routers and T1600 routers configured in a routing matrix, the management Ethernet interface is `em0`.



**NOTE:** Automated scripts that you have developed for standalone T1600 routers (T1600 routers that are not in a routing matrix) might contain references to the `fxp0` management Ethernet interface. Before reusing the scripts on T1600 routers in a routing matrix, edit the command lines that reference the `fxp0` management Ethernet interface so that the commands reference the `em0` management Ethernet interface instead.

To configure an additional IP address for the management Ethernet interface, include the **master-only** statement at the **[edit groups]** hierarchy level.

In the following example, IP address **10.17.40.131** is configured for both Routing Engines and includes a **master-only** statement. With this configuration, the **10.17.40.131** address is active only on the master Routing Engine. The address remains consistent regardless of which Routing Engine is active. IP address **10.17.40.132** is assigned to **fxp0** on **re0**, and address **10.17.40.133** is assigned to **fxp0** on **re1**.

```
[edit groups re0 interfaces fxp0]
unit 0 {
  family inet {
    address 10.17.40.131/25 {
      master-only;
    }
    address 10.17.40.132/25;
  }
}
[edit groups re1 interfaces fxp0]
unit 0 {
  family inet {
    address 10.17.40.131/25 {
      master-only;
    }
    address 10.17.40.133/25;
  }
}
```

This feature is available on all routers that include dual Routing Engines. On the TX Matrix router, this feature is applicable to the switch-card chassis (SCC) only.

---

## Configuring the MAC Address on the Management Ethernet Interface

---

By default, the router's management Ethernet interface uses as its MAC address the MAC address that is burned into the Ethernet card.



**NOTE:** For M Series, MX Series, and most T Series routers, the management Ethernet interface is `fxp0`. For TX Matrix Plus routers and T1600 routers configured in a routing matrix, the management Ethernet interface is `em0`.



**NOTE:** Automated scripts that you have developed for standalone T1600 routers (T1600 routers that are not in a routing matrix) might contain references to the `fxp0` management Ethernet interface. Before reusing the scripts on T1600 routers in a routing matrix, edit the command lines that reference the `fxp0` management Ethernet interface so that the commands reference the `em0` management Ethernet interface instead.

To display the MAC address used by the router's management Ethernet interface, enter the `show interface fxp0` or `show interface em0` operational mode command.

To change the management Ethernet interface's MAC address, include the `mac` statement at the `[edit interfaces fxp0]` or `[edit interfaces em0]` hierarchy level:

```
[edit interfaces (fxp0 | em0)]
mac mac-address;
```

Specify the MAC address as six hexadecimal bytes in one of the following formats:  
`nnnn.nnnn.nnnn` (for example, `0011.2233.4455`) or `nn:nn:nn:nn:nn:nn` (for example, `00:11:22:33:44:55`).



**NOTE:** If you integrate a standalone T640 router into a routing matrix, the PIC MAC addresses for the integrated T640 router are derived from a pool of MAC addresses maintained by the TX Matrix router. For each MAC address you specify in the configuration of a formerly standalone T640 router, you must specify the same MAC address in the configuration of the TX Matrix router.

Similarly, if you integrate a standalone T1600 router into a routing matrix, the PIC MAC addresses for the integrated T1600 router are derived from a pool of MAC addresses maintained by the TX Matrix Plus router. For each MAC address you specify in the configuration of a formerly standalone T1600 router, you must specify the same MAC address in the configuration of the TX Matrix Plus router.



# Configuring 10-Gigabit Ethernet LAN/WAN PICs

This section contains the following topics:

- 10-Gigabit Ethernet LAN/WAN PIC Overview on page 289
- Configuring Line-Rate Mode on 10-Gigabit Ethernet LAN/WAN PIC on page 292
- Configuring Control Queue Disable on a 10-Gigabit Ethernet LAN/WAN PIC on page 292
- Example: Handling Oversubscription on a 10-Gigabit Ethernet LAN/WAN PIC on page 295

## 10-Gigabit Ethernet LAN/WAN PIC Overview

---

This section describes the main features and caveats of the 10-Gigabit Ethernet LAN/WAN PIC with SFP+ and specifies which routers support this PIC. This PIC has a front panel label with the designation “ETHERNET 10GBASE-SFP+ LAN-WAN” and can also be identified by its model number, PD-5-10XGE-SFPP. It is referred to hereafter as the 10-Gigabit Ethernet LAN/WAN PIC.

The 10-Gigabit Ethernet LAN/WAN PIC is supported by TX Matrix, TX Matrix Plus and Juniper Networks T640 and T1600 Core Routers. It has the following features:

- Intelligent handling of oversubscribed traffic in applications such as data centers and dense-core uplinks
- Line-rate operation for five 10-Gigabit Ethernet ports from each port group, or a total WAN bandwidth of 100 Gbps with Packet Forwarding Engine bandwidth of 50 Gbps
- Flexible encapsulation, source address and destination address media access control (MAC) filtering, source address MAC learning, MAC accounting, and MAC policing
- Interface encapsulations, such as the following:
  - **ethernet-ccc**—Ethernet cross-connect
  - **vlan-ccc**—802.1Q tagging for a cross-connect
  - **ethernet-tcc**—Ethernet translational cross-connect
  - **vlan-tcc**—Virtual LAN (VLAN) translational cross-connect

- **extended-vlan-ccc**—Standard Tag Protocol Identifier (TPID) tagging for a cross-connect
- **ethernet-vpls**—Ethernet virtual private LAN service
- **vlan-vpls**—VLAN virtual private LAN service
- **flexible-ethernet-services**—Allows per-unit Ethernet encapsulation configuration
- Single, stacked, and flexible VLAN tagging modes
- Native VLAN configuration to allow untagged frames to be received on the tagged interfaces
- Maximum transmission unit (MTU) size of up to 9192 bytes for Ethernet frames
- Link aggregation group (LAG) on single chassis
- Interoperability with other 10-Gigabit Ethernet PICs in M Series and T Series routers in the LAN PHY and WAN PHY modes
- Interrupt-driven link-down detection mechanism
- Two-to-one oversubscription of traffic across a port group

Traffic from 10 ingress ports to the Packet Forwarding Engine traffic is statically mapped to one of the 5 egress ports. 10 Gbps of bandwidth toward the Packet Forwarding Engine is shared by two ingress ports (called a *port group*), thereby achieving two-to-one oversubscription. This scheme provides two-to-one oversubscription across a port group and not across the entire PIC.

- Four queues per physical interface on ingress and eight queues per physical interface on egress
- A separate control queue per physical interface to ensure that the control packets are not dropped during oversubscribed traffic. The control queue can be disabled in the CLI.
- SFP+ optical diagnostics

SFP+ is a next-generation transceiver module form factor specified by the ANSI T11 Group for 8.5-Gbps and 10-Gbps fiber channel and Ethernet applications. The SFP+ form factor is 30 percent smaller than the XFP form factor. The benefits include higher port density, lower power modules, and lower system costs. The 10-Gigabit Ethernet LAN/WAN PIC supports 10GBASE-SR and 10GBASE-LR SFP+ optics.
- Behavior aggregate (BA) classification (IPv4 DSCP, IPv6 DSCP, Inet precedence, IEEE 802.1P, IEEE 802.1AD, MPLS EXP) and fixed classification
- Weighted round-robin scheduling with two queue priorities (low and strict-high)
- Committed information rate and peak information rate shaping on a per-queue basis
- Excess information rate configuration for allocation of excess bandwidth

The 10-Gigabit Ethernet LAN/WAN PIC has the following caveats:

- Source address and destination address MAC filtering takes place after oversubscription is handled.
- Oversubscription on the PIC operates across a port group of two ports and not at the PIC level.
- Queuing is not supported at the logical interface level.
- Committed information rate and peak information rate configurations are not supported at the physical interface level.
- There is limited packet buffering of 2 MB.
- Delay-bandwidth buffering configuration is not supported.
- Multifield classifiers are not supported at the PIC level.

The multifield classification can be done at the Packet Forwarding Engine using the firewall filters, which overrides the classification done at the PIC level. The multifield classification at the Packet Forwarding Engine occurs after the PIC handles the oversubscribed traffic.

- Egress MAC policer statistics not supported.
- Byte counters are not supported at the queue level.
- Only TPID (0x8100) is supported.
- Line-timing mode is not supported.
- MAC-level Rx VLAN tagged frames counter is not supported.

Table 31 on page 291 lists the capabilities of 10-Gigabit Ethernet LAN/WAN PICs.

**Table 31: Capabilities of 10-Gigabit Ethernet LAN/WAN PICs**

Capability	Support
Maximum VLANs per PIC	4065
Maximum VLANs per port	1022
MAC learning per port	960
MAC accounting per port	960
MAC filtering per port	960 (64 filters per physical or logical interface) 960 filters across multiple logical interfaces
MAC policers	128 ingress Mac policers 128 egress Mac policers
Classifiers	Eight classifiers per PIC for each BA classifier type

## Configuring Line-Rate Mode on 10-Gigabit Ethernet LAN/WAN PIC

---

The 10-Gigabit Ethernet LAN/WAN PIC can be configured in the command-line interface (CLI) to operate in the following two modes:

- Oversubscribed Ethernet mode (default)—In this mode, all ports are enabled on the PIC with two-to-one oversubscription.
- Line-rate mode—In this mode, only five alternate ports (ports 0, 2, 4, 6, and 8) are enabled. The PIC operates in line-rate mode at 50 Gbps.

To configure the PIC in line-rate mode, include the **linerate-mode** statement at the **[edit chassis set fpc fpc-number pic pic-number]** hierarchy level:

```
[edit chassis]
set fpc fpc-number pic pic-number linerate-mode;
```

To return to the default oversubscribed Ethernet mode, delete the **linerate-mode** statement at the **[edit chassis fpc fpc-number pic pic-number]** hierarchy level.



**NOTE:** When the mode of operation of a PIC is changed, the PIC is taken offline and then brought back online immediately.

### Related Documentation

- Example: Handling Oversubscription on a 10-Gigabit Ethernet LAN/WAN PIC on page 295
- 10-Gigabit Ethernet LAN/WAN PIC Overview on page 289

## Configuring Control Queue Disable on a 10-Gigabit Ethernet LAN/WAN PIC

---

On a 10-port 10-Gigabit Ethernet LAN/WAN PIC, a control queue is used to queue all control packets received on an ingress port. This ensures that control protocol packets do not get dropped randomly when there is congestion due to oversubscription. The following list of control protocols are supported:

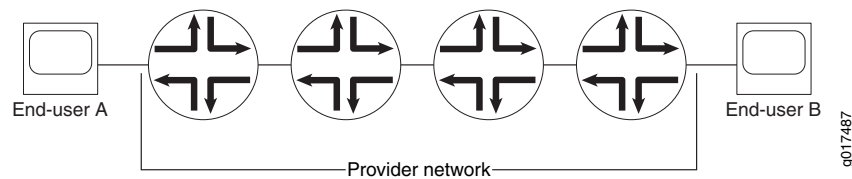
- OSPF
- OSPF3
- VRRP
- IGMP
- RSVP
- PIM
- BGP
- BFD
- LDP
- IS-IS



- RIP
- RIPV6
- LACP
- ARP
- IPv6 NDP

These control packets can either terminate locally or transit through the router. The control queue has a rate limiter to limit the control traffic to 2 Mbps (fixed, not user-configurable) per port. Hence, if transit control traffic is taking too much bandwidth, then it can cause drops on locally terminating control traffic, as shown in Figure 26 on page 293.

**Figure 26: Control Queue Rate Limiter Scenario**



If the end users generate a mass of malicious traffic for which the port number is 179 (BGP), the router dispatches that traffic to the ingress control queue. Further, if congestion occurs in this ingress control queue due to this malicious traffic, the provider's network control packets may be affected.

In some applications, this can be perceived as a new vulnerability. To address this concern, you can disable the control queue feature. With the control queue feature disabled, you must take precautions to protect control traffic through other means, such as mapping control packets (using BA classification) to a queue that is marked strict-high or is configured with a high CIR.

You can disable the control queue for all ports on the PIC. To disable the control queue, use the **set chassis fpc *n* pic *n* no-pre-classifier** command. By default, the **no-pre-classifier** statement is not configured and the control queue is operational.

Deleting the **no-pre-classifier** statement re-enables the control queue feature on all ports of the 10-Gigabit Ethernet LAN/WAN PIC.

**NOTE:**

- This functionality is applicable both in OSE and line-rate modes.
- The control queue feature is enabled by default in both OSE and line-rate modes, which can be overridden by the user configuration.
- When the control queue is disabled, various **show queue** commands will show *control queue* in the output. However, all control queue counters are reported as zeros.
- Changing this configuration (enabling or disabling the control queue feature) results in the PIC being taken offline and brought back online.

Once the control queue is disabled, the Layer 2/Layer 3 control packets are subject to queue selection based on BA classification. However, some control protocol packets will not be classified using BA classification, because they might not have a VLAN, MPLS, or IP header. These are:

- Untagged ARP packets
- Untagged Layer 2 control packets such as LACP or Ethernet OAM
- Untagged IS-IS packets

When the control queue feature is disabled, untagged ARP, IS-IS, and other untagged Layer 2 control packets will go to the restricted queue corresponding to the forwarding class associated with queue 0, as shown in the following two examples.

#### Forwarding Untagged Layer2 Control Packets to Queue 3

With this configuration, the forwarding class (FC) associated with queue 0 is "be" (based on the **forwarding-class** statement configuration). "be" maps to restricted-queue number 3 (based on the "restricted-queue" configuration). Hence, with this particular configuration, untagged ARP, IS-IS, and other untagged Layer 2 control packets will go to ingress queue 3 (not to ingress queue 0).

```
[edit chassis]
forwarding-classes {
  queue 0 be;
  queue 1 af-low8;
  queue 2 af-high;
  queue 3 ef;
  queue 4 ops_control;
  queue 5 net_control;
  queue 6 af-low10_12;
}
restricted-queues {
  forwarding-class ef queue-num 0;
  forwarding-class af-low8 queue-num 1;
  forwarding-class af-low10_12 queue-num 1;
  forwarding-class af-high queue-num 2;
  forwarding-class be queue-num 3;
}
```

Forwarding Untagged Layer2 Control Packets to Queue 3

With this configuration, the FC associated with queue 0 is "ef" (based on the **forwarding-class** statement configuration). "ef" maps to restricted-queue number 0 (based on the **restricted-queue** statement configuration). Hence, with this particular configuration, untagged ARP, IS-IS, and other untagged Layer 2 control packets would go to ingress queue 0.

For tagged ARP, IS-IS, or Layer2 control packets, users should configure an explicit dot1p/dot1ad classifier to make sure these packets are directed to the correct queue. Without an explicit dot1p/dot1ad classifier, tagged ARP, IS-IS, or Layer 2 control packets will go to the restricted-queue corresponding to the forwarding class associated with queue 0.

```
[edit chassis]
forwarding-classes {
  queue 0 ef; <<< ef and be are interchanged
  queue 1 af-low8;
  queue 2 af-high;
  queue 3 be; <<< ef and be are interchanged
  queue 4 ops_control;
  queue 5 net_control;
  queue 6 af-low10_12;
}
restricted-queues {
  forwarding-class ef queue-num 0;
  forwarding-class af-low8 queue-num 1;
  forwarding-class af-low10_12 queue-num 1;
  forwarding-class af-high queue-num 2;
  forwarding-class be queue-num 3;
}
```

Related Documentation

- 10-Gigabit Ethernet LAN/WAN PIC Overview on page 289
- Configuring Line-Rate Mode on 10-Gigabit Ethernet LAN/WAN PIC on page 292
- no-pre-classifier

Example: Handling Oversubscription on a 10-Gigabit Ethernet LAN/WAN PIC

Table 32 on page 295 lists the scenarios of handling oversubscription on the 10-Gigabit Ethernet LAN/WAN PIC for different combinations of port groups and active ports on the PIC.

Table 32: Handling Oversubscription on 10-Gigabit Ethernet LAN/WAN PICs

Number of Port Groups with Two Active Ports (A)	Number of Port Groups with One Active Port (B)	Total Number of Ports Used on PIC (C = A x 2 + B)	Status of Oversubscription and Throughput
0	1	1	Oversubscription is not active. Each port will receive 10 Gbps throughput.
0	2	2	Oversubscription is not active. Each port will receive 10 Gbps throughput.

Table 32: Handling Oversubscription on 10-Gigabit Ethernet LAN/WAN PICs (*continued*)

Number of Port Groups with Two Active Ports (A)	Number of Port Groups with One Active Port (B)	Total Number of Ports Used on PIC ( $C = A \times 2 + B$ )	Status of Oversubscription and Throughput
0	5	5	Oversubscription is not active. Each port will receive 10 Gbps throughput.
1	0	2	Oversubscription is active. Each port will receive 5 Gbps throughput (with default shaper configuration).
1	4	6	<p>Oversubscription is active for the port group that has two active ports. Each port in this port group will receive 5 Gbps throughput (with default shaper configuration).</p> <p>For the remaining four ports, oversubscription is not active. Each port will receive 10 Gbps throughput.</p>
3	0	6	Oversubscription is active. Each port will receive 5 Gbps throughput (with default shaper configuration).
5	0	10	Oversubscription is active on all 10 ports (5 port groups). Each port will receive 5 Gbps throughput (with default shaper configuration).

**Related Documentation**

- 10-Gigabit Ethernet LAN/WAN PIC Overview on page 289
- Configuring Line-Rate Mode on 10-Gigabit Ethernet LAN/WAN PIC on page 292

## CHAPTER 22

# Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength

- 10-Gigabit Ethernet DWDM Interface Wavelength Overview on page 297
- Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength on page 297

### 10-Gigabit Ethernet DWDM Interface Wavelength Overview

---

For M320, M120, T320, and T640 routers, the 10-Gigabit Ethernet DWDM PIC enables you to configure 10-Gigabit Ethernet DWDM interfaces with full C-band International Telecommunication Union (ITU)-Grid tunable optics, as defined in the following specifications:

- *Intel TXN13600 Optical Transceiver I2C Interface and Customer EEPROM Preliminary Specification*, July 2004.
- *I2C Reference Document for 300 Pin MSA 10G and 40G Transponder*, Edition 4, August 04, 2003.

By default, the wavelength is 1550.12 nanometers (nm), which corresponds to 193.40 terahertz (THz).

### Configuring the 10-Gigabit Ethernet DWDM Interface Wavelength

---

To configure the wavelength on a 10-Gigabit Ethernet DWDM interface, include the **wavelength** statement at the **[edit interfaces ge-fpc/pic/port optics-options]** hierarchy level:

```
[edit interfaces ge-0/0/0 optics-options]  
wavelength nm;
```

For interface diagnostics, you can issue the **show interfaces diagnostics optics ge-fpc/pic/port** operational mode command.

Table 33 on page 298 shows configurable wavelengths and the corresponding frequency for each configurable wavelength.

Table 33: Wavelength-to-Frequency Conversion Matrix

Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)
1528.77	196.10	1540.56	194.60	1552.52	193.10
1529.55	196.00	1541.35	194.50	1553.33	193.00
1530.33	195.90	1542.14	194.40	1554.13	192.90
1531.12	195.80	1542.94	194.30	1554.94	192.80
1531.90	195.70	1543.73	194.20	1555.75	192.70
1532.68	195.60	1544.53	194.10	1556.56	192.60
1533.47	195.50	1545.32	194.00	1557.36	192.50
1534.25	195.40	1546.12	193.90	1558.17	192.40
1535.04	195.30	1546.92	193.80	1558.98	192.30
1535.82	195.20	1547.72	193.70	1559.79	192.20
1536.61	195.10	1548.52	193.60	1560.61	192.10
1537.40	195.00	1549.32	193.50	1561.42	192.00
1538.19	194.90	1550.12	193.40	1562.23	191.90
1538.98	194.80	1550.92	193.30	1563.05	191.80
1539.77	194.70	1551.72	193.20	1563.86	191.70

## CHAPTER 23

# Configuring 10-Gigabit Ethernet Framing

- 10-Gigabit Ethernet Framing Overview on page 299
- Configuring 10-Gigabit Ethernet Framing on page 299
- Understanding WAN Framing for 10-Gigabit Ethernet Trio Interfaces on page 300

## 10-Gigabit Ethernet Framing Overview

---

The 10-Gigabit Ethernet interfaces support operation in two modes:

- 10GBASE-R, LAN Physical Layer Device (LAN PHY)
- 10GBASE-W, WAN Physical Layer Device (WAN PHY)

When the external interface is running in LAN PHY mode, it bypasses the WIS sublayer to directly stream block-encoded Ethernet frames on a 10-Gigabit Ethernet serial interface. When the external interface is running in WAN PHY mode, it uses the WIS sublayer to transport 10-Gigabit Ethernet frames in an OC192c SONET payload.

WAN PHY mode is supported on MX240, MX480, MX960, T640, and T1600 routers only. Although the external interface provides a lower throughput when running in WAN PHY mode because of the extra SONET overhead, it can interoperate with SONET section or line level repeaters. This creates an advantage when the interface is used for long-distance, point-to-point 10-Gigabit Ethernet links. When the external interface is running in WAN PHY mode, some SONET options are supported. For information about SONET options supported on this interface, see *Configuring SONET/SDH Physical Interface Properties*.

## Configuring 10-Gigabit Ethernet Framing

---

The 10-Gigabit Ethernet interfaces uses the interface type ***xe-fpc/pic/port***. On single port devices, the port number is always zero.

The ***xe-fpc/pic/port*** interface inherits all the configuration commands that are used for gigabit Ethernet (***ge-fpc/pic/port***) interfaces.

To configure LAN PHY or WAN PHY operating mode, include the **framing** statement with the **lan-phy** or **wan-phy** option at the **[edit interfaces *xe-fpc/pic/0* ]** hierarchy level.

```
[edit interfaces xe-fpc/pic/0 framing]
```

**framing** (lan-phy | wan-phy);

To display interface information, use the operational mode command **show interfaces xe-fpc/pic/port extensive**.



**NOTE:** If you configure the WAN PHY mode on an aggregated Ethernet interface, you must set the aggregated Ethernet link speed to OC192.

---

## Understanding WAN Framing for 10-Gigabit Ethernet Trio Interfaces

---

If you use the **wan-phy** statement option at the **[edit interfaces xe-fpc/pic/O framing]** hierarchy level to configure Trio WAN mode framing for 10-Gigabit Ethernet interfaces, then the alarm behavior of the link, although in full compliance with the IEEE 802.3ae 10-Gigabit Ethernet standard, might not be as expected.

In particular:

- The interface does not distinguish between loss of light (LOL), loss of phase lock loop (PLL), or loss of signal (LOS). If a loss of PLL or LOS alarm occurs, then both PLL and LOS alarms are raised. LOL is also raised because there is no separate LOL indication from the hardware.
- The interface does not raise LOS, PLL, or LOL alarms when the fiber is disconnected from the interface port. You must remove the hardware to raise this alarm.
- The interface line-level alarm indicator signal (AIS-L) is not always raised in response to a loss of framing (LOF) defect alarm.
- If the AIS-L or path-level AIS (AIS-P) occurs, the interface path-level loss of code delineation (LCD-P) is not detected. LCD-P is seen during the path-level remote defect indicator (RDI-P) alarm.
- If an AIS-L alarm occurs, the AIS-P is not detected, but the LOP alarm is detected.

None of the alarm issues are misleading, but they make troubleshooting the root cause of problems more complex.

### Related Documentation

- 10-Gigabit Ethernet Framing Overview on page 299



# Configuring 10-Gigabit Ethernet Notification of Link Down Alarm

- 10-Gigabit Ethernet Notification of Link Down Alarm Overview on page 301
- Configuring 10-Gigabit Ethernet Notification of Link Down Alarm on page 301

## 10-Gigabit Ethernet Notification of Link Down Alarm Overview

---

Notification of link down alarm generation and transfer is supported for all 10-Gigabit Ethernet PIC interfaces, M120, M320, and T Series routers.

## Configuring 10-Gigabit Ethernet Notification of Link Down Alarm

---

To configure this option, include the **asynchronous-notification** statement at the **[edit interfaces ge- *fpc/pic/port* together-options]** hierarchy level:

```
[edit interfaces]
ge-fpc/pic/port {
  together-options {
    asynchronous-notification;
  }
}
```



## CHAPTER 25

# Configuring 10-Gigabit Ethernet Notification of Link Down for Optics Alarms

- 10-Gigabit Ethernet Notification of Link Down for Optics Options Overview on page 303
- Configuring 10-Gigabit Ethernet Link Down Notification for Optics Options Alarm or Warning on page 303

## 10-Gigabit Ethernet Notification of Link Down for Optics Options Overview

---

Notification of link down is supported for IQ2 10-Gigabit Ethernet interfaces and MX Series DPCs.

### Related Documentation

- Configuring 10-Gigabit Ethernet Link Down Notification for Optics Options Alarm or Warning on page 303

## Configuring 10-Gigabit Ethernet Link Down Notification for Optics Options Alarm or Warning

---

To configure this option, include the **alarm** or **warning** statement at the **[edit interfaces ge- fpc/pic/port optics-options]** hierarchy level:

```
[edit interfaces]
ge-fpc/pic/port {
  optics-options {
    alarm alarm-name {
      (syslog | link-down);
    }
    warning warning-name {
      (syslog | link-down);
    }
  }
}
```

### Related Documentation

- 10-Gigabit Ethernet Notification of Link Down for Optics Options Overview on page 303



## CHAPTER 26

# Configuring Point-to-Point Protocol over Ethernet

- PPPoE Overview on page 306
- Understanding PPPoE Service Name Tables on page 309
- Evaluation Order for Matching Client Information in PPPoE Service Name Tables on page 314
- Benefits of Configuring PPPoE Service Name Tables on page 314
- Configuring PPPoE on page 315
- Disabling the Sending of PPPoE Keepalive Messages on page 322
- Configuring PPPoE Service Name Tables on page 323
- Creating a Service Name Table on page 324
- Configuring the Action Taken When the Client Request Includes an Empty Service Name Tag on page 324
- Configuring the Action Taken for the Any Service on page 325
- Assigning a Service to a Service Name Table and Configuring the Action Taken When the Client Request Includes a Non-zero Service Name Tag on page 326
- Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information on page 328
- Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name on page 329
- Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client on page 330
- Enabling Advertisement of Named Services in PADO Control Packets on page 331
- Assigning a Service Name Table to a PPPoE Underlying Interface on page 331
- Example: Configuring a PPPoE Service Name Table on page 331
- Tracing PPPoE Operations on page 334
- Troubleshooting PPPoE Service Name Tables on page 336
- Verifying a PPPoE Configuration on page 338

## PPPoE Overview

---

The Point-to-Point Protocol over Ethernet (PPPoE) connects multiple hosts on an Ethernet LAN to a remote site through a single customer premises equipment (CPE) device. Hosts share a common digital subscriber line (DSL), a cable modem, or a wireless connection to the Internet.

A J Series router can be configured as the CPE device for PPPoE connections. To use PPPoE, you must configure the router as a PPPoE client, encapsulate PPP packets over Ethernet, and initiate a PPPoE session.



**NOTE:** J4300 and J6300 routers with asymmetrical DSL (ADSL) Physical Interface Modules (PIMs) and symmetrical high-speed DSL (SHDSL) PIMs can use PPPoE over Asynchronous Transfer Mode (ATM) to connect through DSL lines only, not for direct ATM connections. For information about configuring ADSL and SHDSL interfaces, see [ATM-over-ADSL Overview](#) and [ATM-over-SHDSL Overview](#).

M120, M320, and MX Series routers can be configured as a PPPoE access concentrator server. To configure a PPPoE server on an M120, M320, or MX Series Ethernet logical interface, specify PPPoE encapsulation, include the **pp0** statement for the pseudo PPPoE physical interface, and include the **server** statement in the PPPoE options under the logical interface.



**NOTE:** PPPoE encapsulation is not supported on M120, M320, or MX Series routers on an ATM2 IQ interface.

On the J Series router, PPPoE establishes a point-to-point connection between the client (the Services Router) and the server, also called an access concentrator. Multiple hosts can be connected to the Services Router, and their data can be authenticated, encrypted, and compressed before the traffic is sent to the PPPoE session on the Services Router's Fast Ethernet or ATM-over-ADSL interface. PPPoE is easy to configure and enables services to be managed on a per-user basis rather than on a per-site basis.

This overview contains the following topics:

- PPPoE Interfaces on page 306
- PPPoE Stages on page 307
- Optional CHAP Authentication on page 308

## PPPoE Interfaces

The PPPoE interface to the access concentrator can be a Fast Ethernet interface on any Services Router, a Gigabit Ethernet interface on J4350 and J6350 Services Routers, an ATM-over-ADSL or ATM-over-SHDSL interface on all J Series Services Routers except the J2300, or an ATM-over-SHDSL interface on a J2300 Services Router. The PPPoE

configuration is the same for both interfaces. The only difference is the encapsulation for the underlying interface to the access concentrator:

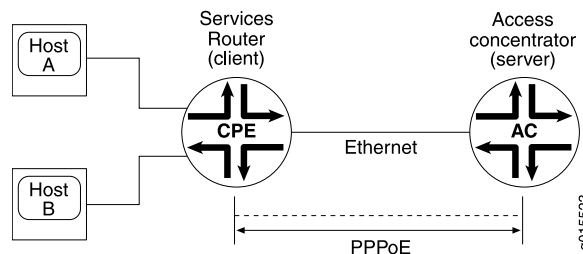
- If the interface is Fast Ethernet, use a PPPoE encapsulation.
- If the interface is ATM over ADSL, use a PPPoE over ATM encapsulation.

The PPPoE interface on M120 or M320 routers acting as a access concentrator can be a Gigabit Ethernet or 10-Gigabit Ethernet interface.

### Ethernet Interface

The Services Router encapsulates each PPP frame in an Ethernet frame and transports the frames over an Ethernet loop. Figure 27 on page 307 shows a typical PPPoE session between a Services Router and an access concentrator on the Ethernet loop.

Figure 27: PPPoE Session on an Ethernet Loop



### PPPoE Stages

PPPoE has two stages, the discovery stage and the PPPoE session stage. In the discovery stage, the client discovers the access concentrator by identifying the Ethernet media access control (MAC) address of the access concentrator and establishing a PPPoE session ID. In the PPPoE session stage, the client and the access concentrator build a point-to-point connection over Ethernet, based on the information collected in the discovery stage.

### PPPoE Discovery Stage

A Services Router initiates the PPPoE discovery stage by broadcasting a PPPoE active discovery initiation (PADI) packet. To provide a point-to-point connection over Ethernet, each PPPoE session must learn the Ethernet MAC address of the access concentrator and establish a session with a unique session ID. Because the network might have more than one access concentrator, the discovery stage allows the client to communicate with all of them and select one.



**NOTE:** A Services Router cannot receive PPPoE packets from two different access concentrators on the same physical interface.

The PPPoE discovery stage consists of the following steps:

1. PPPoE active discovery initiation (PADI)—The client initiates a session by broadcasting a PADI packet on the LAN to request a service.
2. PPPoE active discovery offer (PADO)—Any access concentrator that can provide the service requested by the client in the PADI packet replies with a PADO packet that contains its own name, the unicast address of the client, and the service requested. An access concentrator can also use the PADO packet to offer other services to the client.
3. PPPoE active discovery request (PADR)—From the PADOs it receives, the client selects one access concentrator based on its name or the services offered and sends it a PADR packet to indicate the service or services needed.
4. PPPoE active discovery session-Confirmation (PADS)—When the selected access concentrator receives the PADR packet, it accepts or rejects the PPPoE session.
  - To accept the session, the access concentrator sends the client a PADS packet with a unique session ID for a PPPoE session and a service name that identifies the service under which it accepts the session.
  - To reject the session, the access concentrator sends the client a PADS packet with a service name error and resets the session ID to zero.

---

### PPPoE Session Stage

The PPPoE session stage starts after the PPPoE discovery stage is over. The access concentrator can start the PPPoE session after it sends the PADS packet to the client, or the client can start the PPPoE session after it receives a PADS packet from the access concentrator. A Services Router supports multiple PPPoE sessions on each interface, but no more than 256 PPPoE sessions on all interfaces on the Services Router.

Each PPPoE session is uniquely identified by the Ethernet address of the peer and the session ID. After the PPPoE session is established, data is sent as in any other PPP encapsulation. The PPPoE information is encapsulated within an Ethernet frame and is sent to a unicast address. In this stage, both the client and the server must allocate resources for the PPPoE logical interface.

After a session is established, the client or the access concentrator can send a PPPoE active discovery termination (PADT) packet anytime to terminate the session. The PADT packet contains the destination address of the peer and the session ID of the session to be terminated. After this packet is sent, the session is closed to PPPoE traffic.

### Optional CHAP Authentication

For interfaces with PPPoE encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP). When you enable CHAP on an interface, the interface can authenticate its peer and be authenticated by its peer.

If you configure an interface to handle incoming CHAP packets only (by including the **passive** statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level), the interface does not challenge its peer. However, if the interface is challenged, it responds to the challenge. If you do not include the **passive** statement, the interface always challenges its peer.



For more information about CHAP, see *Configuring the PPP Challenge Handshake Authentication Protocol*.

## Understanding PPPoE Service Name Tables

On an M120 router, M320 router, or MX Series router acting as a remote access concentrator (AC), also referred to as a *PPPoE server*, you can configure up to 32 PPPoE service name tables and assign the service name tables to PPPoE underlying interfaces. A *PPPoE service name table* defines the set of *services* that the router can provide to a PPPoE client. Service entries configured in a PPPoE service name table represent the *service name tags* transmitted between the client and the router in a PPPoE control packet.

This overview covers the following topics to help you understand and configure PPPoE service name tables:

- Interaction Among PPPoE Clients and Routers During the Discovery Stage on page 309
- Service Entries and Actions in PPPoE Service Name Tables on page 310
- ACI/ARI Pairs in PPPoE Service Name Tables on page 311
- Dynamic Profiles and Routing Instances in PPPoE Service Name Tables on page 312
- Maximum Sessions Limit in PPPoE Service Name Tables on page 312
- Static PPPoE Interfaces in PPPoE Service Name Tables on page 313
- PADO Advertisement of Named Services in PPPoE Service Name Tables on page 313

## Interaction Among PPPoE Clients and Routers During the Discovery Stage

In networks with mesh topologies, PPPoE clients are often connected to multiple PPPoE servers (remote ACs). During the PPPoE discovery stage, a PPPoE client identifies the Ethernet MAC address of the remote AC that can service its request, and establishes a unique PPPoE session identifier for a connection to that AC.

The following steps describe, at a high level, how the PPPoE client and the remote AC (router) use the PPPoE service name table to interact during the PPPoE discovery stage:

1. The PPPoE client broadcasts a PPPoE Active Discovery Initiation (PADI) control packet to all remote ACs in the network to request that an AC support certain services.

The PADI packet must contain either, but not both, of the following:

- One and only one nonzero-length service name tag that represents a specific client service
  - One and only one empty (zero-length) service name tag that represents an unspecified service
2. One or more remote ACs respond to the PADI packet by sending a PPPoE Active Discovery Offer (PADO) packet to the client, indicating that the AC can service the client request.

To determine whether it can service a particular client request, the router matches the service name tag received in the PADI packet against the service name tags

configured in its service name table. If a matching service name tag is found in the PPPoE service name table, the router sends the client a PADO packet that includes the name of the AC from which it was sent. If no matching service name tag is found in the PPPoE service name table, the router drops the PADI request and does not send a PADO response to the client.

3. The PPPoE client sends a unicast PPPoE Active Discovery Request (PADR) packet to the AC to which it wants to connect, based on the responses received in the PADO packets.
4. The selected AC sends a PPPoE Active Discovery Session (PADS) packet to establish the PPPoE connection with the client.

## Service Entries and Actions in PPPoE Service Name Tables

A PPPoE service name table can include three types of service entries: named services, an **empty** service, and an **any** service. For each service entry, you specify the action to be taken by the underlying interface when the router receives a PADI packet containing the specified service name tag.

You can configure the following services and actions in a PPPoE service name table:

- **Named service**—Specifies a PPPoE client service that an AC can support. For example, you might configure named services associated with different subscribers who log in to the PPPoE server, such as **user1-service** or **user2-service**, or that correspond to different ISP service level agreements, such as **premium** and **standard**. Each PPPoE service name table can include a maximum of 512 named service entries, excluding **empty** and **any** service entries. A named service is associated with the **terminate** action by default.
- **empty service**—A service tag of zero length that represents an unspecified service. Each PPPoE service name table includes one empty service. The **empty** service is associated with the **terminate** action by default.
- **any service**—Acts as a default service for non-empty service entries that do not match the named service entries or **empty** service entry configured in the PPPoE service name table. Each PPPoE service name table includes one **any** service. The **any** service is useful when you want to match the agent circuit identifier and agent remote identifier information for a PPPoE client, but do not care about the contents of the service name tag transmitted in the control packet. The **any** service is associated with the **drop** action by default.
- **Action**—Specifies the action taken by the underlying PPPoE interface assigned to the PPPoE service name table on receipt of a PADI packet from the client containing a particular service request. You can configure one of the following actions for the associated named service, **empty** service, **any** service, or agent circuit identifier/agent remote identifier (ACI/ARI) pair in the PPPoE service name table on the router:
  - **terminate**—(Default) Directs the router to immediately respond to the PADI packet by sending the client a PADO packet containing the name of the AC that can service the request. Named services, **empty** services, and ACI/ARI pairs are associated with the **terminate** action by default. Configuring the **terminate** action for a service enables

you to more tightly control which PPPoE clients can access and receive services from a particular PPPoE server.

- **delay**—Number of seconds that the PPPoE underlying interface waits after receiving a PADI packet from the client before sending a PADO packet in response. In networks with mesh topologies, you might want to designate a primary PPPoE server and a backup PPPoE server for handling a particular service request. In such a scenario, you can configure a delay for the associated service entry on the backup PPPoE server to allow sufficient time for the primary PPPoE server to respond to the client with a PADO packet. If the primary server does not send the PADO packet within the delay period configured on the backup server, then the backup server sends the PADO packet after the delay period expires.
- **drop**—Directs the router to drop (ignore) a PADI packet containing the specified service name tag when received from a PPPoE client, which effectively denies the client's request to provide the associated service. The **any** service is associated with the **drop** action by default. To prohibit the router from responding to PADI packets that contain **empty** or **any** service name tags, you can configure the **drop** action for the empty or **any** service. You can also use the **drop** action in combination with ACI/ARI pairs to accept specific service name tags only from specific subscribers, as described in the following information about ACI/ARI pairs.

### ACI/ARI Pairs in PPPoE Service Name Tables

To specify agent circuit identifier (ACI) and agent remote identifier (ARI) information for a named service, **empty** service, or **any** service in a PPPoE service name table, you can configure an ACI/ARI pair. An ACI/ARI pair contains an agent circuit ID string that identifies the DSLAM interface that initiated the service request, and an agent remote ID string that identifies the subscriber on the DSLAM interface that initiated the service request. You can think of an ACI/ARI pair as the representation of one or more PPPoE clients accessing the router by means of the PPPoE service name table.

ACI/ARI specifications support the use of wildcard characters in certain formats. You can configure a combined maximum of 8000 ACI/ARI pairs, both with and without wildcards, per PPPoE service name table. You can distribute the ACI/ARI pairs in any combination among the service entries in the service name table.

You must specify the action—**terminate**, **delay**, or **drop**—taken by the underlying PPPoE interface when it receives a client request containing vendor-specific ACI/ARI information that matches the ACI/ARI information configured in the PPPoE service name table on the router. An ACI/ARI pair is associated with the **terminate** action by default.

For example, assume that for the **user1-service** named service, you configure the **drop** action for the service and the **terminate** action for the associated ACI/ARI pairs. In this case, the ACI/ARI pairs identify the DSLAM interfaces and associated subscribers authorized to access the PPPoE server. Using this configuration causes the router to drop PADI packets containing the **user1-service** tag *unless* the PADI packet also contains vendor-specific ACI/ARI information that matches the subscribers identified in one or more of the ACI/ARI pairs. For PADI packets containing matching ACI/ARI information,

the router sends an immediate PADO response to the client indicating that it can provide the requested service for the specified subscribers.

You can also associate a PPPoE dynamic profile, routing instance, and static PPPoE interface with an ACI/ARI pair.

## Dynamic Profiles and Routing Instances in PPPoE Service Name Tables

You can associate a previously configured PPPoE dynamic profile with a named service, **empty** service, or **any** service in the PPPoE service name table, or with an ACI/ARI pair defined for these services. The router uses the attributes defined in the profile to instantiate a dynamic PPPoE subscriber interface based on the service name, ACI, and ARI information provided by the PPPoE client during PPPoE negotiation. The dynamic profile configured for a service entry or ACI/ARI pair in a PPPoE service name table overrides the dynamic profile assigned to the PPPoE underlying interface on which the dynamic PPPoE interface is created.

To specify the routing instance in which to instantiate the dynamic PPPoE interface, you can associate a previously configured routing instance with a named service, **empty** service, or **any** service in the PPPoE service name table, or with an ACI/ARI pair defined for these services. Like dynamic profiles configured for service entries or ACI/ARI pairs, the routing instance configured for the PPPoE service name table overrides the routing instance assigned to the PPPoE underlying interface.

For information about configuring the PPPoE service name table to create a dynamic PPPoE subscriber interface, see *Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation* in the [Junos OS Subscriber Access Configuration Guide](#).

## Maximum Sessions Limit in PPPoE Service Name Tables

To limit the number of PPPoE client sessions that can use a particular service entry in the PPPoE service name table, you can configure the maximum number of active PPPoE sessions using either dynamically-created or statically-created PPPoE interfaces that the router can establish with a particular named service, **empty** service, or **any** service. (You cannot configure the maximum sessions limit for an ACI/ARI pair.) The maximum sessions limit must be in the range 1 through the platform-specific maximum PPPoE sessions supported for your routing platform. The router maintains a count of active PPPoE sessions for each service entry to determine when the maximum sessions limit has been reached.

The router uses the maximum sessions value for a service entry in the PPPoE service name table in conjunction with both of the following:

- The maximum sessions (**max-sessions**) value configured for the PPPoE underlying interface
- The maximum number of PPPoE sessions supported on your routing platform

If your configuration exceeds either of these maximum session limits, the router cannot establish the PPPoE session.

## Static PPPoE Interfaces in PPPoE Service Name Tables

To reserve a previously configured static PPPoE interface for use only by the PPPoE client with matching ACI/ARI information, you can specify a single static PPPoE interface for each ACI/ARI pair defined for a named service entry, **empty** service entry, or **any** service entry in a PPPoE service name table. (You cannot configure a static interface for a service entry that does not have an ACI/ARI pair defined.) The static PPPoE interface associated with an ACI/ARI pair takes precedence over the general pool of static PPPoE interfaces associated with the PPPoE underlying interface configured on the router.

When you configure a static interface in the PPPoE service name table, make sure there is a one-to-one correspondence between the PPPoE client and the static interface. For example, if two clients have identical ACI/ARI information that matches the information in the PPPoE service name table, the router reserves the static interface for exclusive use by the first client that logs in to the router. As a result, the router prevents the second client from logging in.



**NOTE:** You cannot configure a static interface for an ACI/ARI pair already configured with a dynamic profile and routing instance. Conversely, you cannot configure a dynamic profile and routing instance for an ACI/ARI pair already configured with a static interface.

## PADO Advertisement of Named Services in PPPoE Service Name Tables

By default, the advertisement of named services in PADO control packets sent by the router to the PPPoE client is disabled. You can enable advertisement of named services in the PADO packet as a global option when you configure the PPPoE protocol on the router. Configuring PADO advertisement notifies PPPoE clients of the services that the router (AC) can offer.

If you enable advertisement of named services in PADO packets, make sure the number and length of all advertised service entries does not exceed the maximum transmission unit (MTU) size supported by the PPPoE underlying interface.

### Related Documentation

- Evaluation Order for Matching Client Information in PPPoE Service Name Tables on page 314
- Benefits of Configuring PPPoE Service Name Tables on page 314
- Configuring PPPoE Service Name Tables on page 323
- Example: Configuring a PPPoE Service Name Table on page 331
- For information about creating dynamic PPPoE subscriber interfaces, see *Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles* in the [Junos OS Subscriber Access Configuration Guide](#)

## Evaluation Order for Matching Client Information in PPPoE Service Name Tables

---

When the router receives a service request from a PPPoE client, it evaluates the entries configured in the PPPoE service name table to find a match for the client's ACI/ARI information so it can take the appropriate action.

The order of evaluation is as follows:

1. The router evaluates the ACI/ARI information configured for the **any** service entry, and ignores the contents of the service name tag transmitted by the client.
2. If no match is found for the client information, the router evaluates the ACI/ARI information for the **empty** service entry and the named service entries. If an ACI/ARI pair is not configured for these service entries, the router evaluates the other attributes configured for the **empty** service and named services.
3. If there is still no match for the client information, the router evaluates the other attributes configured for the **any** service entry, and ignores both the ACI/ARI information for the **any** service and the contents of the service name tag transmitted by the client. If the **any** service is configured for the default action, **drop**, the router drops the PADR packet. If the **any** service is configured for a nondefault action (**terminate** or **delay**), the router evaluates the other attributes configured for the **any** service.

### Related Documentation

- Understanding PPPoE Service Name Tables on page 309
- Benefits of Configuring PPPoE Service Name Tables on page 314
- Configuring PPPoE Service Name Tables on page 323
- Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation

## Benefits of Configuring PPPoE Service Name Tables

---

This topic describes the benefits of configuring PPPoE service name tables.

Configuring PPPoE service name tables provides the following benefits:

- Enables support for multiple services requested by PPPoE clients, and configuration of an action for the underlying PPPoE interface to take (**delay**, **drop**, or **terminate**) upon receipt of a PPPoE Active Discovery Initiation (PADI) packet requesting that service.
- Provides tighter control over which PPPoE clients can log in to and receive services from a particular PPPoE server.
- Provides load balancing across a set of remote access concentrators (ACs) in a mesh topology by enabling you to configure agent circuit identifier/agent remote identifier (ACI/ARI) pairs for named, **empty**, and **any** service entries to specify the appropriate AC to receive and service a particular PPPoE client request.

- Offers a more targeted approach to configuration of PPPoE sessions based on the service name and ACI/ARI information provided by the PPPoE client during PPPoE negotiation.
- Supports creation of dynamic PPPoE subscriber interfaces in a specified routing instance based on configuration of a service entry or ACI/ARI pair in the PPPoE service name table.
- Enables you to reserve a specified static PPPoE interface for use only by the PPPoE client with matching ACI/ARI information.
- Enables you to specify the maximum number of PPPoE client sessions that can use a particular service entry in the PPPoE service name table.
- Provides redundancy across a set of remote ACs in a mesh topology by enabling you to configure a primary AC and a backup AC for handling a specific service request from a PPPoE client.

For example, on the primary AC for handling a client service, you might configure the **terminate** action for the associated service to direct the primary AC to immediately send a PPPoE Active Discovery Offer (PADO) packet in response to a PADI packet containing that service name tag. On the backup AC for the client service, you might configure the **delay** action for the associated service to specify the number of seconds the backup AC waits after receiving a PADI packet from the client before sending a PADO packet in response. If the primary AC does not send a PADO packet to the client within the delay period configured on the backup AC, then the backup AC sends the PADO packet after the delay period expires.

#### Related Documentation

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Example: Configuring a PPPoE Service Name Table on page 331

---

## Configuring PPPoE

To configure PPPoE on a J Series Services Router, perform the following tasks:

1. Configure PPPoE encapsulation for an Ethernet interface or Ethernet over ATM encapsulation for an ATM-over-ADSL interface.
2. If you are configuring ATM over ADSL, configure LLC encapsulation on the logical interface.
3. Specify the logical Ethernet interface or the logical ATM interface as the underlying interface for the PPPoE session.
4. Configure the operational mode as client.
5. Identify the access concentrator by a unique name.
6. Optionally, specify how many seconds to wait before attempting to reconnect.
7. Provide a name for the type of service provided by the access concentrator.

8. Optionally, configure the maximum transmission unit (MTU) of the interface.
9. Configure the PPPoE interface address.
10. Configure the destination PPPoE interface address.
11. Optionally, configure the MTU size for the protocol family.
12. Optionally, disable the sending of keepalive messages on the logical interface.

To configure PPPoE on an M120 or M320 Multiservice Edge Router or MX Series Universal Edge Router operating as an access concentrator, perform the following tasks:

1. Configure PPPoE encapsulation for an Ethernet interface.
2. Specify the logical Ethernet interface as the underlying interface for the PPPoE session.
3. Optionally, configure the maximum transmission unit (MTU) of the interface.
4. Configure the operational mode as server.
5. Configure the PPPoE interface address.
6. Configure the destination PPPoE interface address.
7. Optionally, configure the MTU size for the protocol family.
8. Optionally, configure one or more PPPoE service name tables and the action taken for each service in the tables.

## Setting the Appropriate Encapsulation on the PPPoE Interface

For PPPoE on an Ethernet interface, you must configure encapsulation on the logical interface and use PPP over Ethernet encapsulation.

For PPPoE on an ATM-over-ADSL interface, you must configure encapsulation on both the physical and logical interfaces. To configure encapsulation on an ATM-over-ADSL physical interface, use Ethernet over ATM encapsulation. To configure encapsulation on an ATM-over-ADSL logical interface, use PPPoE over AAL5 LLC encapsulation. LLC encapsulation allows a single ATM virtual connection to transport multiple protocols.



**NOTE:** PPPoE encapsulation is not supported on an M120 or M320 router on an ATM2 IQ interface.

---

When you configure a point-to-point encapsulation such as PPP on a physical interface, the physical interface can have only one logical interface (only one **unit** statement) associated with it.

To configure physical interface properties, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]  
encapsulation ethernet-over-atm;
```

To configure logical interface encapsulation properties, include the **encapsulation** statement:



```
encapsulation ppp-over-ether;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Perform the task appropriate for the interface on which you are using PPPoE:

- Configuring PPPoE Encapsulation on an Ethernet Interface on page 317
- Configuring PPPoE Encapsulation on an ATM-over-ADSL Interface on page 317

### Configuring PPPoE Encapsulation on an Ethernet Interface

Both the client and the server must be configured to support PPPoE. To configure PPPoE encapsulation on an Ethernet interface, include the **encapsulation** statement:

```
encapsulation ppp-over-ether;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces **pp0** unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces **pp0** unit *logical-unit-number*]

### Configuring PPPoE Encapsulation on an ATM-over-ADSL Interface

To configure the PPPoE encapsulation on a ATM-over-ADSL interface, perform the following steps:

1. Include the **encapsulation** statement at the [edit interfaces *interface-name*] hierarchy level, and specify **ethernet-over-atm**:

```
[edit interfaces pp0]
encapsulation ethernet-over-atm;
```

2. Configure LLC encapsulation on the logical interface by including the **encapsulation** statement and specifying **ppp-over-ether-over-atm-llc**:

```
encapsulation ppp-over-ether-over-atm-llc;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces **pp0** unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces **pp0** unit *logical-unit-number*]

## Configuring a PPPoE Interface

- Configuring the PPPoE Underlying Interface on page 318
- Identifying the Access Concentrator on page 318
- Configuring the PPPoE Automatic Reconnect Wait Timer on page 319
- Configuring the PPPoE Service Name on page 319
- Configuring the PPPoE Server Mode on page 319

- Configuring the PPPoE Client Mode on page 319
- Configuring the PPPoE Source and Destination Addresses on page 320
- Deriving the PPPoE Source Address From a Specified Interface on page 320
- Configuring the PPPoE IP Address by Negotiation on page 320
- Configuring the Protocol MTU PPPoE on page 320
- Example: Configuring a PPPoE Client Interface on a J Series Services Router on page 321
- Example: Configuring a PPPoE Server Interface on an M120 or M320 Router on page 322



**NOTE:** When you configure a static PPPoE logical interface, you must include the `pppoe-options` subhierarchy at the `[edit interfaces pp0 unit logical-unit-number]` hierarchy level or at the `[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number]` hierarchy level. If you omit the `pppoe-options` subhierarchy from the configuration, the commit operation fails.

---

### Configuring the PPPoE Underlying Interface

To configure the underlying Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or ATM interface, include the `underlying-interface` statement:

```
underlying-interface interface-name;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces pp0 unit logical-unit-number pppoe-options]`
- `[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number pppoe-options]`

Specify the logical Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or ATM interface as the underlying interface—for example, `at-0/0/1.0` (ATM VC), `fe-1/0/1.0` (Fast Ethernet interface), or `ge-2/0/0` (Gigabit Ethernet interface).

---

### Identifying the Access Concentrator

When configuring a PPPoE client, identify the access concentrator by a unique name by including the `access-concentrator` statement:

```
access-concentrator name;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces pp0 unit logical-unit-number pppoe-options]`
- `[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number pppoe-options]`

### Configuring the PPPoE Automatic Reconnect Wait Timer

---

By default, after a PPPoE session is terminated, the session attempts to reconnect immediately. When configuring a PPPoE client, you can specify how many seconds to wait before attempting to reconnect, by including the **auto-reconnect** statement:

```
auto-reconnect seconds;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *pp0* unit *logical-unit-number* *pppoe-options*]
- [edit logical-systems *logical-system-name* interfaces *pp0* unit *logical-unit-number* *pppoe-options*]

You can configure the reconnection attempt to occur in 0 through 4,294,967,295 seconds after the session terminates.

### Configuring the PPPoE Service Name

---

When configuring a PPPoE client, identify the type of service provided by the access concentrator—such as the name of the Internet service provider (ISP), class, or quality of service—by including the **service-name** statement:

```
service-name name;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *pp0* unit *logical-unit-number* *pppoe-options*]
- [edit logical-systems *logical-system-name* interfaces *pp0* unit *logical-unit-number* *pppoe-options*]

### Configuring the PPPoE Server Mode

---

When configuring a PPPoE server, identify the mode by including the **server** statement:

```
server;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *pp0* unit *logical-unit-number* *pppoe-options*]
- [edit logical-systems *logical-system-name* interfaces *pp0* unit *logical-unit-number* *pppoe-options*]

### Configuring the PPPoE Client Mode

---

When configuring a PPPoE client, identify the mode by including the **client** statement:

```
client;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *pp0* unit *logical-unit-number* *pppoe-options*]
- [edit logical-systems *logical-system-name* interfaces *pp0* unit *logical-unit-number* *pppoe-options*]

### Configuring the PPPoE Source and Destination Addresses

---

When configuring a PPPoE client or server, assign source and destination addresses—for example, 192.168.1.1/32 and 192.168.1.2. To assign the source and destination address, include the **address** and **destination** statements:

```
address address {  
    destination address;  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces pp0.0 family inet]
- [edit logical-systems *logical-system-name* interfaces pp0.0 family inet]

### Deriving the PPPoE Source Address From a Specified Interface

---

For a router supporting PPPoE, you can derive the source address from a specified interface—for example, the loopback interface, lo0.0—and assign a destination address—for example, 192.168.1.2. The specified interface must include a logical unit number and have a configured IP address. To derive the source address and assign the destination address, include the **unnumbered-address** and **destination** statements:

```
unnumbered-address interface-name destination address;  
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces pp0.0 family inet]
- [edit logical-systems *logical-system-name* interfaces pp0.0 family inet]

### Configuring the PPPoE IP Address by Negotiation

---

You can have the PPPoE client router obtain an IP address by negotiation with the remote end. This method might require the access concentrator to use a RADIUS authentication server. To obtain an IP address from the remote end by negotiation, include the **negotiate-address** statement:

```
negotiate-address;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces pp0.0 family (inet | inet6 | mpls)]
- [edit logical-systems *logical-system-name* interfaces pp0.0 family (inet | inet6 | mpls)]

### Configuring the Protocol MTU PPPoE

---

You can configure the maximum transmission unit (MTU) size for the protocol family. Specify a range from 0 through 5012 bytes. Ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. To set the MTU, include the **mtu** statement:

```
mtu bytes;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces pp0.0 family (inet | inet6 | mpls)]
- [edit logical-systems *logical-system-name* interfaces pp0.0 family (inet | inet6 | mpls)]

You can modify the MTU size of the interface by including the **mtu bytes** statement at the [edit interfaces pp0] hierarchy level:

```
[edit interfaces pp0]
mtu bytes;
```

The default media MTU size used and the range of available sizes on a physical interface depends on the encapsulation used on that interface.

### Example: Configuring a PPPoE Client Interface on a J Series Services Router

Configure a PPPoE over ATM-over-ADSL interface:

```
[edit interfaces]
at-2/0/0 {
  encapsulation ethernet-over-atm;
  atm-options {
    vpi 0;
  }
  dsl-options {
    operating-mode auto;
  }
  unit 0 {
    encapsulation ppp-over-ether-over-atm-llc;
    vci 0.120;
  }
}
pp0 {
  mtu 1492;
  unit 0 {
    ppp-options {
      chap {
        access-profile A-ppp-client;
        local-name A-at-2/0/0.0;
      }
    }
    pppoe-options {
      underlying-interface at-2/0/0;
      client;
      access-concentrator ispl.com;
      service-name "video@ispl.com";
      auto-reconnect 100;
    }
    no-keepalives;
    family inet {
      negotiate-address;
      mtu 100;
    }
    family inet6 {
      negotiate-address;
    }
  }
}
```

```
        mtu 200;
      }
      family mpls {
        negotiate-address;
        mtu 300;
      }
    }
  }
```

---

### Example: Configuring a PPPoE Server Interface on an M120 or M320 Router

---

Configure a PPPoE server over a Gigabit Ethernet interface:

```
[edit interfaces]
ge-1/0/0 {
  vlan-tagging;
  unit 1 {
    encapsulation ppp-over-ether;
    vlan-id 10;
  }
}
pp0 {
  unit 0 {
    pppoe-options {
      underlying-interface ge-1/0/0.0;
      server;
    }
    ppp-options {
    }
    family inet {
      address 22.2.2.1/32 {
        destination 22.2.2.2;
      }
    }
  }
}
```

---

### Disabling the Sending of PPPoE Keepalive Messages

---

When configuring the client, you can disable the sending of keepalive messages on a logical interface by including the **no-keepalives** statement:

```
no-keepalives;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces pp0 unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces pp0 unit *logical-unit-number*]

---

## Configuring PPPoE Service Name Tables

---

To configure PPPoE service name tables:

1. Create a PPPoE service name table.  
See “Creating a Service Name Table” on page 324.
2. (Optional) Configure the action taken for the **empty** service.  
See “Configuring the Action Taken When the Client Request Includes an Empty Service Name Tag” on page 324.
3. (Optional) Configure the action taken for the **any** service.  
See “Configuring the Action Taken for the Any Service” on page 325.
4. Assign a named service to the service name table and optionally configure the action taken for the specified service name.  
See “Assigning a Service to a Service Name Table and Configuring the Action Taken When the Client Request Includes a Non-zero Service Name Tag” on page 326.
5. (Optional) Configure the action taken for an ACI/ARI pair associated with a service.  
See “Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information” on page 328.
6. (Optional) Assign a dynamic profile and routing instance to a service name or ACI/ARI pair to instantiate a dynamic PPPoE subscriber interface.  
See Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation.
7. (Optional) Limit the number of active PPPoE sessions that the router can establish with the specified service.  
See “Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name” on page 329.
8. (Optional) Assign a static PPPoE interface to an ACI/ARI pair to reserve the interface for exclusive use by the PPPoE client with matching ACI/ARI information.  
See “Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client” on page 330.
9. (Optional) Enable advertisement of named services in the PADO control packet sent by the router to the client.  
See “Enabling Advertisement of Named Services in PADO Control Packets” on page 331.
10. Assign a service name table to a PPPoE underlying interface.  
See “Assigning a Service Name Table to a PPPoE Underlying Interface” on page 331.
11. (Optional) Configure trace options for troubleshooting the configuration.  
See “Tracing PPPoE Operations” on page 334.

- Related Documentation**
- Understanding PPPoE Service Name Tables on page 309
  - Benefits of Configuring PPPoE Service Name Tables on page 314
  - Example: Configuring a PPPoE Service Name Table on page 331

---

## Creating a Service Name Table

You can create up to 32 PPPoE service name tables on the router. You can optionally create named services and add them to a service name table. By default, the **empty** service and the **any** service are present in each service name table.

A named service specifies a PPPoE client service that the router, functioning as an access concentrator or PPPoE server, can support. The **empty** service is a service tag of zero length that represents an unspecified service. The **any** service acts as a default service for non-empty service entries that do not match the named or **empty** service entries configured in the PPPoE service name table. Named services and the **empty** service are associated with the **terminate** action by default, and the **any** service is associated with the **drop** action by default.

To create a PPPoE service name table:

- Specify the table name.  

```
[edit protocols pppoe]  
user@host# set service-name-tables table1
```

- Related Documentation**
- Configuring PPPoE Service Name Tables on page 323
  - Understanding PPPoE Service Name Tables on page 309

---

## Configuring the Action Taken When the Client Request Includes an Empty Service Name Tag

You can configure the action taken by the PPPoE underlying interface when it receives a PADI packet that includes a zero-length (empty) service name tag. The **empty** service is present by default in every PPPoE service name table.

To indicate that it can service the client request, the interface returns a PADO packet in response to the PADI packet. By default, the interface immediately responds to the request; this is the **terminate** action. Alternatively, you can configure the **drop** action to ignore (drop) the PADI packet, or the **delay** action to set a delay between receipt of the PADI packet and transmission of the PADO packet.

(Optional) To configure the action taken for the **empty** service in response to a PADI packet from a PPPoE client:

- Specify the action.  

```
[edit protocols pppoe service-name-tables table1]  
user@host# set service empty drop
```



You can also accomplish the following optional tasks when you configure the **empty** service:

- Specify the agent circuit identifier (ACI) and agent remote identifier (ARI) information to determines the action taken by the PPPoE underlying interface when it receives a PADI packet with matching ACI/ARI information.
- Specify a dynamic profile and routing instance with which the router instantiates a dynamic PPPoE subscriber interface.
- Limit the number of active PPPoE sessions that the router can establish with the **empty** service.

#### Related Documentation

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information on page 328
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
- Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name on page 329

## Configuring the Action Taken for the Any Service

The **any** service acts as a default service for service name tags transmitted by the client that do not match any of the service entries configured in the PPPoE service name table on the router. By configuring an action for the **any** service, you specify the action taken by the PPPoE underlying interface when it receives a PADI control packet from a client that includes a non-empty service name tag that does not match any of the named service entries or **empty** service entry in the PPPoE service name table.

Each PPPoE service name table includes one **any** service entry associated by default with the **drop** action. The **drop** action ignores a PADI packet containing a nonmatching service name tag. Alternatively, you can configure the **terminate** action to immediately respond to the PADI packet with a PADO packet, or the **delay** action to specify a delay between receipt of the PADI packet and transmission of the PADO packet.

To configure the action taken for the **any** service in response to a PADI packet from a PPPoE client:

- Specify the action.

```
[edit protocols pppoe service-name-tables table]
user@host# set service any terminate
```

You can also accomplish the following optional tasks when you configure the **any** service:

- Specify the agent circuit identifier (ACI) and agent remote identifier (ARI) information to determine the action taken by the PPPoE underlying interface when it receives a PADI packet with matching ACI/ARI information.
- Specify a dynamic profile and routing instance with which the router instantiates a dynamic PPPoE subscriber interface.
- Limit the number of active PPPoE sessions that the router can establish with the **any** service.

**Related  
Documentation**

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information on page 328
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
- Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name on page 329

---

## Assigning a Service to a Service Name Table and Configuring the Action Taken When the Client Request Includes a Non-zero Service Name Tag

---

You can configure a maximum of 512 named service entries, excluding **empty** and **any** service entries, across all PPPoE service name tables on the router. A named service specifies a PPPoE client service that the router, functioning as an access concentrator or PPPoE server, can support. You can optionally configure the action taken by the PPPoE underlying interface when it receives a PADI packet that includes a matching named service (service name tag).

To indicate that it can service the client request, the interface returns a PADO packet in response to the PADI packet. By default, the interface immediately responds to the request; this is the **terminate** action. Alternatively, you can configure the **drop** action to ignore (drop) the PADI packet, or the **delay** action to set a delay between receipt of the PADI packet and transmission of the PADO packet.

(Optional) To configure a named service for a PPPoE service name table, do one of the following:

- Assign a service name to the table. The **terminate** action is applied to the service by default.  

```
[edit protocols pppoe service-name-tables table1]  
user@host# set service gold-service
```
- Specify the action taken for a service in response to a PADI packet from a PPPoE client.  

```
[edit protocols pppoe service-name-tables table1]  
user@host# set service gold-service delay 25
```

You can also accomplish the following optional tasks when you configure a named service:

- Specify the agent circuit identifier (ACI) and agent remote identifier (ARI) information to determine the action taken by the PPPoE underlying interface when it receives a PADI packet with matching ACI/ARI information.
- Specify a dynamic profile and routing instance with which the router instantiates a dynamic PPPoE subscriber interface.
- Limit the number of active PPPoE sessions that the router can establish with the specified named service.

**Related  
Documentation**

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information on page 328
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
- Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name on page 329

## Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information

---

You can configure up to 8000 agent circuit identifier/agent remote identifier (ACI/ARI) pairs per PPPoE service name table, distributed in any combination among the named, **empty**, and **any** service entries in the service name table. You can optionally configure the action taken by the PPPoE underlying interface when it receives a PADI packet that includes a service name tag and the vendor-specific tag with ACI/ARI information that matches the ACI/ARI pair that you specify.

You can use an asterisk (\*) as a wildcard character to match ACI/ARI pairs, the ACI alone, or the ARI alone. The asterisk can be placed only at the beginning, the end, or both the beginning and end of the identifier string. You can also specify an asterisk alone for either the ACI or the ARI. You cannot specify only an asterisk for both the ACI and the ARI. When you specify a single asterisk as the identifier, that identifier is ignored in the PADI packet.

For example, suppose you care about matching only the ACI and do not care what value the ARI has in the PADI packet, or even whether the packet contains an ARI value. In this case you can set the *remote-id-string* to a single asterisk. Then the interface ignores the ARI received in the packet and the interface takes action based only on matching the specified ACI.

To indicate that it can service the client request, the interface returns a PADO packet in response to the PADI packet. By default, the interface immediately responds to the request; this is the **terminate** action. Alternatively, you can configure the **drop** action to ignore (drop) the PADI packet, or the **delay** action to set a delay between receipt of the PADI packet and transmission of the PADO packet.

To configure an ACI/ARI pair for a named, **empty**, or **any** service, do one of the following:

- Assign an ACI/ARI pair to the service name. The **terminate** action is applied to the pair by default.

```
[edit protocols pppoe service-name-tables table1]  
user@host# set service gold-service agent-specifier aci DSLAM:3/0/1/101 ari *user*
```

- Specify the action taken for the ACI/ARI pair in response to a PADI packet from a PPPoE client.

```
[edit protocols pppoe service-name-tables table1]  
user@host# set service any agent-specifier aci velorum-ge-2/0/3 ari westford delay  
90
```

In this example, an ACI/ARI pair and the **delay** action are configured for the **any** service. Configuring an ACI/ARI pair for the **any** service is useful when you want to match the agent circuit identifier and agent remote identifier information for a specific PPPoE client, but do not care about the contents of the service name tag transmitted by the client in the PADI packet.

You can also accomplish the following optional tasks when you configure an ACI/ARI pair:

- Specify a dynamic profile and routing instance with which the router instantiates a dynamic PPPoE subscriber interface.
- Reserve a specified static PPPoE interface for exclusive use by the PPPoE client with match ACI/ARI information.

**Related  
Documentation**

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
- Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client on page 330

---

## Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name

---

To limit the number of PPPoE client sessions that can use a particular service entry in the PPPoE service name table, you can configure the maximum number of PPPoE sessions using static or dynamic PPPoE interfaces that the router can establish with the specified named service, **empty** service, or **any** service. You cannot configure a maximum sessions limit for an ACI/ARI pair in the service name table.

The maximum sessions limit must be in the range 1 through the platform-specific maximum PPPoE sessions supported for your routing platform. The router maintains a count of active PPPoE sessions for each service entry to determine when the maximum sessions limit has been reached.

To limit the number of PPPoE client sessions for a particular named, **empty**, or **any** service:

- Configure the maximum sessions limit for the specified service:

```
[edit protocols pppoe service-name-tables tableEast]  
user@host# set service premium-service max-sessions 100
```

**Related  
Documentation**

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323

## Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client

---

To reserve a static PPPoE interface for exclusive use by the PPPoE client with matching agent circuit identifier/agent remote identifier (ACI/ARI) information, you can assign a previously configured static PPPoE interface to an ACI/ARI pair defined for a named service entry, **empty** service entry, or **any** service entry in a PPPoE service name table. You cannot assign a static PPPoE interface directly to a service entry that does not have an ACI/ARI pair defined.

Observe the following guidelines when you configure a static PPPoE interface for an ACI/ARI pair:

- You can specify only one static PPPoE interface per ACI/ARI pair.
- If the ACI/ARI pair represents an individual PPPoE client, make sure there is a one-to-one correspondence between the client and the static PPPoE interface.
- The static interface associated with the ACI/ARI pair takes precedence over the general pool of static interfaces associated with the PPPoE underlying interface.
- You cannot configure a static interface for an ACI/ARI pair already configured with a dynamic profile and routing instance. Conversely, you cannot configure a dynamic profile and routing instance for an ACI/ARI pair already configured with a static interface.

Before you begin:

- Configure the static PPPoE interface on a M120, M320, or MX Series router.

See “Configuring PPPoE” on page 315.

To reserve a static PPPoE interface for exclusive use by the PPPoE client with matching ACI/ARI information:

- Assign a previously configured static PPPoE interface to the ACI/ARI pair defined for a named, **empty**, or **any** service entry:

```
[edit protocols pppoe service-name-tables tableEast]
user@host# set service any agent-specifier aci velorum-ge-2/0/3 ari westford
static-interface pp0.100
```

### Related Documentation

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323

## Enabling Advertisement of Named Services in PADO Control Packets

You can enable advertisement of named services in PADO control packets sent by the router to the PPPoE client to indicate the services that the router can offer. By default, advertisement of named services in PADO packets is disabled. You can enable PADO advertisement as a global option on the router when you configure the PPPoE protocol.



**NOTE:** Make sure the combined number and length of all named services advertised in the PADO packet does not exceed the MTU size of the PPPoE underlying interface.

To enable advertisement of named services in PADO packets:

- Configure the PPPoE protocol to enable PADO advertisement:

```
[edit protocols pppoe]
user@host# set pado-advertise
```

### Related Documentation

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323

## Assigning a Service Name Table to a PPPoE Underlying Interface

You must assign the PPPoE service name table to a PPPoE underlying interface.

Before you begin:

- Specify PPPoE as the encapsulation method on the underlying interface.

See *Setting the Appropriate Encapsulation on the PPPoE Interface* in “Configuring PPPoE” on page 315.

To assign a service name table to a PPPoE underlying interface:

- Specify the table name:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set pppoe-underlying-options service-name-table table1
```

### Related Documentation

- Configuring PPPoE Service Name Tables on page 323
- Example: Configuring a PPPoE Service Name Table on page 331

## Example: Configuring a PPPoE Service Name Table

This example shows how you can configure a PPPoE service name table on an M120 router, M320 router, or MX Series router with service entries that correspond to different client services. By configuring the appropriate actions (**delay**, **terminate**, or **drop**) and

agent circuit identifier/agent remote identifier (ACI/ARI) pairs for the service entries, you can provide load balancing and redundancy across a set of remote access concentrators (ACs) in a mesh topology, and determine how best to allocate service requests from PPPoE clients to the servers in your network.

In this example, the PPPoE service name table, Table1, contains the following service entries:

- **user1-service**—Named service representing the subscriber service for user1.
- **user2-service**—Named service representing the subscriber service for user2.
- **empty** service—Represents an unspecified service.

To configure a PPPoE service name table with service entries that correspond to different subscriber services:

1. Create the PPPoE service name table and define the services and associated actions.

```
[edit protocols pppoe]
service-name-tables Table1 {
  service empty {
    drop;
  }
  service user1-service {
    terminate;
    agent-specifier {
      aci "east*" ari "wfd*" delay 10;
      aci "west*" ari "svl*" delay 10;
    }
  }
  service user2-service {
    delay 20;
  }
}
```

This example creates a PPPoE service name table named Table1 with three service entries, as follows:

- The **empty** service is configured with the **drop** action. This action prohibits the router (AC) from responding to PADI packets from the client that contain empty service name tags.
- The **user1-service** named service is configured with both the **terminate** action, and two ACI/ARI (agent-specifier) pairs:
  - The **terminate** action directs the router to immediately respond to PADI packets from the client that contain the **user1-service** tag, and is the default action for named services.
  - The 10-second delay configured for each ACI/ARI pair applies only to PADI packets from the client that contains a vendor-specific tag with matching ACI and ARI information. In this example, configuring the **delay** action indicates that the **east** or **west** server is considered the backup AC for handling these client requests, and that you expect an AC other than **east** or **west** to handle the request as the primary server. If the primary AC does not respond to the client with a PADO packet within



10 seconds, then the **east** or **west** backup AC sends the PADO packet after the 10-second delay expires.

- The **user2-service** named service is configured with a 20-second delay, indicating that you expect an AC other than the one on which this PPPoE service name table is configured to be the primary AC for handling this client request. If the primary AC does not respond to the client with a PADO packet within 20 seconds, then the backup AC (that is, the router on which you are configuring the service name table) sends the PADO packet after the 20-second delay expires.
2. Assign the PPPoE service name table to a PPPoE underlying interface configured with PPPoE encapsulation.

```
[edit interfaces]
ge-2/0/3 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    encapsulation ppp-over-ethernet;
    pppoe-underlying-options {
      service-name-table Table1;
    }
  }
}
```

3. (Optional) Verify the PPPoE service name table configuration.

```
user@host> show pppoe service-name-tables Table1
```

```
Service Name Table: Table1
Service Name: <empty>
Service Action: Drop

Service Name: user1-service
Service Action: Terminate
  ACI: east*
  ARI: wfd*
    ACI/ARI Action: Delay 10 seconds
  ACI: west*
  ARI: svl*
    ACI/ARI Action: Delay 10 seconds

Service Name: user2-service
Service Action: Delay 20 seconds
```

4. (Optional) Verify whether the PPPoE service name table has been properly assigned to the underlying PPPoE interface, and whether packet transfer between the router (AC) and PPPoE client is working correctly.

```
user@host> show pppoe underlying-interfaces ge-2/0/3.0 extensive
```

```
ge-2/0/3.0 Index 72
State: Static, Dynamic Profile: None,
Max Sessions: 4000, Active Sessions: 2,
Service Name Table: Table1, Duplicate Protection: Off,
AC Name: east
PacketType          Sent      Received
  PADI                0          2
  PADO                2          0
```

PADR	0	2
PADS	2	0
PADT	0	1
Service name error	0	0
AC system error	0	0
Generic error	0	0
Malformed packets	0	0
Unknown packets	0	0

Examine the command output to ensure the following:

- The **Service Name Table** field displays the name of the correct PPPoE service name table. This field displays **none** if no service name table has been associated with the specified interface.
- The **Sent** and **Received** values for the **Service name error** field are 0 (zero). For example, a nonzero value in the **Received** field for **Service name error** indicates that there are errors in the control packets received from PPPoE clients, such as a PADI packet that does not contain a service name tag.

**Related  
Documentation**

- Understanding PPPoE Service Name Tables on page 309
- Configuring PPPoE Service Name Tables on page 323
- Troubleshooting PPPoE Service Name Tables on page 336

---

## Tracing PPPoE Operations

The Junos OS trace feature tracks PPPoE operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file called **pppoed** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **pppoed** reaches 128 kilobytes (KB), it is renamed **pppoed.0**, then **pppoed.1**, and finally **pppoed.2**, until there are three trace files. Then the oldest trace file (**pppoed.2**) is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the [Junos OS System Log Messages Reference](#).)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure PPPoE tracing operations:

1. Specify that you want to configure tracing options.

```
[edit protocols pppoe]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure the number and size of the log files.
4. (Optional) Configure access to the log file.
5. (Optional) Configure a regular expression to filter logging events.
6. (Optional) Configure flags to filter the operations to be logged.

Optional PPPoE traceoptions operations are described in the following sections:

- Configuring the PPPoE Trace Log Filename on page 335
- Configuring the Number and Size of PPPoE Log Files on page 335
- Configuring Access to the PPPoE Log File on page 335
- Configuring a Regular Expression for PPPoE Lines to Be Logged on page 335
- Configuring the PPPoE Tracing Flags on page 336

## Configuring the PPPoE Trace Log Filename

By default, the name of the file that records trace output for PPPoE is **pppoed**. You can specify a different name with the **file** option.

## Configuring the Number and Size of PPPoE Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **filename.0**, then **filename.1**, and finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB).

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (**filename**) reaches 2 MB, **filename** is renamed **filename.0**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0** is renamed **filename.1** and **filename** is renamed **filename.0**. This process repeats until there are 20 trace files. Then the oldest file (**filename.19**) is overwritten by the newest file (**filename.0**).

## Configuring Access to the PPPoE Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

## Configuring a Regular Expression for PPPoE Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions to be matched.

## Configuring the PPPoE Tracing Flags

By default, no events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

**Table 34: PPPoE Trace Operation Flags**

Flag	Description
<b>all</b>	Trace all operations
<b>config</b>	Trace configuration events
<b>events</b>	Trace events
<b>gres</b>	Trace GRES events
<b>init</b>	Trace initialization events
<b>interface-db</b>	Trace interface database events
<b>memory</b>	Trace memory processing events
<b>protocol</b>	Trace protocol events
<b>rtsock</b>	Trace routing socket events
<b>session-db</b>	Trace connection events and flow
<b>signal</b>	Trace signal operations
<b>state</b>	Trace state handling events
<b>timer</b>	Trace timer processing
<b>ui</b>	Trace user interface processing

To configure the flags for the events to be logged, configure the flags:

- `[edit protocols pppoe traceoptions]`  
`user@host# set flag authentication`

---

## Troubleshooting PPPoE Service Name Tables

**Problem** A misconfiguration of a PPPoE service name table can prevent PPPoE services from being properly activated. Configuration options for PPPoE service name tables are simple, which should simplify discovering where a misconfiguration exists. PPPoE clients cannot connect if the service name table contains no match for the service name tag carried in the PADI packet.

The symptom of a service name table misconfiguration is that the client connection process stops at the negotiation stage and the PADI packets are ignored. You can use the **show pppoe statistics** command to examine the PPPoE packet counts for a problem.

When the service name table is properly configured, packets sent and received increment symmetrically. The following sample output shows a PADO sent count equal to the PADI received count, and PADS sent count equal to the PADR received count. This output indicates that the PPPoE negotiation is proceeding successfully and that the service name table is not misconfigured.

```
user@host> show pppoe statistics ge-2/0/3.1
```

```
Active PPPoE sessions: 2
```

PacketType	Sent	Received
PADI	0	16
PADO	16	0
PADR	0	16
PADS	16	0
PADT	0	0
Service name error	0	0
AC system error	0	0
Generic error	0	0
Malformed packets	0	0
Unknown packets	0	0

When the service name table is misconfigured, the output of the **show pppoe statistics** command indicates that the number of PADI packets received on the underlying interface is increasing, but the number of PADO packets sent remains at zero. The following sample output shows a PADI count of 100 and a PADO count of 0.

```
user@host> show pppoe statistics ge-2/0/3.1
```

```
Active PPPoE sessions: 0
```

PacketType	Sent	Received
PADI	0	100
PADO	0	0
PADR	0	0
PADS	0	0
PADT	0	0
Service name error	0	0
AC system error	0	0
Generic error	0	0
Malformed packets	0	0
Unknown packets	0	0

When you believe a misconfiguration exists, use the **monitor traffic interface** command on the underlying interface to determine which service name is being requested by the PPPoE client. The following sample output shows that the client is requesting Service1 in the service name tag.

```
user@host> monitor traffic interface ge-2/0/3.1 print-hex print-ascii
Listening on ge-2/0/3.1, capture size 96 bytes
```

```
11:49:41.436682 In PPPoE PADI [Service-Name "Service1"] [Host-Uniq UTF8]
[Tag-0x120 UTF8] [Vendor-Specific UTF8]
0x0000 ffff ffff ffff 0090 1a42 0ac1 8100 029a .....B.....
0x0010 8863 1109 0000 00c9 0101 0008 5365 7276 .c.....Serv
0x0020 6963 6531 0103 0004 1200 9c43 0120 0002 ice1.....C....
```

```
0x0030  044a 0105 00ab 0000 0de9 0124 783a 3132  .J.....$x:12
0x0040  3030 3963                                009c
```

You can then use the **show pppoe service-name-tables** command to determine whether you have misspelled the name of the service or perhaps not configured the service at all.

**Cause** Typical misconfigurations appear in the service name table configurations.

**Solution** Use the appropriate statements to correct the misconfiguration.

**Related Documentation**

- [Configuring PPPoE Service Name Tables on page 323](#)
- `show pppoe service-name-tables`
- `show pppoe statistics`
- `show pppoe underlying-interfaces`

---

## Verifying a PPPoE Configuration

---

**Purpose** You can use show commands to display and verify the PPPoE configuration.

**Action** To verify a PPPoE configuration, you can issue the following operational mode commands:

- `show interfaces at-fpc/pic/port extensive`
- `show interfaces pp0`
- `show pppoe interfaces`
- `show pppoe version`
- `show pppoe service-name-tables`
- `show pppoe sessions`
- `show pppoe statistics`
- `show pppoe underlying-interfaces`

For more information about these operational mode commands, see the [Junos OS Administration Guide for Security Devices](#) and the [Junos OS Interfaces Command Reference](#).

# Configuring Ethernet Ring Protection Switching

- Ethernet Ring Protection Switching Overview on page 339
- Understanding Ethernet Ring Protection Switching Functionality on page 340
- Configuring Ethernet Ring Protection Switching on page 344
- Example: Ethernet Ring Protection Switching Configuration on page 345

## Ethernet Ring Protection Switching Overview

---

MX Series routers support *Ethernet ring protection switching*, which helps achieve high reliability and network stability. Links in the ring will never form loops that fatally affect the network operation and services availability. The basic idea of an Ethernet ring is to use one specific link to protect the whole ring. This special link is called a *ring protection link (RPL)*. If no failure happens in other links of the ring, the RPL blocks the traffic and is not used. RPL is controlled by a special node called an *RPL owner*. There is only one RPL owner in a ring. The RPL owner is responsible for blocking traffic over the RPL. Under ring failure conditions, the RPL owner is responsible for unblocking traffic over the RPL. A ring failure results in protection switching of the RPL traffic. An APS protocol is used to coordinate the protection actions over the ring. Protection switching blocks traffic on the failed link and unblocks the traffic on the RPL. When the failure clears, revertive protection switching blocks traffic over the RPL and unblocks traffic on the link on which the failure is cleared.

The following standards provide detailed information on Ethernet ring protection switching:

- IEEE 802.1Q - 1998
- IEEE 802.1D - 2004
- IEEE 802.1Q - 2003
- Draft ITU-T Recommendation G.8032/Y.1344, *Ethernet Ring protection switching*
- ITU-T Y.1731, *OAM functions and mechanisms for Ethernet-based networks*

For additional information on configuring Ethernet ring protection switching on MX Series routers, see the *Layer 2 Configuration Guide* for a complete example of Ethernet rings and information about STP loop avoidance and prevention.

- Related Documentation**
- Understanding Ethernet Ring Protection Switching Functionality on page 340
  - Configuring Ethernet Ring Protection Switching on page 344
  - Example: Ethernet Ring Protection Switching Configuration on page 345

## Understanding Ethernet Ring Protection Switching Functionality

---

- Acronyms on page 340
- Ring Nodes on page 340
- Ring Node States on page 341
- Failure Detection on page 341
- Logical Ring on page 341
- FDB Flush on page 341
- Traffic Blocking and Forwarding on page 341
- RAPS Message Blocking and Forwarding on page 341
- Dedicated Signaling Control Channel on page 343
- RAPS Message Termination on page 343
- Manual Switch on page 343
- Nonrevertive Switch on page 343
- Multiple Rings on page 343
- Node ID on page 343
- Bridge Domains with the Ring Port on page 343

## Acronyms

The following acronyms are used in this section:

- MA—Maintenance association
- MEP—Maintenance association end point
- OAM—Connectivity fault management daemon
- FDB—MAC forwarding database
- STP—Spanning Tree Protocol
- RAPS—Ring automatic protection switching
- WTR—Wait to restore
- RPL—Ring protection link

## Ring Nodes

Multiple nodes are used to form a ring. For each ring node. There are two different node types:

- Normal node—The node has no special role on the ring.



- RPL owner node—The node owns the RPL and blocks or unblocks traffic over the RPL. This node also initiates the RAPS message.

## Ring Node States

There are three different states for each node of a specific ring:

- init—Not a participant of a specific ring.
- idle—No failure on the ring, the node is performing normally. For normal node, traffic is unblocked on both ring ports. For the RPL owner, traffic is blocked on the ring port that connects to the RPL and unblocked on the other ring port.
- protection—A failure occurred on the ring. For normal node, traffic is blocked on the ring port that connects to the failing link and unblocked on working ring ports. For the RPL owner, traffic is unblocked on both ring ports if they connect to non-failure links.

There can be only one RPL owner for each ring. The user configuration must guarantee this, because the APS protocol cannot check this.

## Failure Detection

Ethernet ring operation depends on quick and accurate failure detection. The failure condition *signal failure (SF)* is supported. For SF detection, an Ethernet continuity check MEP must be configured for each ring link. For fast protection switching, a 10-ms transmission period for this MEP group is supported. OAM monitors the MEP group's MA and reports SF or SF clear events to the Ethernet ring control module. For this MEP group, the action profile must be configured to update the interface device IFF\_LINKDOWN flag. OAM updates the IFF\_LINKDOWN flag to notify the Ethernet ring control module.

## Logical Ring

This feature currently supports only the physical ring, which means that two adjacent nodes of a ring must be physically connected and the ring must operate on the physical interface, not the VLAN.

## FDB Flush

When ring protection switching occurs, normally an *FDB flush* should be executed. The Ethernet ring control module should use the same mechanism as the STP to trigger the FDB flush. The Ethernet ring control module controls the ring port physical interface's default STP index to execute the FDB flush.

## Traffic Blocking and Forwarding

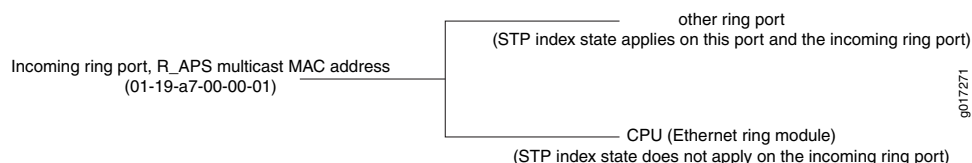
The Ethernet ring control module uses the same mechanism as the STP to control forwarding or discarding of user traffic. The Ethernet ring control module sets the ring port physical interface default STP index state to forwarding or discarding in order to control user traffic.

## RAPS Message Blocking and Forwarding

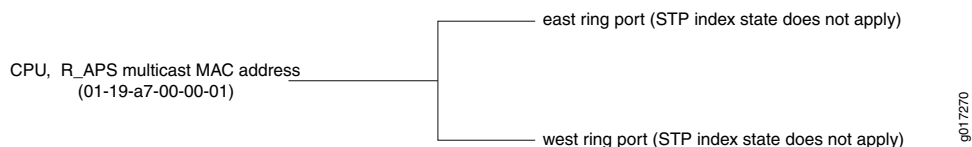
The router treats the ring automatic protection switching (RAPS) message the same as user traffic for forwarding RAPS messages between two ring ports. The ring port physical

interface default STP index state also controls forwarding RAPS messages between the two ring ports. Other than forwarding RAPS between the two ring ports, as shown in Figure 28 on page 342, the system also needs to forward the RAPS message between the CPU (Ethernet ring control module) and the ring port. This type of forwarding does not depend on the ring port physical interfaces STP index state. The RAPS message is always sent by the router through the ring ports, as shown in Figure 29 on page 342. A RAPS message received from a discarding ring port is sent to the Ethernet ring control module, but is not sent to the other ring port.

**Figure 28: Protocol Packets from the Network to the Router**



**Figure 29: Protocol Packets from the Router to the Network**



Juniper Networks routers use an implicit filter to achieve these routes. Each implicit filter binds to a bridge domain. Therefore, the east ring port control channel and the west ring port control channel of a particular ring instance must be configured to the same bridge domain. For each ring port control channel, a filter term is generated to control RAPS message forwarding. The filter number is the same as the number of bridge domains that contain the ring control channels. If a bridge domain contains control channels from multiple rings, the filter related to this bridge domain will have multiple terms and each term will relate to a control channel. The filter has command parts and control-channel related parts, as follows:

- Common terms:
    - term 1: if [Ethernet type is not OAM Ethernet type (0x8902)]  
          { accept packet }
    - term 2: if [source MAC address belongs to this bridge]  
          { drop packet, our packet loop through the ring and come back to home }
    - term 3: if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,0x00,0x00,0x01) AND [ring port STP status is DISCARDING]  
          { send to CPU }
  - Control channel related terms:
    - if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,0x00,0x00,0x01) AND [ring port STP status is FORWARDING] AND [Incoming interface IFL equal to control channel IFL]  
      { send packet to CPU and send to the other ring port }
- default term: accept packet.

## Dedicated Signaling Control Channel

For each ring port, a dedicated signaling control channel with a dedicated VLAN ID must be configured. In Ethernet ring configuration, only this control logical interface is configured and the underlying physical interface is the physical ring port. Each ring requires that two control physical interfaces be configured. These two logical interfaces must be configured in a bridge domain in order to forward RAPS PDUs between the two ring control physical interfaces. If the control channel logical interface is not a trunk port, only control logical interfaces will be configured in ring port configuration. If this control channel logical interface is a trunk port, in addition to the control channel logical interfaces, a dedicated VLAN ID must be configured.

## RAPS Message Termination

The RAPS message starts from the originating node, travels through the entire ring, and terminates in the originating node unless a failure is present in the ring. The originating node must drop the RAPS message if the source MAC address in the RAPS message belongs to itself. The source MAC address is the node's node ID.

## Manual Switch

Manual switch is not supported in this release.

## Nonrevertive Switch

In revertive operation, once the condition causing a switch has cleared, traffic is blocked on the RPL and restored to the working transport entity. In nonrevertive operation, traffic is allowed to use the RPL if it has not failed, even after a switch condition has cleared. Nonrevertive switching is not supported in this release.

## Multiple Rings

The Ethernet ring control module supports multiple rings in each node, (two logical interfaces are part of each ring). However, interconnection of multiple rings is not supported in this release. The interconnection of two rings means that two rings may share the same link or share the same node.

## Node ID

For each node in the ring, a unique *node ID* identifies each node. The node ID is the node's MAC address. You can configure this node ID when configuring the ring on the node or automatically select an ID such as STP. In most cases, you will not configure this and the router will select a node ID, like STP does. It should be the manufacturing MAC address. The ring node ID should not be changed, even if you change the manufacturing MAC address. Any MAC address can be used if you make sure each node in the ring has a different node ID.

## Bridge Domains with the Ring Port

From the router point of view, the protection group is seen as an abstract logical port that can be configured to any bridge domain. Therefore, if you configure one ring port or its logical interface in a bridge domain; you must configure the other related ring port or

its logical interface to the same bridge domain. The bridge domain that includes the ring port acts as any other bridge domain and supports the IRB layer 3 interface.

**Related  
Documentation**

- Ethernet Ring Protection Switching Overview on page 339
- Configuring Ethernet Ring Protection Switching on page 344
- Example: Ethernet Ring Protection Switching Configuration on page 345

---

## Configuring Ethernet Ring Protection Switching

---

The inheritance model follows:

```
protection-group {  
  ethernet-ring ring-name (  
    node-id mac-address;  
    ring-protection-link-owner;  
    east-interface {  
      control-channel channel-name {  
        ring-protection-link-end;  
      }  
    }  
    west-interface {  
      node-id mac-address;  
      control-channel channel-name {  
        ring-protection-link-end;  
      }  
    }  
    data-channel {  
      vlan number;  
    }  
    guard-interval number;  
    restore-interval number;  
  }  
}
```

For each ring, a protection group must be configured. There may be several rings in each node, so there should be multiple protection groups corresponding to the related Ethernet rings.

Three interval parameters (**restore-interval**, **guard-interval**, and **hold-interval**) can be configured at the protection group level. These configurations are global configurations and apply to all Ethernet rings if the Ethernet ring doesn't have a more specific configuration for these values. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

**Related  
Documentation**

- Ethernet Ring Protection Switching Overview on page 339
- Understanding Ethernet Ring Protection Switching Functionality on page 340
- Example: Ethernet Ring Protection Switching Configuration on page 345

## Example: Ethernet Ring Protection Switching Configuration

This example describes how to configure Ethernet ring protection switching:

- Requirements on page 345
- Ethernet Ring Overview and Topology on page 345
- Configuring a Three-Node Ring on page 345

### Requirements

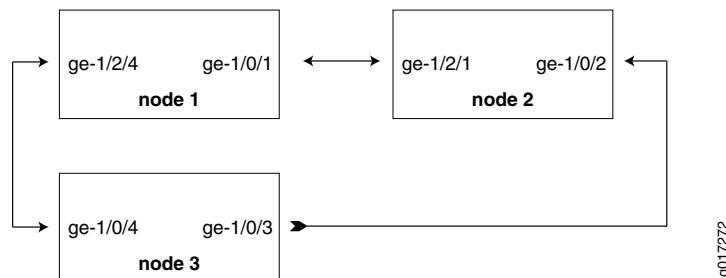
This example uses the following hardware and software components:

- Router node 1 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 2 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 3 running Junos OS with two Gigabit Ethernet interfaces.

### Ethernet Ring Overview and Topology

This section describes a configuration example for a three-node ring. The ring topology is shown in Figure 30 on page 345.

Figure 30: Example of a Three-Node Ring Topology



The configuration in this section is only for the RAPS channel. The bridge domain for user traffic is the same as the normal bridge domain. The only exception is if a bridge domain includes a ring port, then it must also include the other ring port of the same ring.

### Configuring a Three-Node Ring

To configure Ethernet Ring Protection Switching on a three-node ring, perform these tasks:

- Configuring Ethernet Ring Protection Switching on a Three-Node Ring on page 345

#### Configuring Ethernet Ring Protection Switching on a Three-Node Ring

##### Step-by-Step Procedure

##### 1. Configuring Node 1

```

interfaces {
  ge-1/0/1 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {

```

```
        encapsulation vlan-bridge;
        vlan-id 100;
    }
}
ge-1/2/4 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-bridge;
        vlan-id 100;
    }
}
bridge-domains {
    bd1 {
        domain-type bridge;
        interface ge-1/2/4.1;
        interface ge-1/0/1.1;
    }
}
protocols {
    protection-group {
        ethernet-ring pg101 {
            node-id 00:01:01:00:00:01;
            ring-protection-link-owner;
            east-interface {
                control-channel ge-1/0/1.1;
                ring-protection-link-end;
            }
            west-interface {
                control-channel ge-1/2/4.1;
            }
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                action-profile rmep-defaults {
                    default-action {
                        interface-down;
                    }
                }
            }
            maintenance-domain d1 {
                level 0;
                maintenance-association 100 {
                    mep 1 {
                        interface ge-1/0/1;
                    }
                    remote-mep 2 {
                        action-profile rmep-defaults;
                    }
                }
            }
            maintenance-domain d2 {
```

```

level 0;
maintenance-association 100 {
  mep 1 {
    interface ge-1/2/4;
    remote-mep 2 {
      action-profile rmep-defaults;
    }
  }
}
}
}
}
}
}
}
}
}
}

```

## 2. Configuring Node 2

```

interfaces {
  ge-1/0/2 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
      encapsulation vlan-bridge;
      vlan-id 100;
    }
  }
}

ge-1/2/1 {
  vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-bridge;
    vlan-id 100;
  }
}

bridge-domains {
  bd1 {
    domain-type bridge;
    interface ge-1/2/1.1;
    interface ge-1/0/2.1;
  }
}

protocols {
  protection-group {
    ethernet-ring pg102 {
      east-interface {
        control-channel ge-1/0/2.1;
      }
      west-interface {
        control-channel ge-1/2/1.1;
      }
    }
  }
}

```

```
    }  
  }  
  
  protocols {  
    oam {  
      ethernet {  
        connectivity-fault-management {  
          action-profile rmep-defaults {  
            default-action {  
              interface-down;  
            }  
          }  
        }  
        maintenance-domain d1 {  
          level 0;  
          maintenance-association 100 {  
            mep 2 {  
              interface ge-1/2/1;  
              remote-mep 1 {  
                action-profile rmep-defaults;  
              }  
            }  
          }  
        }  
        maintenance-domain d3 {  
          level 0;  
          maintenance-association 100 {  
            mep 1 {  
              interface ge-1/0/2;  
              remote-mep 2 {  
                action-profile rmep-defaults;  
              }  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

### 3. Configuring Node 3

```
interfaces {  
  ge-1/0/4 {  
    vlan-tagging;  
    encapsulation flexible-ethernet-services;  
    unit 1 {  
      encapsulation vlan-bridge;  
      vlan-id 100;  
    }  
  }  
  
  ge-1/0/3 {  
    vlan-tagging;  
    encapsulation flexible-ethernet-services;  
    unit 1 {  
      encapsulation vlan-bridge;  
    }  
  }  
}
```



```

        vlan-id 100;
    }
}

bridge-domains {
    bd1 {
        domain-type bridge;
        interface ge-1/0/4.1;
        interface ge-1/0/3.1;
    }
}

protocols {
    protection-group {
        ethernet-ring pg103 {
            east-interface {
                control-channel ge-1/0/3.1;
            }
            west-interface {
                control-channel ge-1/0/4.1;
            }
        }
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                action-profile rmep-defaults {
                    default-action {
                        interface-down;
                    }
                }
            }
            maintenance-domain d2 {
                level 0;
                maintenance-association 100 {
                    mep 2 {
                        interface ge-1/0/4;
                        remote-mep 1 {
                            action-profile rmep-defaults;
                        }
                    }
                }
            }
            maintenance-domain d3 {
                level 0;
                maintenance-association 100 {
                    mep 2 {
                        interface ge-1/0/3;
                        remote-mep 1 {
                            action-profile rmep-defaults;
                        }
                    }
                }
            }
        }
    }
}

```

```

    }
  }
}
}
}
}

```

### Examples: Ethernet RPS Output

This section provides output examples based on the configuration shown in “Example: Ethernet Ring Protection Switching Configuration” on page 345. The show commands used in these examples can help verify configuration and correct operation.

### Normal Situation—RPL Owner Node

If the ring has no failure, the **show** command will have the following output for Node 1:

```
user@node1> show protection-group ethernet-ring aps
```

Ethernet Ring Name	Request/state	No Flush	Ring Protection Link Blocked
pg101	NR	No	Yes

```
Originator Remote Node ID
Yes
```

```
user@node1> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg101
```

Interface	Control Channel	Forward State	Ring Protection Link End
ge-1/0/1	ge-1/0/1.1	discarding	Yes
ge-1/2/4	ge-1/2/4.1	forwarding	No

```
Signal Failure Admin State
Clear          IFF ready
Clear          IFF ready
```

```
user@node1> show protection-group ethernet-ring node-state
```

Ethernet ring	APS State	Event	Ring Protection Link Owner
pg101	idle	NR-RB	Yes

```
Restore Timer Quard Timer Operation state
disabled      disabled    operational
```

```
user@node1> show protection-group ethernet-ring statistics group-name pg101
```

```
Ethernet Ring statistics for PG pg101
```

```

RAPS sent           : 1
RAPS received       : 0
Local SF happened:   : 0
Remote SF happened:  : 0
NR event happened:   : 0
NR-RB event happened: : 1

```

### Normal Situation—Other Nodes

For Node 2 and Node 3, the outputs should be the same:

```
user@node2> show protection-group ethernet-ring aps
```

Ethernet Ring Name	Request/state	No Flush	Ring Protection Link Blocked
pg102	NR	No	Yes

```
Originator Remote Node ID
No          00:01:01:00:00:01
```

```
user@node2> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg102
```

```

Interface      Control Channel Forward State Ring Protection Link End
ge-1/2/1       ge-1/2/1.1      forwarding   No
ge-1/0/2       ge-1/0/2.1      forwarding   No

Signal Failure Admin State
Clear          IFF ready
Clear          IFF ready

user@node2> show protection-group ethernet-ring node-state
Ethernet ring   APS State   Event      Ring Protection Link Owner
pg102          idle       NR-RB      No

Restore Timer   Quard Timer   Operation state
disabled        disabled      operational

user@node2> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg101
RAPS sent              : 0
RAPS received          : 1
Local SF happened:      : 0
Remote SF happened:     : 0
NR event happened:      : 0
NR-RB event happened:   : 1

```

**Failure Situation—RPL Owner Node** If the ring has a link failure between Node 2 and Node 3, the **show** command will have the following outputs for Node 1:

```

user@node1> show protection-group ethernet-ring aps
Ethernet Ring Name Request/state No Flush Ring Protection Link Blocked
pg101              SF           NO      No

Originator Remote Node ID
No          00:01:02:00:00:01

user@node1> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface      Control Channel Forward State Ring Protection Link End
ge-1/0/1       ge-1/0/1.1      forwarding   Yes
ge-1/2/4       ge-1/2/4.1      forwarding   No

Signal Failure Admin State
Clear          IFF ready
Clear          IFF ready

user@node1> show protection-group ethernet-ring node-state
Ethernet ring   APS State   Event      Ring Protection Link Owner
pg101          protected SF          Yes

Restore Timer   Quard Timer   Operation state
disabled        disabled      operational

user@node1> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent              : 1
RAPS received          : 1
Local SF happened:      : 0
Remote SF happened:     : 1
NR event happened:      : 0
NR-RB event happened:   : 1

```

<b>Failure Situation—Other Nodes</b>	For Node 2 and Node 3, the outputs should be the same:
	<pre>user@node2&gt; show protection-group ethernet-ring aps Ethernet Ring Name Request/state No Flush Ring Protection Link Blocked pg102                SF                No                No  Originator Remote Node ID Yes          00:00:00:00:00:00  user@node2&gt; show protection-group ethernet-ring interface Ethernet ring port parameters for protection group pg102  Interface Control Channel Forward State Ring Protection Link End ge-1/2/1   ge-1/2/1.1         forwarding No ge-1/0/2   ge-1/0/2.1         discarding No  Signal Failure Admin State Clear          IFF ready set            IFF ready  user@node2&gt; show protection-group ethernet-ring node-state Ethernet ring APS State Event Ring Protection Link Owner pg102          idle      NR-RB No  Restore Timer Quard Timer Operation state disabled      disabled operational  user@node2&gt; show protection-group ethernet-ring statistics group-name pg102 Ethernet Ring statistics for PG pg101 RAPS sent : 1 RAPS received : 1 Local SF happened: : 1 Remote SF happened: : 0 NR event happened: : 0 NR-RB event happened: : 1</pre>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ethernet Ring Protection Switching Overview on page 339</li><li>• Understanding Ethernet Ring Protection Switching Functionality on page 340</li><li>• Configuring Ethernet Ring Protection Switching on page 344</li></ul>

## Example Ethernet Configurations

- Example: Configuring Fast Ethernet Interfaces on page 353
- Example: Configuring Gigabit Ethernet Interfaces on page 353
- Example: Configuring Aggregated Ethernet Interfaces on page 354
- Example: Configuring Aggregated Ethernet Link Protection on page 355

### Example: Configuring Fast Ethernet Interfaces

---

The following configuration is sufficient to get a Fast Ethernet interface up and running. By default, IPv4 Fast Ethernet interfaces use Ethernet version 2 encapsulation.

```
[edit]
user@host# set interfaces fe-5/2/1 unit 0 family inet address local-address
user@host# show
interfaces {
  fe-5/2/1 {
    unit 0 {
      family inet {
        address local-address;
      }
    }
  }
}
```

### Example: Configuring Gigabit Ethernet Interfaces

---

The following configuration is sufficient to get a Gigabit Ethernet, Tri-Rate Ethernet copper, or 10-Gigabit Ethernet interface up and running. By default, IPv4 Gigabit Ethernet interfaces on MX Series, M Series, and T Series routers use 802.3 encapsulation. J Series Gigabit Ethernet interfaces do not support 802.3 encapsulation.

```
[edit]
user@host# set interfaces ge-2/0/1 unit 0 family inet address local-address
user@host# show
interfaces {
  ge-2/0/1 {
    unit 0 {
      family inet {
        address local-address;
      }
    }
  }
}
```

```
    }  
  }  
}
```

The M160, M320, M120, T320, and T640 2-port Gigabit Ethernet PIC supports two independent Gigabit Ethernet links.

Each of the two interfaces on the PIC is named:

*ge-fpc/pic/[0.1]*

Each of these interfaces has functionality identical to the Gigabit Ethernet interface supported on the single-port PIC.

---

## Example: Configuring Aggregated Ethernet Interfaces

---

Aggregated Ethernet interfaces can use interfaces from different FPCs, DPCs, or PICs. The following configuration is sufficient to get an aggregated Gigabit Ethernet interface up and running.

```
[edit chassis]  
aggregated-devices {  
  ethernet {  
    device-count 15;  
  }  
}  
  
[edit interfaces]  
ge-1/3/0 {  
  gigether-options {  
    802.3ad ae0;  
  }  
}  
ge-2/0/1 {  
  gigether-options {  
    802.3ad ae0;  
  }  
}  
ae0 {  
  aggregated-ether-options {  
    link-speed 1g;  
    minimum-links 1;  
  }  
}  
vlan-tagging;  
unit 0 {  
  vlan-id 1;  
  family inet {  
    address 14.0.100.50/24;  
  }  
}  
unit 1 {  
  vlan-id 1024;  
  family inet {  
    address 14.0.101.50/24;  
  }  
}
```

```

    }
    unit 2 {
        vlan-id 1025;
        family inet {
            address 14.0.102.50/24;
        }
    }
    unit 3 {
        vlan-id 4094;
        family inet {
            address 14.0.103.50/24;
        }
    }
}

```

### Example: Configuring Aggregated Ethernet Link Protection

The following configuration enables link protection on the **ae0** interface, and specifies the **ge-1/0/0** interface as the primary link and **ge-1/0/1** as the secondary link.

```

[edit interfaces]
ae0 {
    aggregated-ether-options {
        link protection;
    }
}
[edit interfaces]
ge-1/0/0 {
    gigether-options {
        802.3ad ae0 primary;
    }
}
[edit interfaces]
ge-1/0/1 {
    gigether-options {
        802.3ad ae0 backup;
    }
}

```





## PART 3

# Ethernet Interface Configuration Statements

- Summary of Ethernet Interfaces Configuration Statements on page 359



## CHAPTER 29

# Summary of Ethernet Interfaces Configuration Statements

The following descriptions explain each of the interface configuration statements. The statements are organized alphabetically.

### 802.3ad

---

<b>Syntax</b>	<pre>802.3ad {     aex (primary   backup);     lacp {         port-priority;     } }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gletcher-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>primary</b> and <b>backup</b> options added in Junos OS Release 8.3.
<b>Description</b>	Specify aggregated Ethernet logical interface number.
<b>Options</b>	<b>aex</b> —Aggregated Ethernet logical interface number. <b>Range:</b> 0 through 15  <b>primary</b> —For link protection configurations, specify the primary link for egress traffic.  <b>backup</b> —For link protection configurations, specify the backup link for egress traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring an Aggregated Ethernet Interface on page 77</li><li>• Configuring Aggregated Ethernet Link Protection on page 100</li></ul>

## aggregate (Gigabit Ethernet CoS Policer)

---

<b>Syntax</b>	<pre>aggregate {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a policer to apply to nonpremium traffic.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Gigabit Ethernet Policers on page 265</li><li>• premium (Hierarchical Policer) on page 415</li><li>• ieee802.1p on page 379</li></ul>

## aggregated-ether-options

```
Syntax  aggregated-ether-options {
        ethernet-switch-profile {
            ethernet-policer-profile {
                input-priority-map {
                    ieee802.1p premium [ values ];
                }
                output-priority-map {
                    classifier {
                        premium {
                            forwarding-class class-name {
                                loss-priority (high | low);
                            }
                        }
                    }
                }
            }
            policer cos-policer-name {
                aggregate {
                    bandwidth-limit bps;
                    burst-size-limit bytes;
                }
                premium {
                    bandwidth-limit bps;
                    burst-size-limit bytes;
                }
            }
        }
        (mac-learn-enable | no-mac-learn-enable);
    }
    (flow-control | no-flow-control);
    lacp {
        (active | passive);
        link-protection {
            disable;
            (revertive | non-revertive);
            periodic interval;
            system-priority priority;
        }
        link-protection;
        link-speed speed;
        logical-interface-fpc-redundancy;
        (loopback | no-loopback);
        minimum-links number;
        rebalance-periodic time hour:minute <interval hours>;
        source-address-filter {
            mac-address;
            (source-filtering | no-source-filtering);
        }
    }
}
```

**Hierarchy Level** [edit interfaces aex]

**Release Information** Statement introduced before Junos OS Release 7.4.

<b>Description</b>	Configure aggregated Ethernet-specific interface properties.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ethernet Interfaces Overview on page 31</li></ul>

## auto-negotiation

<b>Syntax</b>	(auto-negotiation   no-auto-negotiation) remote-fault <local-interface-online   local-interface-offline>;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ether-options], [edit interfaces <i>interface-name</i> gige-ether-options], [edit interfaces <i>ge-pim</i> /0/0 switch-options switch-port <i>port-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 8.4 for J Series Services Routers. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	<p>For Gigabit Ethernet interfaces on M Series, MX Series, T Series, and TX Matrix routers, explicitly enable autonegotiation and remote fault. For EX Series switches and J Series Services Routers, explicitly enable autonegotiation only.</p> <ul style="list-style-type: none"> <li>• <b>auto-negotiation</b>—Enables autonegotiation. This is the default.</li> <li>• <b>no-auto-negotiation</b>—Disable autonegotiation. When autonegotiation is disabled, you must explicitly configure the link mode and speed.</li> </ul> <p>When you configure Tri-Rate Ethernet copper interfaces to operate at 1 Gbps, autonegotiation must be enabled.</p> <p>On J Series Services Routers with universal Physical Interface Modules (uPIMs), if the link speed and duplex mode are also configured, the interfaces use the values configured as the desired values in the negotiation. If autonegotiation is disabled, the link speed and link mode must be configured.</p>
<b>Default</b>	Autonegotiation is automatically enabled. No explicit action is taken after the autonegotiation is complete or if the negotiation fails.
<b>Options</b>	<p><b>remote-fault (local-interface-online   local-interface-offline)</b>—(Optional) For M Series, MX Series, T Series, and TX matrixrouters only, manually configure remote fault on an interface.</p> <p><b>Default:</b> local-interface-online</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Gigabit Ethernet Autonegotiation Overview on page 277</li> <li>• Configuring J Series Services Router Switching Interfaces on page 36</li> <li>• Configuring Gigabit Ethernet Interfaces (CLI Procedure)</li> <li>• Configuring Gigabit Ethernet Interfaces (CLI Procedure)</li> </ul>

## bandwidth-limit (Policer for Gigabit Ethernet Interfaces)

---

<b>Syntax</b>	<code>bandwidth-limit <i>bps</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <i>gigether-options</i> ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> aggregate], [edit interfaces <i>interface-name</i> <i>gigether-options</i> ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> premium]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a policer to apply to nonpremium traffic.
<b>Options</b>	<b><i>bps</i></b> —Bandwidth limit, in bits per second. Specify either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000). <b>Range:</b> 32 Kbps through 32 gigabits per second (Gbps). For IQ2 and IQ2-E interfaces 65,536 bps through 1 Gbps. For 10-Gigabit IQ2 and IQ2-E interfaces 65,536 bps through 10 Gbps.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gigabit Ethernet Policers on page 265</li><li><b>burst-size-limit (Policer for Gigabit Ethernet Interfaces)</b> on page 364</li></ul>

## burst-size-limit (Policer for Gigabit Ethernet Interfaces)

---

<b>Syntax</b>	<code>burst-size-limit <i>bytes</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <i>gigether-options</i> ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> aggregate], [edit interfaces <i>interface-name</i> <i>gigether-options</i> ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> premium]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a policer to apply to nonpremium traffic.
<b>Options</b>	<b><i>bytes</i></b> —Burst length. <b>Range:</b> 1500 through 100,000,000 bytes
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gigabit Ethernet Policers on page 265</li><li><b>bandwidth-limit (Policer for Gigabit Ethernet Interfaces)</b> on page 364</li></ul>



## classifier

---

<b>Syntax</b>	<pre> classifier {   per-unit-scheduler {     forwarding-class <i>class-name</i> {       loss-priority (high   low);     }   } } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the classifier for the output priority map to be applied to outgoing frames on this interface.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Specifying an Output Priority Map on page 267</li> <li>input-priority-map on page 382</li> </ul>

## ethernet (Protocols OAM)

```

Syntax  ethernet {
        connectivity-fault-management {
            action-profile profile-name {
                default-actions {
                    interface-down;
                }
            }
        }
        performance-monitoring {
            delegate-server-processing;
            hardware-assisted-timestamping;
            sla-iterator-profiles {
                profile-name {
                    disable;
                    calculation-weight {
                        delay delay-weight;
                        delay-variation delay-variation-weight;
                    }
                    cycle-time milliseconds;
                    iteration-period connections;
                    measurement-type (loss | statistical-frame-loss | two-way-delay);
                }
            }
        }
        linktrace {
            age (30m | 10m | 1m | 30s | 10s);
            path-database-size path-database-size;
        }
        maintenance-domain domain-name {
            level number;
            name-format (character-string | none | dns | mac+2octet);
            maintenance-association ma-name {
                short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
                continuity-check {
                    convey-loss-threshold;
                    hold-interval minutes;
                    interface-status-tlv;
                    interval (10m | 10s | 1m | 1s | 100ms);
                    loss-threshold number;
                    port-status-tlv;
                }
            }
            mep mep-id {
                auto-discovery;
                direction (up | down);
                interface interface-name (protect | working);
                lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
                    rem-err-xcon | xcon );
                priority number;
                remote-mep mep-id {
                    action-profile profile-name;
                    sla-iterator-profile profile-name {
                        data-tlv-size size;
                        iteration-count count-value;
                    }
                }
            }
        }
    }

```

367

```
    evc-map-type (all-to-one-bundling | bundling | service-multiplexing);
    evc evc-name {
        default-evc;
        vlan-list vlan-id-list;
    }
}
}
```

**Hierarchy Level** [edit protocols oam]

**Release Information** Statement introduced in Junos OS Release 8.2.

**Description** For Ethernet interfaces on M320, MX Series, and T Series routers, provide fault signaling and detection for 802.3ah Operation, Administration, and Management (OAM) support.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Enabling IEEE 802.3ah OAM Support on page 254
- Example: Configuring Connectivity Fault Management for a PBB Network on MX Series Routers

## ethernet-policer-profile

<b>Syntax</b>	<pre> ethernet-policer-profile {   input-priority-map {     ieee802.1p premium [ values ];   }   output-priority-map {     classifier {       premium {         forwarding-class class-name {           loss-priority (high   low);         }       }     }   }   policer cos-policer-name {     aggregate {       bandwidth-limit bps;       burst-size-limit bytes;     }     premium {       bandwidth-limit bps;       burst-size-limit bytes;     }   } } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile], [edit interfaces <i>interface-name</i> aggregated-ether-options ethernet-switch-profile]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ, 10-Gigabit Ethernet, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), configure a class of service (CoS)-based policer. Policing applies to the inner VLAN identifiers, not to the outer tag. For Gigabit Ethernet interfaces with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), the <b>premium</b> policer is not supported.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Gigabit Ethernet Policers on page 265</li> </ul>

## ethernet-ring

---

**Syntax**    ethernet-ring *ring-name* (  
              east-interface {  
                  control-channel *channel-name* {  
                      vlan *number*;  
                  }  
              }  
              guard-interval *number*;  
              node-id *mac-address*;  
              restore-interval *number*;  
              ring-protection-link-owner;  
              west-interface {  
                  control-channel *channel-name* {  
                      vlan *number*;  
                  }  
              }  
          })  
      }

**Hierarchy Level**    [edit protocols protection-group]

**Release Information**    Statement introduced in Junos OS Release 9.4.

**Description**    For Ethernet PICs on MX Series routers, specify the Ethernet ring in an Ethernet ring protection switching configuration.

**Options**    The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • Ethernet Ring Protection Switching Overview on page 339

## ethernet-switch-profile

```
Syntax ethernet-switch-profile {
    ethernet-policer-profile {
        input-priority-map {
            ieee802.1p premium [ values ];
        }
        output-priority-map {
            classifier {
                premium {
                    forwarding-class class-name {
                        loss-priority (high | low);
                    }
                }
            }
        }
    }
    policer cos-policer-name {
        aggregate {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        premium {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
    }
    tag-protocol-id tpid;
}
(mac-learn-enable | no-mac-learn-enable);
}
```

**Hierarchy Level** [edit interfaces *interface-name* *gigether-options*],  
[edit interfaces *interface-name* *aggregated-ether-options*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** For Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ2 and IQ2-E, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC, aggregated Ethernet with Gigabit Ethernet IQ interfaces, and the built-in Gigabit Ethernet port on the M7i router), configure VLAN tag and MAC address accounting and filtering properties.

The statements are explained separately.



**NOTE:** When you gather interfaces into a bridge domain, the `no-mac-learn-enable` statement at the [edit interfaces *interface-name* *gigether-options* *ethernet-switch-profile*] hierarchy level is not supported. You must use the `no-mac-learning` statement at the [edit bridge-domains *bridge-domain-name* *bridge-options* interface *interface-name*] hierarchy level to disable MAC learning on an interface in a bridge domain. For information on disabling MAC learning for a bridge domain, see the *MX Series Layer 2 Configuration Guide*.

<b>Default</b>	If the <b>ethernet-switch-profile</b> statement is not configured, Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router) behave like Gigabit Ethernet interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Gigabit Ethernet Policers on page 265</li><li>• Configuring MAC Address Filtering on page 269</li><li>• Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview on page 119</li></ul>

---

## fastether-options

---

<b>Syntax</b>	<pre>fastether-options {   802.3ad {     aex (primary   backup);     lacp {       port-priority;     }   }   (flow-control   no-flow-control);   ignore-l3-incompletes;   ingress-rate-limit <i>rate</i>;   (loopback   no-loopback);   mpls {     pop-all-labels {       required-depth <i>number</i>;     }   }   source-address-filter {     <i>mac-address</i>;   }   (source-filtering   no-source-filtering); }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure Fast Ethernet-specific interface properties.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ethernet Interfaces Overview on page 31</li></ul>



## flow-control

<b>Syntax</b>	(flow-control   no-flow-control);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> aggregated-ether-options], [edit interfaces <i>interface-name</i> ether-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options], [edit interfaces <i>interface-name</i> multiservice-options], [edit interfaces interface-range <i>name</i> aggregated-ether-options], [edit interfaces interface-range <i>name</i> ether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 in EX Series switches.
<b>Description</b>	For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the router or switch to the remote side of the connection. Enabling flow control is useful when the remote device is a Gigabit Ethernet switch. Flow control is not supported on the 4-port Fast Ethernet PIC.
<b>Default</b>	Flow control is enabled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Flow Control on page 41</li> <li>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</li> </ul>

## flow-control-options

---

<b>Syntax</b>	<pre>flow-control-options {   down-on-flow-control;   dump-on-flow-control;   reset-on-flow-control; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>mo-fpc/pic/port</i> multiservice-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 8.4.
<b>Description</b>	<p>Configure the flow control options for application recovery in case of a prolonged flow control failure.</p> <ul style="list-style-type: none"><li>• <b>down-on-flow-control</b>—Bring interface down during prolonged flow control.</li><li>• <b>dump-on-flow-control</b>—Cause core dump during prolonged flow control.</li><li>• <b>reset-on-flow-control</b>—Reset interface during prolonged flow control.</li></ul>
<b>Usage Guidelines</b>	See Configuring Flow Monitoring.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## forwarding-class (Gigabit Ethernet IQ Classifier)

---

<b>Syntax</b>	<pre>forwarding-class <i>class-name</i> {   loss-priority (high   low); }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> together-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier premium]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ interfaces only, define forwarding class name and option values.
<b>Options</b>	<p><b><i>class-name</i></b>—Name of forwarding class.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an Output Priority Map on page 267</li><li>• <b>input-priority-map</b> on page 382</li><li>• <b>forwarding-class</b> statement in the <a href="#">Junos OS Class of Service Configuration Guide</a></li></ul>

## forwarding-mode (100-Gigabit Ethernet)

<b>Syntax</b>	<pre>forwarding-mode {   (sa-multicast   ...the following vlan-steering statement...);   vlan-steering {     vlan-rule (high-low   odd-even);   } }</pre>
<b>Hierarchy Level</b>	[edit chassis fpc slot pic slot]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Configure the interoperation mode for 100-Gigabit Ethernet PIC.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring 100-Gigabit Ethernet PIC VLAN Steering Mode</li> <li><a href="#">sa-multicast (100-Gigabit Ethernet) on page 422</a></li> <li><a href="#">vlan-rule (100-Gigabit Ethernet) on page 446</a></li> <li><a href="#">vlan-steering (100-Gigabit Ethernet) on page 447</a></li> </ul>

## framing (10-Gigabit Ethernet Interfaces)

---

<b>Syntax</b>	framing (lan-phy   wan-phy);
<b>Hierarchy Level</b>	[edit interfaces xe- <i>fpc/pic/port</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0.
<b>Description</b>	For routers supporting the 10-Gigabit Ethernet interface, configure the framing format. WAN PHY mode is supported on MX240, MX480, MX960, T640, and T1600 routers only.
<b>Default</b>	Operates in LAN PHY mode.
<b>Options</b>	<p><b>lan-phy</b>—10GBASE-R interface framing format that bypasses the WIS sublayer to directly stream block-encoded Ethernet frames on a 10-Gigabit Ethernet serial interface.</p> <p><b>wan-phy</b>—10GBASE-W interface framing format that allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and SONET devices.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• 10-Gigabit Ethernet Framing Overview on page 299</li><li>• Configuring SONET Options for 10-Gigabit Ethernet Interfaces</li></ul>

## gigether-options

```
Syntax  gigether-options {
        802.3ad {
            aex (primary | backup);
            lacp {
                port-priority;
            }
        }
        (asynchronous-notification | no-asynchronous-notification);
        (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
        local-interface-offline>;
        (flow-control | no-flow-control);
        ignore-l3-incompletes;
        (loopback | no-loopback);
        mpls {
            pop-all-labels {
                required-depth number;
            }
        }
        no-auto-mdix
        source-address-filter {
            mac-address;
        }
        (source-filtering | no-source-filtering);
        speed
        ethernet-switch-profile {
            (mac-learn-enable | no-mac-learn-enable);
            tag-protocol-id [ tpids ];
            ethernet-policer-profile {
                input-priority-map {
                    ieee802.1p premium [ values ];
                }
                output-priority-map {
                    classifier {
                        premium {
                            forwarding-class class-name {
                                loss-priority (high | low);
                            }
                        }
                    }
                }
            }
            policer cos-policer-name {
                aggregate {
                    bandwidth-limit bps;
                    burst-size-limit bytes;
                }
                premium {
                    bandwidth-limit bps;
                    burst-size-limit bytes;
                }
            }
        }
    }
```

```
}
```

<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure Gigabit Ethernet specific interface properties.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Ethernet Interfaces Overview on page 31</li></ul>

---

## gratuitous-arp-reply

---

<b>Syntax</b>	(gratuitous-arp-reply   no-gratuitous-arp-reply);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 in EX Series switches.
<b>Description</b>	For Ethernet interfaces, enable updating of the ARP cache for replies received in response to gratuitous ARP requests.
<b>Default</b>	Updating of the ARP cache is disabled on all Ethernet interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gratuitous ARP on page 42</li><li>no-gratuitous-arp-request on page 398</li></ul>

## ieee802.1p

---

<b>Syntax</b>	ieee802.1p premium [ <i>values</i> ];
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile input-priority-map]
<b>Release Information</b>	Statement introduced before JUNOS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, configure premium priority values for IEEE 802.1p input traffic.
<b>Options</b>	<b>values</b> —Define IEEE 802.1p priority values to be treated as premium. <b>Range:</b> 0 through 7
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an Input Priority Map on page 266</li></ul>

## ignore-l3-incompletes

---

<b>Syntax</b>	ignore-l3-incompletes;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Ignore the counting of Layer 3 incomplete errors on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ignoring Layer 3 Incomplete Errors on page 41</li></ul>

## ingress-rate-limit

---

<b>Syntax</b>	<code>ingress-rate-limit rate;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> fastether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Perform port-based rate limiting on ingress traffic arriving on Fast Ethernet 8-port, 12-port, and 48-port PICs.
<b>Options</b>	<b>rate</b> —Traffic rate, in megabits per second (Mbps). <b>Range:</b> 1 through 100 Mbps
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the Ingress Rate Limit on page 44</li></ul>

## inner-tag-protocol-id

---

<b>Syntax</b>	<code>inner-tag-protocol-id tpid;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, configure the IEEE 802.1Q TPID value to rewrite for the inner tag. All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile tag-protocol-id [ <i>tpids</i> ]] hierarchy level.
<b>Default</b>	If the <b>inner-tag-protocol-id</b> statement is not configured, the TPID value is 0x8100.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Inner and Outer TPIDs and VLAN IDs on page 124</li></ul>



## inner-vlan-id

<b>Syntax</b>	<code>inner-vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map],  [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map],  [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map],  [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	<p>For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN ID to rewrite for the inner tag of the final packet.</p> <p>You cannot include the <b>inner-vlan-id</b> statement with the <b>swap</b> statement, <b>swap-push</b> statement, <b>push-push</b> statement, or <b>push-swap</b> statement and the <b>inner-vlan-id</b> statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the <b>inner-vlan-id</b> statement you include at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>] hierarchy level.</p>
<b>Options</b>	<p><i>number</i>—VLAN ID number.</p> <p><b>Range:</b> 0 through 4094</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Inner and Outer TPIDs and VLAN IDs on page 124</li> </ul>

## inner-vlan-id-range

---

<b>Syntax</b>	<code>inner-vlan-id-range start <i>start-id</i> end <i>end-id</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	The range of VLAN IDs to be used in the ATM-to-Ethernet interworking cross-connect. Specify the starting VLAN ID and ending VLAN ID.
<b>Options</b>	<b>start-id</b> —The lowest VLAN ID to be used.  <b>end-id</b> —The highest VLAN ID to be used. <b>Range:</b> 32 through 4094
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring ATM-to-Ethernet Interworking</li></ul>

## input-priority-map

---

<b>Syntax</b>	<code>input-priority-map {     ieee802.1p premium [ <i>values</i> ]; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>gigether-options</b> <b>ethernet-switch-profile</b> <b>ethernet-policer-profile</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the input policer priority map to be applied to incoming frames on this interface.  The statements are explained separately.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Specifying an Input Priority Map on page 266</li><li><b>output-priority-map</b> on page 402</li></ul>

## input-vlan-map

See the following sections:

- **input-vlan-map (Aggregated Ethernet)** on page 383
- **input-vlan-map (Gigabit Ethernet IQ and 10-Gigabit Ethernet SFPP)** on page 384

### input-vlan-map (Aggregated Ethernet)

<b>Syntax</b>	<pre>input-vlan-map {   (pop   push   swap);   tag-protocol-id <i>tpid</i>;   vlan-id <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	<p>For aggregated Ethernet interfaces using Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces only, define the rewrite profile to be applied to incoming frames on this logical interface.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Stacking a VLAN Tag on page 127</li> <li>• output-vlan-map (Aggregated Ethernet)</li> </ul>

## input-vlan-map (Gigabit Ethernet IQ and 10-Gigabit Ethernet SFPP)

<b>Syntax</b>	<pre>input-vlan-map {     (pop   pop-pop   pop-swap   push   push-push   swap   swap-push   swap-swap);     inner-tag-protocol-id <i>tpid</i>;     inner-vlan-id <i>number</i>;     tag-protocol-id <i>tpid</i>;     vlan-id <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>pop-pop</b> , <b>pop-swap</b> , <b>push-push</b> , <b>swap-push</b> , and <b>swap-swap</b> statements introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet SFPP interfaces only, define the rewrite profile to be applied to incoming frames on this logical interface.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Stacking a VLAN Tag on page 127</li><li>output-vlan-map (Gigabit Ethernet IQ and 10-Gigabit Ethernet with SFPP)</li></ul>

---

## interfaces

<b>Syntax</b>	<pre>interfaces { ... }</pre>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Physical Interface Configuration Statements Overview</li><li>Configuring Aggregated Ethernet Link Protection on page 100</li></ul>

## lacp

See the following sections:

- **lacp (802.3ad) on page 385**
- **lacp (Aggregated Ethernet) on page 386**

### lacp (802.3ad)

<b>Syntax</b>	<pre>lacp {     traceoptions {         file lacpd;         flag all;     }     ppm (centralized   distributed); }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> fastether-options 802.3ad], [edit interfaces <i>interface-name</i> gigether-options 802.3ad]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <b>ppm (centralized   distributed)</b> option introduced in Junos OS Release 9.4.
<b>Description</b>	<p>For aggregated Ethernet interfaces only, configure the Link Aggregation Control Protocol (LACP).</p> <p>On MX Series routers you can specify distributed or centralized periodic packet management (PPM).</p>
<b>Default</b>	<p>If you do not specify <b>lacp</b> as either <b>active</b> or <b>passive</b>, LACP remains passive.</p> <p>If you do not specify <b>ppm</b> as either <b>centralized</b> or <b>distributed</b>, PPM is distributed.</p>
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>active</b>—Initiate transmission of LACP packets.</li> <li>• <b>passive</b>—Respond to LACP packets.</li> <li>• <b>ppm</b>—Set PPM to centralized or distributed.</li> </ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <b>Configuring Aggregated Ethernet LACP on page 102</b></li> </ul>

## lACP (Aggregated Ethernet)

<b>Syntax</b>	<pre>lACP {     (active   passive);     admin-key <i>key</i>;     link-protection {         disable;         (revertive   non-revertive);     }     periodic <i>interval</i>;     system-id <i>mac-address</i>;     system-priority <i>priority</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces aex aggregated-ether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For aggregated Ethernet interfaces only, configure Link Aggregation Control Protocol (LACP).
<b>Default</b>	If you do not specify <b>LACP</b> as either active or passive, LACP remains passive.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>active</b>—Initiate transmission of LACP packets.</li><li>• <b>passive</b>—Respond to LACP packets.</li></ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Aggregated Ethernet LACP on page 102</li><li>• Configuring Aggregated Ethernet LACP (CLI Procedure)</li><li>• Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch</li></ul>

## link-discovery

---

<b>Syntax</b>	link-discovery (active   passive);
<b>Hierarchy Level</b>	[edit protocols oam ethernet link-fault-management interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	For Ethernet interfaces on M320, M120, MX Series, and T Series routers, specify the discovery mode used for IEEE 802.3ah Operation, Administration, and Management (OAM) support. The discovery process is triggered automatically when OAM 802.3ah functionality is enabled on a port. Link monitoring is done when the interface sends periodic OAM PDUs.
<b>Options</b>	(active   passive)—Passive or active mode. In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. In passive mode, the peer initiates the discovery process. Once the discovery process is initiated, both sides participate in discovery.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Link Discovery on page 255</li></ul>

## link-fault-management

---

**Syntax**

```
link-fault-management {  
  action-profile profile-name {  
    action {  
      link-down;  
      send-critical-event;  
      syslog;  
    }  
    event {  
      link-adjacency-loss;  
      link-event-rate {  
        frame-error count;  
        frame-period count;  
        frame-period-summary count;  
        symbol-period count;  
      }  
    }  
    protocol-down;  
  }  
}  
interface interface-name {  
  apply-action-profile profile-name;  
  link-discovery (active | passive);  
  pdu-interval interval;  
  pdu-threshold threshold-value;  
  remote-loopback;  
  event-thresholds {  
    frame-error count;  
    frame-period count;  
    frame-period-summary count;  
    symbol-period count;  
  }  
  negotiation-options {  
    allow-remote-loopback;  
    no-allow-link-events;  
  }  
}
```

**Hierarchy Level** [edit protocols oam ethernet]

**Release Information** Statement introduced in Junos OS Release 8.2.

**Description** For Ethernet interfaces on M320, M120, MX Series, and T Series routers, specify fault signaling and detection for IEEE 802.3ah Operation, Administration, and Management (OAM) support.



The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.



- Related Documentation**
- Enabling IEEE 802.3ah OAM Support on page 254

## link-mode

<b>Syntax</b>	<code>link-mode mode (automatic   full-duplex   half-duplex);</code>
<b>Hierarchy Level</b>	<code>[edit interfaces interface-name],</code> <code>[edit interfaces interface-name ether-options],</code> <code>[edit interfaces ge-pim/0/0 switch-options switch-port port-number]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Set the device's link connection characteristic.
<b>Options</b>	<p><i>mode</i>—Link characteristics:</p> <ul style="list-style-type: none"> <li>• <b>automatic</b>—Link mode is negotiated. This is the default for EX Series switches.</li> <li>• <b>full-duplex</b>—Connection is full duplex.</li> <li>• <b>half-duplex</b>—Connection is half duplex.</li> </ul> <p><b>Default:</b> Fast Ethernet interfaces, except the J Series ePIM Fast Ethernet interfaces, can operate in either full-duplex or half-duplex mode. The router's management Ethernet interface, <b>fxp0</b> or <b>em0</b>, the built-in Fast Ethernet interfaces on the FIC (M7i router), and the Gigabit Ethernet ports on J Series Services Routers with uPIMs installed and configured for access switching mode autonegotiate whether to operate in full-duplex or half-duplex mode. Unless otherwise noted here, all other interfaces operate only in full-duplex mode.</p>
	<p> <b>NOTE:</b> On J Series ePIM Fast Ethernet interfaces, if you specify half-duplex (or if full-duplex mode is not autonegotiated), the following message is written to the system log: "Half-duplex mode not supported on this PIC, forcing full-duplex mode."</p>
	<p> <b>NOTE:</b> On EX Series switches, if no-auto-negotiation is specified in <code>[edit interfaces interface-name ether-options]</code>, you can select only full-duplex or half-duplex. If auto-negotiation is specified, you can select any mode.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring the Link Characteristics on Ethernet Interfaces on page 41</li> </ul>

## link-protection

---

<b>Syntax</b>	<pre>link-protection {     disable;     (revertive  non-revertive); }</pre>
<b>Hierarchy Level</b>	<pre>[edit interfaces aex aggregated-ether-options] [edit interfaces aex aggregated-ether-options lcp]</pre>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for <b>disable</b>, <b>revertive</b>, and <b>non-revertive</b> statements added in Junos OS Release 9.3.</p>
<b>Description</b>	<p>On the router, for aggregated Ethernet interfaces only, configure link protection. In addition to enabling link protection, a primary and a secondary (backup) link must be configured to specify what links egress traffic should traverse. To configure primary and secondary links on the router, include the <b>primary</b> and <b>backup</b> statements at the <b>[edit interfaces ge-fpc/pic/port gigether-options 802.3ad aex]</b> hierarchy level or the <b>[edit interfaces fe-fpc/pic/port fastether-options 802.3ad aex]</b> hierarchy level.</p> <p>To configure those links on the switch, configure those statements at the <b>[edit interfaces ge-fpc/pic/port ether-options 802.3ad aex]</b> hierarchy level or at the <b>[edit interfaces xe-fpc/pic/port ether-options 802.3ad aex]</b> hierarchy level.</p>
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Aggregated Ethernet Link Protection on page 100</li></ul>

## link-speed (Aggregated Ethernet)

<b>Syntax</b>	link-speed <i>speed</i> ;
<b>Hierarchy Level</b>	[edit interfaces aex aggregated-ether-options], [edit interfaces interface-range <i>name</i> aggregated-ether-options], [edit interfaces interface-range <i>name</i> aggregated-sonet-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For aggregated Ethernet interfaces only, set the required link speed.
<b>Options</b>	<p><b>speed</b>—For aggregated Ethernet links, you can specify <b>speed</b> in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p>Aggregated Ethernet links on the M120 router can have one of the following speed values:</p> <ul style="list-style-type: none"> <li>• <b>100m</b>—Links are 100 Mbps.</li> <li>• <b>10g</b>—Links are 10 Gbps.</li> <li>• <b>1g</b>—Links are 1 Gbps.</li> <li>• <b>oc192</b>—Links are OC192 or STM64c.</li> </ul> <p>Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speed values:</p> <ul style="list-style-type: none"> <li>• <b>10m</b></li> <li>• <b>100m</b></li> <li>• <b>1g</b></li> <li>• <b>10g</b></li> </ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring Aggregated Ethernet Link Speed on page 109</li> <li>• Configuring Aggregated Ethernet Interfaces (CLI Procedure)</li> <li>• Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch</li> </ul>

## loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet)

---

<b>Syntax</b>	(loopback   no-loopback);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> aggregated-ether-options], [edit interfaces <i>interface-name</i> ether-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options], [edit interfaces interface-range <i>name</i> ether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, enable or disable loopback mode.



**NOTE:** By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system.


<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Ethernet Loopback Capability on page 40</li></ul>

## loss-priority

---

<b>Syntax</b>	loss-priority (high   low);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier premium forwarding-class <i>class-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the packet loss priority value.
<b>Options</b>	<b>high</b> —Packet has high loss priority. <b>low</b> —Packet has low loss priority.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Specifying an Output Priority Map on page 267</li></ul>

## mac-learn-enable

<b>Syntax</b>	(mac-learn-enable   no-mac-learn-enable);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and for Gigabit Ethernet DPCs on MX Series routers, configure whether source and destination MAC addresses are dynamically learned:</p> <ul style="list-style-type: none"> <li>• <b>mac-learn-enable</b>—Allow the interface to dynamically learn source and destination MAC addresses.</li> <li>• <b>no-mac-learn-enable</b>—Prohibit the interface from dynamically learning source and destination MAC addresses.</li> </ul> <p>MAC address learning is based on source addresses. You can start accounting for traffic after there has been traffic sent from the MAC address. Once the MAC address is learned, the frames and bytes transmitted to or received from the MAC address can be tracked.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> <b>NOTE:</b> When you gather interfaces into a bridge domain, the <b>no-mac-learn-enable</b> statement at the [edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile] hierarchy level is not supported. You must use the <b>no-mac-learning</b> statement at the [edit bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>] hierarchy level to disable MAC learning on an interface in a bridge domain. For information on disabling MAC learning for a bridge domain, see <i>MX Series Layer 2 Configuration Guide</i>.</p> </div>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring MAC Address Filtering on page 269</li> </ul>

## mep

---

**Syntax**    `mep mep-id {  
              auto-discovery;  
              direction (up | down);  
              interface interface-name (protect | working);  
              priority number;  
              remote-mep mep-id {  
                  action-profile profile-name;  
                  sla-iterator-profile profile-name {  
                      data-tlv-size size;  
                      iteration-count count-value;  
                      priority priority-value;  
                  }  
              }  
          }`

**Hierarchy Level**    `[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name  
                          maintenance-association ma-name]`

**Release Information**    Statement introduced in Junos OS Release 8.4.

**Description**    The numeric identifier of the maintenance association end point (MEP) within the maintenance association.

**Options**    **mep-id**—Specify the numeric identifier of the MEP.

**Range:** 1 through 8191

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**


- Configuring a Maintenance Endpoint on page 166
- Example: Configuring Connectivity Fault Management for a PBB Network on MX Series Routers

## minimum-links

<b>Syntax</b>	<code>minimum-links <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces aex aggregated-ether-options], [edit interfaces aex aggregated-sonet-options], [edit interfaces <i>interface-name</i> mlfr-uni-nni-bundle-options], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit interfaces interface-range <i>range</i> aggregated-ether-options], [edit interfaces interface-range <i>range</i> aggregated-sonet-options], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For aggregated Ethernet, SONET/SDH, multilink, link services, and voice services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up.
<b>Options</b>	<p><b><i>number</i></b>—Number of links.</p> <p><b>Range:</b> 1 through 8 (1 through 16 for Ethernet and SONET interfaces on the MX Series, M320, M120, T Series, or TX Matrix routers, and 1 through 12 for EX8200 switches)</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Aggregated Ethernet Minimum Links on page 110</li> <li>Configuring Aggregated SONET/SDH Minimum Links</li> <li>Configuring Aggregated Ethernet Interfaces (CLI Procedure)</li> <li>Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch</li> <li><a href="#">Junos OS Services Interfaces Configuration Guide</a></li> </ul>

## mip-half-function

---

<b>Syntax</b>	mip-half-function (none   default   explicit);
<b>Hierarchy Level</b>	[edit protocols oam ethernet connectivity-fault-managementmaintenance-domain <i>md-name</i> ], [edit protocols oam ethernet connectivity-fault-managementmaintenance-association <i>ma-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the OAM Ethernet CFM maintenance domain MIP half functions.
	<div><p><b>NOTE:</b> Whenever a MIP is configured and a bridge domain is mapped to multiple maintenance domains or maintenance associations, it is essential that the <b>mip-half-function</b> value for all maintenance domains and maintenance associations are the same.</p></div>
<b>Options</b>	<p><b>none</b>—Specify to not use the mip-half-function.</p> <p><b>default</b>—Specify to use the default mip-half-function.</p> <p><b>explicit</b>—Specify an explicit mip-half-function.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Creating the Maintenance Domain on page 161</li><li>• Example: Configuring Connectivity Fault Management for a PBB Network on MX Series Routers</li><li>• maintenance-domain</li></ul>



## mpls

<b>Syntax</b>	<pre> mpls {     pop-all-labels {         required-depth <i>number</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> atm-options], [edit interfaces <i>interface-name</i> sonet-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For passive monitoring on ATM and SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode, process incoming IP packets that have MPLS labels.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Removing MPLS Labels from Incoming Packets</li> <li>Removing MPLS Labels from Incoming Packet</li> <li><a href="#">Junos OS Services Interfaces Configuration Guide</a></li> </ul>

## no-auto-mdix

<b>Syntax</b>	no-auto-mdix;
<b>Hierarchy Level</b>	[edit interface ge- <i>fpc/port/pic</i> gigether-options]
<b>Description</b>	<p>On MX Series routers, disable the Auto MDI/MDIX feature.</p> <p>MX Series routers with Gigabit Ethernet interfaces automatically detect MDI and MDIX port connections. Use this statement to override the default setting. Remove this statement to return to the default setting.</p>
<b>Default</b>	Auto MDI/MDIX is enabled by default.
<b>Options</b>	There are no options for this statement.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Ethernet Interfaces Overview on page 31</li> <li><a href="#">gigether-options on page 377.</a></li> </ul>

## no-gratuitous-arp-request

---

<b>Syntax</b>	no-gratuitous-arp-request;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6 for EX Series switches.
<b>Description</b>	For Ethernet interfaces, do not respond to gratuitous ARP requests.
<b>Default</b>	Gratuitous ARP responses are enabled on all Ethernet interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Gratuitous ARP on page 42</a></li><li>• <a href="#">gratuitous-arp-reply on page 378</a></li></ul>

## oam

```

Syntax  oam {
        ethernet {
            connectivity-fault-management {
                action-profile profile-name {
                    default-actions {
                        interface-down;
                    }
                }
            }
            performance-monitoring {
                delegate-server-processing;
                hardware-assisted-timestamping;
                sla-iterator-profiles {
                    profile-name {
                        disable;
                        calculation-weight {
                            delay delay-weight;
                            delay-variation delay-variation-weight;
                        }
                        cycle-time milliseconds;
                        iteration-period connections;
                        measurement-type (loss | statistical-frame-loss | two-way-delay);
                    }
                }
            }
            linktrace {
                age (30m | 10m | 1m | 30s | 10s);
                path-database-size path-database-size;
            }
            maintenance-domain domain-name {
                level number;
                name-format (character-string | none | dns | mac+2octet);
                maintenance-association ma-name {
                    short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
                    continuity-check {
                        convey-loss-threshold;
                        hold-interval minutes;
                        interface-status-tlv;
                        interval (10m | 10s | 1m | 1s | 100ms);
                        loss-threshold number;
                        port-status-tlv;
                    }
                }
                mep mep-id {
                    auto-discovery;
                    direction (up | down);
                    interface interface-name (protect | working);
                    lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
                        rem-err-xcon | xcon );
                    priority number;
                    remote-mep mep-id {
                        action-profile profile-name;
                        sla-iterator-profile profile-name {
                            data-tlv-size size;
                        }
                    }
                }
            }
        }
    }

```

```

        iteration-count count-value;
        priority priority-value;
    }
}
}
}
}
link-fault-management {
    action-profile profile-name {
        action {
            link-down;
            send-critical-event;
            syslog;
        }
        event {
            link-adjacency-loss;
            link-event-rate {
                frame-error count;
                frame-period count;
                frame-period-summary count;
                symbol-period count;
            }
            protocol-down;
        }
    }
}
interface interface-name {
    apply-action-profile
    link-discovery (active | passive);
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
    negotiation-options {
        allow-remote-loopback;
        no-allow-link-events;
    }
}
}
}
}
}

```

**Hierarchy Level** [edit protocols]

**Release Information** Statement introduced in Junos OS Release 8.2.

**Description** For Ethernet interfaces on M320, M120, MX Series, and T Series routers, provide IEEE 802.3ah Operation, Administration, and Management (OAM) support.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>IEEE 802.3ah OAM Link-Fault Management Overview on page 253</li> </ul>

## optics-options

---

<b>Syntax</b>	<pre> optics-options {     alarm low-light-alarm {         (link-down   syslog);     }     warning low-light-warning {         (link-down   syslog);     }     wavelength nm; } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>alarm</b> option and <b>warning</b> options introduced in Junos OS Release 10.0.
<b>Description</b>	For 10-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces only, configure full C-band International Telecommunication Union (ITU)-Grid tunable optics.
<b>Options</b>	The <b>alarm</b> and <b>warning</b> and <b>wavelength</b> statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>10-Gigabit Ethernet DWDM Interface Wavelength Overview on page 297</li> </ul>

## output-priority-map

---

<b>Syntax</b>	<pre>output-priority-map {   classifier {     premium {       forwarding-class <i>class-name</i> {         loss-priority (high   low);       }     }   } }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>gigether-options ethernet-switch-profile ethernet-policer-profile</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the output policer priority map to be applied to outgoing frames on this interface.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an Output Priority Map on page 267</li><li>• <a href="#">input-priority-map</a> on page 382</li></ul>

## pdu-interval

---

<b>Syntax</b>	<pre>pdu-interval <i>interval</i>;</pre>
<b>Hierarchy Level</b>	[edit protocols <b>oam ethernet link-fault-management</b> interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	<p>For Ethernet interfaces on M320, M120, MX Series, and T Series routers, specify the periodic OAM PDU sending interval for fault detection. Used for IEEE 802.3ah Operation, Administration, and Management (OAM) support.</p>
<b>Options</b>	<p><b>interval</b>—Periodic OAM PDU sending interval.</p> <p><b>Range:</b> 100 through 1000 milliseconds</p> <p><b>Default:</b> 1000 milliseconds</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring the OAM PDU Interval on page 255</li></ul>

## pdu-threshold

---

<b>Syntax</b>	<code>pdu-threshold <i>threshold-value</i>;</code>
<b>Hierarchy Level</b>	<code>[edit protocols oam ethernet link-fault-management interface <i>interface-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	For Ethernet interfaces on M320, M120, MX Series, and T Series routers, specify the number of OAM PDUs to miss before an error is logged. Used for IEEE 802.3ah Operation, Administration, and Management (OAM) support.
<b>Options</b>	<b><i>threshold-value</i></b> —The number of PDUs missed before declaring the peer lost. <b>Range:</b> 3 through 10 PDUs <b>Default:</b> 3 PDUs
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the OAM PDU Threshold on page 255</li></ul>

## periodic

---

<b>Syntax</b>	<code>periodic interval;</code>
<b>Hierarchy Level</b>	[edit interfaces aex <b>aggregated-ether-options</b> lacp], [edit interfaces interface-range <i>name</i> <b>aggregated-ether-options</b> lacp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For aggregated Ethernet interfaces only, configure the interval for periodic transmission of LACP packets.
<b>Options</b>	<i>interval</i> —Interval for periodic transmission of LACP packets. <ul style="list-style-type: none"><li>• <b>fast</b>—Transmit packets every second.</li><li>• <b>slow</b>—Transmit packets every 30 seconds.</li></ul> <b>Default:</b> <b>fast</b>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Aggregated Ethernet LACP on page 102</li><li>• Configuring Aggregated Ethernet LACP (CLI Procedure)</li><li>• Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch</li></ul>



## policer

---

See the following sections:

- [policer \(CFM Firewall\) on page 405](#)
- [policer \(CFM Global\) on page 406](#)
- [policer \(CFM Session\) on page 407](#)
- [policer \(CoS\) on page 408](#)
- [policer \(MAC\) on page 409](#)

### policer (CFM Firewall)

<b>Syntax</b>	<pre> policer <i>cfm-policer</i> {     if-exceeding {         bandwidth-limit 8k;         burst-size-limit 2k;     }     then discard; } </pre>
<b>Hierarchy Level</b>	[edit firewall]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Attach an explicit policer to CFM sessions.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Rate Limiting of Ethernet OAM Messages on page 196</a></li> <li>• <a href="#">policer (CFM Global) on page 406</a></li> <li>• <a href="#">policer (CFM Session) on page 407</a></li> </ul>

## policer (CFM Global)

<b>Syntax</b>	<pre>policer {     all <i>cfm-policer-name</i>;     continuity-check <i>cfm-policer-name</i>;     other <i>cfm-policer-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit protocols oam ethernet connectivity-fault-management]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a policer at the global level to police the CFM traffic belonging to all sessions.
<b>Options</b>	<p><b>continuity-check <i>cfm-policer-name</i></b>—Police all continuity check packets with the policer specified.</p> <p><b>other <i>cfm-policer-name</i></b>—Police all non-continuity check packets with the policer specified.</p> <p><b>all <i>cfm-policer-name</i></b>—Police all CFM packets with policer specified. If the <b>all</b> option is used, then you cannot specify above two options.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Rate Limiting of Ethernet OAM Messages on page 196</li><li><b>policer (CFM Session)</b> on page 407</li></ul>


## policer (CFM Session)

<b>Syntax</b>	<pre>policer {   all <i>cfm-policer-name</i>;   continuity-check <i>cfm-policer-name</i>;   other <i>cfm-policer-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>name</i> level <i>number</i> maintenance-association <i>name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a separate policer to rate-limit packets specific to that session.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>continuity-check <i>cfm-policer-name</i></b>—Police continuity check packets belonging to this session.</li><li>• <b>other <i>cfm-policer-name</i></b>—Police all non-continuity check packets belonging to this session.</li><li>• <b>all <i>cfm-policer-name</i></b>—Police all CFM packets belonging to this session. If the <b>all</b> option is used, then you cannot specify the above two options.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Rate Limiting of Ethernet OAM Messages on page 196</li><li>• <b>policer (CFM Global)</b> on page 406</li></ul>

## policer (CoS)

<b>Syntax</b>	<pre>policer <i>cos-policer-name</i> {   aggregate {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>;   }   premium {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <i>gigether-options</i> ethernet-switch-profile ethernet-policer-profile]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), define a CoS policer template to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits. For Gigabit Ethernet interfaces with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), the premium policer is not supported.
<b>Options</b>	<p><i>cos-policer-name</i>—Name of one policer to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gigabit Ethernet Policers on page 265</li></ul>

**policer (MAC)**

<b>Syntax</b>	<pre> policer {   input <i>cos-policer-name</i>;   output <i>cos-policer-name</i>; } </pre>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> accept-source-mac mac-address <i>mac-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> accept-source-mac mac-address <i>mac-address</i>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), configure MAC policing.
<div>  <p><b>NOTE:</b></p> <p>On MX Series routers with Gigabit Ethernet or Fast Ethernet PICs, the following considerations apply:</p> <ul style="list-style-type: none"> <li>• Interface counters do not count the 7-byte preamble and 1-byte frame delimiter in Ethernet frames.</li> <li>• In MAC statistics, the frame size includes MAC header and CRC before any VLAN rewrite/imposition rules are applied.</li> <li>• In traffic statistics, the frame size encompasses the L2 header without CRC after any VLAN rewrite/imposition rule.</li> </ul> </div>	
<b>Options</b>	<p><b>input <i>cos-policer-name</i></b>—Name of one policer to specify the premium bandwidth and aggregate bandwidth.</p> <p><b>output <i>cos-policer-name</i></b>—Name of one policer to specify the premium bandwidth and aggregate bandwidth.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring MAC Address Filtering on page 269</li> </ul>

## pop

---

<b>Syntax</b>	<code>pop;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and aggregated Ethernet interfaces using Gigabit Ethernet IQ interfaces, specify the VLAN rewrite operation to remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Removing a VLAN Tag on page 128</li></ul>

## pop-pop

---

<b>Syntax</b>	<code>pop-pop;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN rewrite operation to remove both the outer and inner VLAN tags of the frame.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Removing the Outer and Inner VLAN Tags on page 128</li></ul>

## pop-swap

<b>Syntax</b>	pop-swap;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2, and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN rewrite operation to remove the outer VLAN tag of the frame, and replace the inner VLAN tag of the frame with a user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag on page 129</li> </ul>

## port-status-tlv

<b>Syntax</b>	port-status-tlv blocked;
<b>Hierarchy Level</b>	[edit protocols oam ethernet connectivity-fault-management action-profile <i>tlv-action</i> event]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define an <b>action-profile</b> consisting of various events and the action. Based on values of <b>port-status-tlv</b> in the received CCM packets, specific action such as <i>interface-down</i> can be taken using action-profile options.
<b>Options</b>	blocked—When the incoming CCM packet contains port status TLV with value blocked, the action will be triggered for this action-profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Connectivity Fault Management Action Profile on page 170</li> <li>Configuring Remote MEP Action Profile Support on page 190</li> </ul>

## ppp-options

---

<b>Syntax</b>	<pre>ppp-options {   chap {     access-profile <i>name</i>;     default-chap-secret <i>name</i>;     local-name <i>name</i>;     passive;   }   compression {     acfc;     pfc;   }   dynamic-profile <i>profile-name</i>;   lcp-max-conf-req <i>number</i>   lcp-restart-timer <i>milliseconds</i>;   loopback-clear-timer <i>seconds</i>;   ncp-max-conf-req <i>number</i>   ncp-restart-timer <i>milliseconds</i>;   pap {     access-profile <i>name</i>;     default-pap-password <i>password</i>;     local-name <i>name</i>;     local-password <i>password</i>;     passive;   } }</pre>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</p>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4. lcp-restart-timer statement introduced in Junos OS Release 8.1. ncp-restart-timer statement introduced in Junos OS Release 8.1. loopback-clear-timer statement introduced in Junos OS Release 8.5. dynamic-profile statement introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>On interfaces with PPP encapsulation, configure PPP-specific interface properties.</p> <p>For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:</p> <ul style="list-style-type: none"><li>• <b>atm-ppp-llc</b>—PPP over AAL5 LLC encapsulation.</li><li>• <b>atm-ppp-vc-mux</b>—PPP over AAL5 multiplex encapsulation.</li></ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>



- Related Documentation**
- Configuring the PPP Challenge Handshake Authentication Protocol

## pppoe-options

---

<b>Syntax</b>	<pre>pppoe-options {     access-concentrator <i>name</i>;     auto-reconnect <i>seconds</i>;     (client   server);     service-name <i>name</i>;     underlying-interface <i>interface-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces pp0 unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces pp0 unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>client</b> Statement introduced in Junos OS Release 8.5. <b>server</b> Statement introduced in Junos OS Release 8.5.
<b>Description</b>	<p>For J Series Services Routers, M120 Multiservice Edge Routers, M320 Multiservice Edge Service Routers, and MX Series Universal Edge Routers with PPP over Ethernet interfaces, configure PPP over Ethernet-specific interface properties.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring a PPPoE Interface on page 317</li></ul>

## pppoe-underlying-options (Static and Dynamic Subscribers)

---

<b>Syntax</b>	<pre>pppoe-underlying-options {     access-concentrator <i>name</i>;     dynamic-profile <i>profile-name</i>;     duplicate-protection;     max-sessions <i>number</i>;     service-name-table <i>table-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Configure PPPoE-specific interface properties for the underlying interface on which the router creates a static or dynamic PPPoE logical interface. The underlying interface must be configured with PPPoE (<b>ppp-over-ether</b>) encapsulation.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring PPPoE on page 315 (for static interfaces)</li><li>• Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces</li><li>• Assigning a Service Name Table to a PPPoE Underlying Interface on page 331</li></ul>

## premium

See the following sections:

- [premium \(Hierarchical Policer\) on page 415](#)
- [premium \(Output Priority Map\) on page 416](#)
- [premium \(Policer\) on page 416](#)

### premium (Hierarchical Policer)

**Syntax**

```
premium {
  if-exceeding {
    bandwidth-limit bandwidth;
    burst-size-limit burst;
  }
  then {
    discard;
  }
}
```

**Hierarchy Level** [edit firewall hierarchical-policer]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, specify a premium level for a hierarchical policer.

**Options** Options are described separately.

**Required Privilege Level** firewall—To view this statement in the configuration.  
firewall-control—To add this statement to the configuration.

**Related Documentation**

- Applying Policers
- [Junos OS Class of Service Configuration Guide](#)

## premium (Output Priority Map)

<b>Syntax</b>	<pre>premium {     forwarding-class <i>class-name</i> {         loss-priority (high   low);     } }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ interfaces only, define the classifier for egress premium traffic.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an Output Priority Map on page 267</li><li>• input-priority-map on page 382</li></ul>

## premium (Policer)

<b>Syntax</b>	<pre>premium {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile ethernet-policer-profile policer <i>cos-policer-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a policer to apply to nonpremium traffic.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Gigabit Ethernet Policers on page 265</li><li>• aggregate (Gigabit Ethernet CoS Policer) on page 360</li><li>• ieee802.1p on page 379</li></ul>

## protection-group

**Syntax**

```

protection-group {
  ethernet-ring ring-name (
    node-id mac-address;
    ring-protection-link-owner;
    east-interface {
      control-channel channel-name {
        ring-protection-link-end;
      }
    }
    west-interface {
      node-id mac-address;
      control-channel channel-name {
        ring-protection-link-end;
      }
    }
    data-channel {
      vlan number;
    }
    guard-interval number;
    restore-interval number;
  }
}

```

**Hierarchy Level** [edit protocols]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Configure Ethernet ring protection switching.

The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Ring Protection Switching Overview on page 339
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers

## protocol-down

---

<b>Syntax</b>	protocol-down;
<b>Hierarchy Level</b>	[edit protocols oam ethernet link-fault-management action-profile event]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Upper layer indication of protocol down event. When the <b>protocol-down</b> statement is included, the protocol down event triggers the action specified under the <b>action</b> statement.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring an OAM Action Profile on page 256</li></ul>

## push

---

<b>Syntax</b>	push;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and aggregated Ethernet interfaces using Gigabit Ethernet IQ interfaces, specify the VLAN rewrite operation to add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag. If you include the <b>push</b> statement in the configuration, you must also include the <b>pop</b> statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Stacking a VLAN Tag on page 127</li></ul>

## push-push

<b>Syntax</b>	push-push;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN rewrite operation to push two VLAN tags in front of the frame.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Stacking Two VLAN Tags on page 129</li> </ul>

## remote-mep

---

<b>Syntax</b>	<pre>remote-mep <i>mep-id</i> {     action-profile <i>profile-name</i>;     sla-iterator-profile <i>profile-name</i> {         data-tlv-size <i>size</i>;         iteration-count <i>count-value</i>;         priority <i>priority-value</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit protocols oam ethernet connectivity-fault-management maintenance-domain <i>md-name</i> maintenance-association <i>ma-name</i> mep <i>mep-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the numeric identifier of the remote maintenance association end point (MEP) within the maintenance association.
<b>Options</b>	<p><b>mep-id</b>—Numeric identifier of the MEP.</p> <p><b>Range:</b> 1 through 8191</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	Configure—To enter configuration mode. Control—To modify any configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Maintenance Endpoint on page 166</li></ul>

## request

---

<b>Syntax</b>	<pre>request (protect   working);</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> sonet-options aps]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.
<b>Options</b>	<p><b>protect</b>—Request that the circuit become the protect circuit.</p> <p><b>working</b>—Request that the circuit become the working circuit.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Switching Between the Working and Protect Circuits</li><li>force</li></ul>



## ring-protection-link-end

---

<b>Syntax</b>	ring-protection-link-end;
<b>Hierarchy Level</b>	[edit protocols <b>protection-group ethernet-ring</b> <i>ring-name</i> (east-interface   west-interface)]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	For MS Series routers, specify that the port is one side of a ring protection link (RPL) by setting the RPL end flag.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ethernet Ring Protection Switching Overview on page 339</li></ul>

## ring-protection-link-owner

---

<b>Syntax</b>	ring-protection-link-owner;
<b>Hierarchy Level</b>	[edit protocols <b>protection-group ethernet-ring</b> <i>ring-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	For MS Series routers, specify the ring protection link (RPL) owner flag in the Ethernet protection ring. Include this statement only once for each ring (only one node can function as the RPL owner).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Ethernet Ring Protection Switching Overview on page 339</li></ul>

## sa-multicast (100-Gigabit Ethernet)

---

<b>Syntax</b>	sa-multicast;
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot</i> pic <i>slot</i> forwarding-mode]
<b>Description</b>	<p>Configure the 100-Gigabit Ethernet PIC to interoperate with other Juniper Networks 100-Gigabit Ethernet PICs.</p> <p>See <b>vlan-steering</b> for information on interoperability with 100 gigabit Ethernet interfaces from other vendors.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring 100-Gigabit Ethernet PIC VLAN Steering Mode</li><li>• <b>forwarding-mode (100-Gigabit Ethernet)</b> on page 375</li><li>• <b>vlan-steering (100-Gigabit Ethernet)</b> on page 447</li></ul>

## source-address-filter

<b>Syntax</b>	source-address-filter { <i>mac-address</i> ; }
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> aggregated-ether-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, Gigabit Ethernet IQ interfaces, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), specify the MAC addresses from which the interface can receive packets. For this statement to have any effect, you must include the <b>source-filtering</b> statement in the configuration to enable source address filtering. This statement is not supported on the J Series Services Routers.
<b>Options</b>	<p><b>mac-address</b>—MAC address filter. You can specify the MAC address as <i>nn:nn:nn:nn:nn:nn</i> or <i>nnnn.nnnn.nnnn</i>, where <i>n</i> is a decimal digit. To specify more than one address, include multiple <b>mac-address</b> options in the <b>source-address-filter</b> statement.</p> <p>If you enable the VRRP on a Fast Ethernet or Gigabit Ethernet interface, as described in “VRRP and VRRP for IPv6 Overview” on page 261, and if you enable MAC source address filtering on the interface, you must include the virtual MAC address in the list of source MAC addresses that you specify in the <b>source-address-filter</b> statement. MAC addresses ranging from <b>00:00:5e:00:01:00</b> through <b>00:00:5e:00:01:ff</b> are reserved for VRRP, as defined in RFC 3768, <i>Virtual Router Redundancy Protocol</i>. When you configure the VRRP group, the group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.</p> <p>On untagged Gigabit Ethernet interfaces you should not configure the <b>source-address-filter</b> statement and the <b>accept-source-mac</b> statement simultaneously. On tagged Gigabit Ethernet interfaces you should not configure the <b>source-address-filter</b> statement and the <b>accept-source-mac</b> statement with an identical MAC address specified in both filters.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling Ethernet MAC Address Filtering on page 38</li> <li><b>source-filtering</b> on page 424</li> </ul>

## source-filtering

---

<b>Syntax</b>	(source-filtering   no-source-filtering);
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> aggregated-ether-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gigether-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and Gigabit Ethernet IQ interfaces only, enable the filtering of MAC source addresses, which blocks all incoming packets to that interface. To allow the interface to receive packets from specific MAC addresses, include the <b>source-address-filter</b> statement.</p> <p>If the remote Ethernet card is changed, the interface is no longer able to receive packets from the new card because it has a different MAC address.</p>
<b>Default</b>	Source address filtering is disabled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Enabling Ethernet MAC Address Filtering on page 38</li><li>• accept-source-mac</li><li>• <b>source-address-filter</b> on page 423</li></ul>

## speed


See the following sections:

- **speed (Ethernet) on page 425**
- **speed (MX Series DPC) on page 426**

### speed (Ethernet)

<b>Syntax</b>	<code>speed (10m   100m   1g   auto);</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ], [edit interfaces <i>ge-pim</i> /0/0 <b>switch-options</b> <b>switch-port</b> <i>port-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface speed. This statement applies to the management Ethernet interface ( <b>fxp0</b> or <b>em0</b> ), Fast Ethernet 12-port and 48-port PICs, the built-in Fast Ethernet port on the FIC (M7i router), the built-in Ethernet interfaces on J Series Services Routers, Combo Line Rate DPCs and Tri-Rate Ethernet Copper interfaces on MX Series routers, and on the Gigabit Ethernet ports on J Series Services Routers with uPIMs installed and configured for access switching mode. When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled. When you configure 100BASE-FX SFP, you must set the port speed at 100 Mbps.
<b>Options</b>	You can specify the speed as either <b>10m</b> (10 Mbps), <b>100m</b> (100 Mbps), or on J Series routers with uPIMs installed and on MX Series routers, <b>1g</b> (1 Gbps). You can specify the <b>auto</b> option only on MX Series routers.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring the Interface Speed</li> <li>• Configuring the Interface Speed on Ethernet Interfaces on page 44</li> <li>• Configuring Gigabit Ethernet Autonegotiation on page 277</li> <li>• Configuring J Series Services Router Switching Interfaces on page 36</li> </ul>

## speed (MX Series DPC)

<b>Syntax</b>	<code>speed (auto   1Gbps   100Mbps   10Mbps);</code>
<b>Hierarchy Level</b>	[edit interfaces <i>ge-fpc/pic/port</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>On MX Series routers with Combo Line Rate DPCs and Tri-Rate Copper SFPs you can set auto negotiation of speed. To specify the auto negotiation speed, use the <b>speed (auto   1Gbps   100Mbps   10Mbps)</b> statement under the [edit interface <i>ge-/fpc/pic/port</i>] hierarchy level. The <b>auto</b> option will attempt to automatically match the rate of the connected interface. To set port speed negotiation to a specific rate, set the port speed to <b>1Gbps</b>, <b>100Mbps</b>, or <b>10Mbps</b>.</p>
	<div><p><b>NOTE:</b> If the negotiated speed and the interface speed do not match, the link will not be brought up. Half duplex mode is not supported.</p></div>
<b>Options</b>	You can specify the speed as either <b>auto</b> (autonegotiate), <b>10Mbps</b> (10 Mbps), <b>100Mbps</b> (100 Mbps), or <b>1Gbps</b> (1 Gbps).
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Gigabit Ethernet Autonegotiation on page 277</a></li><li>• <a href="#">no-auto-mdix on page 397</a></li></ul>

## swap

<b>Syntax</b>	swap;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and aggregated Ethernet using Gigabit Ethernet IQ interfaces, specify the VLAN rewrite operation to replace a VLAN tag. The outer VLAN tag of the frame is overwritten with the user-specified VLAN tag information.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Rewriting the VLAN Tag on Tagged Frames on page 130</li> </ul>

## swap-push

<b>Syntax</b>	swap-push;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN rewrite operation to replace the outer VLAN tag of the frame with a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Rewriting a VLAN Tag and Adding a New Tag on page 133</li> </ul>

## swap-swap

---

<b>Syntax</b>	swap-swap;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, specify the VLAN rewrite operation to replace both the inner and the outer VLAN tags of the frame with a user-specified VLAN tag value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Rewriting the Inner and Outer VLAN Tags on page 134</li></ul>

## switch-options

---

<b>Syntax</b>	switch-options { switch-port <i>port-number</i> { (auto-negotiation   no-auto-negotiation); speed (10m   100m   1g); link-mode (full-duplex   half-duplex); } }
<b>Hierarchy Level</b>	[edit interfaces <i>ge-pim</i> /0/0]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	On a J Series Services Router with multiport Gigabit Ethernet uPIMs installed and operating in access switching mode, only one physical interface is configured for the entire multiport Gigabit Ethernet uPIM. Configuration of the physical port characteristics is done under the single physical interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring J Series Services Router Switching Interfaces on page 36</li></ul>



## switch-port

<b>Syntax</b>	<pre>switch-port <i>port-number</i> {     (auto-negotiation   no-auto-negotiation);     speed (10m   100m   1g);     link-mode (full-duplex   half-duplex); }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>ge-pim</i> /0/0 <b>switch-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	On a J Series Services Router with Ethernet uPIMs installed and operating in access switching mode, configuration of the physical port characteristics, done under the single physical interface.
<b>Default</b>	Autonegotiation is enabled by default. If the link speed and duplex are also configured, the interfaces use the values configured as the desired values in the negotiation.
<b>Options</b>	<p><b><i>port-number</i></b>—Ports are numbered 0 through 5 on the 6-port Gigabit Ethernet uPIM, 0 through 7 on the 8-port Gigabit Ethernet uPIM, and 0 through 15 on the 16-port Gigabit Ethernet uPIM.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring J Series Services Router Switching Interfaces on page 36</li> </ul>

## tag-protocol-id

---

See the following sections:

- [tag-protocol-id \(TPIDs Expected to Be Sent or Received\)](#) on page 430
- [tag-protocol-id \(TPID to Rewrite\)](#) on page 431

### tag-protocol-id (TPIDs Expected to Be Sent or Received)

<b>Syntax</b>	<code>tag-protocol-id [ <i>tpids</i> ];</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <i>gether-options</i> ethernet-switch-profile], [edit interfaces <i>interface-name</i> <i>aggregated-ether-options</i> ethernet-switch-profile]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, aggregated Ethernet with Gigabit Ethernet IQ interfaces, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC, and the built-in Gigabit Ethernet port on the M7i router), define the TPIDs expected to be sent or received on a particular VLAN. For each Gigabit Ethernet port, you can configure up to eight TPIDs using the <b>tag-protocol-id</b> statement; but only the first four TPIDs are supported on IQ2 and IQ2-E interfaces.</p> <p>For 10-Gigabit Ethernet LAN/WAN PIC interfaces on T Series routers, only the default TPID value (0x8100) is supported.</p>
<b>Options</b>	<i>tpids</i> —TPIDs to be accepted on the VLAN. Specify TPIDs in hexadecimal.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames</a> on page 123</li></ul>

**tag-protocol-id (TPID to Rewrite)**

<b>Syntax</b>	<code>tag-protocol-id <i>tpid</i>;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces only, configure the outer TPID value. All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces <i>interface-name</i> <b>gether-options ethernet-switch-profile tag-protocol-id [ <i>tpids</i> ]</b>] hierarchy level.</p> <p>For 10-Gigabit Ethernet LAN/WAN PIC interfaces on T Series routers, value the default TPID value (0x8100) is supported.</p>
<b>Default</b>	If the <b>tag-protocol-id</b> statement is not configured, the TPID value is 0x8100.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Inner and Outer TPIDs and VLAN IDs on page 124</li> </ul>

## unit

```

Syntax  unit logical-unit-number {
            accept-source-mac {
                mac-address mac-address {
                    policer {
                        input cos-policer-name;
                        output cos-policer-name;
                    }
                }
            }
            accounting-profile name;
            allow-any-vci;
            atm-scheduler-map (map-name | default);
            backup-options {
                interface interface-name;
            }
            bandwidth rate;
            cell-bundle-size cells;
            clear-dont-fragment-bit;
            compression {
                rtp {
                    maximum-contexts number <force>;
                    f-max-period number;
                    queues [ queue-numbers ];
                    port {
                        minimum port-number;
                        maximum port-number;
                    }
                }
            }
            compression-device interface-name;
            copy-tos-to-outer-ip-header;
            demux-destination family;
            demux-source family;
            demux-options {
                underlying-interface interface-name;
            }
            description text;
            dial-options {
                l2tp-interface-id name;
                (dedicated | shared);
            }
            dialer-options {
                activation-delay seconds;
                callback;
                callback-wait-period time;
                deactivation-delay seconds;
                dial-string [ dial-string-numbers ];
                idle-timeout seconds;
                incoming-map {
                    caller caller-id) | accept-all;
                    initial-route-check seconds;
                    load-interval seconds;
                }
            }
        }

```

```

    load-threshold percent;
    pool pool-name;
    redial-delay time;
    watch-list {
        [ routes ];
    }
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold cells plp1 cells;
family family-name {
    ... the family subhierarchy appears after the main [edit interfaces interface-name unit
        logical-unit-number] hierarchy ...
}
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap |
    swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
interleave-fragments;
inverse-arp;
layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
}
link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
    up-count cells;
    down-count cells;
}
oam-period (disable | seconds);
output-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap |
    swap-push | swap-swap);
    inner-tag-protocol-id tpid;

```

```
    inner-vlan-id number;  
    tag-protocol-id tpid;  
    vlan-id number;  
}  
passive-monitor-mode;  
peer-unit unit-number;  
plp-to-clp;  
point-to-point;  
ppp-options {  
    chap {  
        access-profile name;  
        default-chap-secret name;  
        local-name name;  
        passive;  
    }  
    compression {  
        acfc;  
        pfc;  
    }  
    dynamic-profile profile-name;  
    lcp-restart-timer milliseconds;  
    loopback-clear-timer seconds;  
    ncp-restart-timer milliseconds;  
    pap {  
        access-profile name;  
        default-pap-password password;  
        local-name name;  
        local-password password;  
        passive;  
    }  
}  
pppoe-options {  
    access-concentrator name;  
    auto-reconnect seconds;  
    (client | server);  
    service-name name;  
    underlying-interface interface-name;  
}  
pppoe-underlying-options {  
    access-concentrator name;  
    dynamic-profile profile-name;  
    max-sessions number;  
}  
proxy-arp;  
service-domain (inside | outside);  
shaping {  
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst  
    length);  
    queue-length number;  
}  
short-sequence;  
targeted-distribution;  
transmit-weight number;  
(traps | no-traps);  
trunk-bandwidth rate;  
trunk-id number;
```

```

tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
vci vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
    access-concentrator name;
    address address {
        ... the address subhierarchy appears after the main [edit interfaces interface-name unit
            logical-unit-number family family-name] hierarchy ...
    }
    bridge-domain-type (bvlan | svlan);
    bundle interface-name;
    core-facing;
    demux-destination {
        destination-prefix;
    }
    demux-source {
        source-prefix;
    }
    duplicate-protection;
    dynamic-profile profile-name;
    filter {
        group filter-group-number;
        input filter-name;
        input-list [ filter-names ];
        output filter-name;
        output-list [ filter-names ];
    }
    interface-mode (access | trunk);
    ipsec-sa sa-name;
    isid-list all-service-groups;
    keep-address-and-control;
    mac-validate (loose | strict);
    max-sessions number;
    mtu bytes;
    multicast-only;
    no-redirects;
    policer {

```

```

    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
protocols [inet iso mpls];
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name
    mode loose;
}
sampling {
    input;
    output;
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name <service-filter filter-name>;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
service-name-table table-name
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    master-only;
    multipoint-destination address {
        dlci dlci-identifier;
        epd-threshold cells <plp1 cells>;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
            sustained rate);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
}

```



```

preferred;
primary;
(vrrp-group | vrrp-inet6-group) group-number {
  (accept-data | no-accept-data);
  advertise-interval seconds;
  authentication-type authentication;
  authentication-key key;
  fast-interval milliseconds;
  (preempt | no-preempt) {
    hold-time seconds;
  }
  priority number;
  track {
    interface interface-name {
      bandwidth-threshold bits-per-second priority-cost number;
    }
    priority-hold-time seconds;
    route ip-address/prefix-length routing-instance instance-name priority-cost cost;
  }
  virtual-address [ addresses ];
  virtual-link-local-address ipv6-address;
  vrrp-inherit-from {
    active-interface interface-name;
    active-group group-number;
  }
}
}
}

```

Hierarchy Level	[edit interfaces <i>interface-name</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> ], [edit interfaces interface-set <i>interface-set-name</i> interface <i>interface-name</i> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options	<p><b>logical-unit-number</b>—Number of the logical unit.</p> <p><b>Range:</b> 0 through 1,073,741,823 for demux and PPPoE static interfaces only. 0 through 16,385 for all other static interface types.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <li>Configuring Logical Interface Properties</li> <li>Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers</li> <li><a href="#">Junos OS Services Interfaces Configuration Guide</a></li> </ul>

## vlan-id

---

See the following sections:

- [vlan-id \(Logical Port in Bridge Domain\) on page 438](#)
- [vlan-id \(Outer VLAN ID\) on page 439](#)
- [vlan-id \(VLAN ID to Be Bound to a Logical Interface\) on page 439](#)
- [vlan-id \(VLAN ID to Rewrite\) on page 440](#)

### vlan-id (Logical Port in Bridge Domain)

<b>Syntax</b>	<code>vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family bridge], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family bridge]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	The VLAN ID configured on the logical port. Received packets with no VLAN tags are forwarded within the bridge domain with the matching VLAN ID.
<b>Options</b>	<b>number</b> —The VLAN ID. <b>Range:</b> 1 through 4095
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Logical Interface for Access Mode on page 69</a></li></ul>

**vlan-id (Outer VLAN ID)**

<b>Syntax</b>	<code>vlan-id <i>outer-vlan-id</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	The outer VLAN ID to be used in ATM-to-Ethernet interworking cross-connects. Outer VLAN IDs are converted to the ATM VPI. The outer VLAN ID must match the VPI value configured. The allowable VPI range is 0 to 255. Do not configure the outer VLAN ID to be greater than 255.
<b>Options</b>	<b>outer-vlan-id</b> —Outer VLAN ID number. <b>Range:</b> 0 through 4094
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ATM-to-Ethernet Interworking</li> </ul>

**vlan-id (VLAN ID to Be Bound to a Logical Interface)**

<b>Syntax</b>	<code>vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Fast Ethernet, Gigabit Ethernet, and Aggregated Ethernet interfaces only, bind a 802.1Q VLAN tag ID to a logical interface.
<b>Options</b>	<b>number</b> —A valid VLAN identifier. <b>Range:</b> For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for management and internal Ethernet interfaces, 1 through 1023.  For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094.  VLAN ID 0 is reserved for tagging the priority of frames.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mixed Tagging on page 51</li> </ul>

## vlan-id (VLAN ID to Rewrite)

<b>Syntax</b>	<code>vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map]</code> , <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</code> , <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map]</code> , <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2, 10-Gigabit Ethernet LAN/WAN PIC, and IQ2-E interfaces and aggregated Ethernet using Gigabit Ethernet IQ interfaces, specify the line VLAN identifiers to be rewritten at the input or output interface.</p> <p>You cannot include the <b>vlan-id</b> statement with the <b>swap</b> statement, <b>swap-push</b> statement, <b>push-push</b> statement, or <b>push-swap</b> statement at the <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</code> hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the <b>vlan-id</b> statement that you include at the <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code> hierarchy level.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Rewriting the VLAN Tag on Tagged Frames on page 130</li><li>• Binding VLAN IDs to Logical Interfaces on page 53</li></ul>

## **vlan-id-list**

---

See the following sections:

- **vlan-id-list (Ethernet VLAN Circuit) on page 442**
- **vlan-id-list (Interface in Bridge Domain) on page 443**

## vlan-id-list (Ethernet VLAN Circuit)

<b>Syntax</b>	<code>vlan-id-list [ <i>vlan-id</i> <i>vlan-id</i>–<i>vlan-id</i> ];</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	(MX Series routers only) Binds a single-tag logical interface to a list of VLAN IDs. Configures a logical interface to receive and forward any tag frame whose VLAN ID tag matches the list of VLAN IDs you specify.



---

### NOTE:

When you create a circuit cross-connect (CCC) using VLAN-bundled single-tag logical interfaces on Layer 2 VPN routing instances, the circuit automatically uses ethernet encapsulation. For Layer 2 VPN, you need to include the `encapsulation-type` statement and specify the value `ethernet` at either of the following hierarchy levels:

- `[edit routing-instances routing-instance-name protocols l2vpn]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn]`

For more information about the `encapsulation-type` configuration statement and the Layer 2 encapsulation types `ethernet` and `ethernet-vlan`, see the [Junos OS VPNs Configuration Guide](#).

---

**Options** `[vlan-id vlan-id–vlan-id]`—A list of valid VLAN ID numbers. Specify the VLAN IDs individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both.

**Range:** 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.



---

**NOTE:** Configuring `vlan-id-list` with the entire `vlan-id` range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1-4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name
vlan-tagging;
unit number {
    vlan-id-range 1-4094;
}
```

```
[edit interfaces interface-name
unit 0;
```

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Binding VLAN IDs to Logical Interfaces on page 53
- encapsulation (Logical Interface)
- encapsulation (Physical Interface)
- encapsulation-type (Layer 2 VPN routing instance), see the [Junos OS VPNs Configuration Guide](#)
- flexible-vlan-tagging
- **vlan-tagging on page 448**
- **vlan-tags (Dual-Tagged Logical Interface) on page 450**

### vlan-id-list (Interface in Bridge Domain)

**Syntax** `vlan-id-list [ number number-number ];`

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family bridge],  
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family bridge]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Configure a logical interface to forward packets and learn MAC addresses within each bridge domain configured with a VLAN ID that matches a VLAN ID specified in the list. VLAN IDs can be entered individually using a space to separate each ID, entered as an inclusive list separating the starting VLAN ID and ending VLAN ID with a hyphen, or a combination of both.

**Options** *number number*—Individual VLAN IDs separated by a space.  
*number-number*—Starting VLAN ID and ending VLAN ID in an inclusive range.  
**Range:** 1 through 4095

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring a Logical Interface for Trunk Mode on page 70
- Configuring the VLAN ID List for a Trunk Interface on page 70

## vlan-id-range

---

<b>Syntax</b>	<code>vlan-id-range <i>vlan-id-vlan-id</i></code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Bind a range of VLAN IDs to a logical interface.
<b>Options</b>	<b>number</b> —The first number is the lowest VLAN ID in the range the second number is the highest VLAN ID in the range. <b>Range:</b> 1 through 4094



**NOTE:** Configuring `vlan-id-range` with the entire `vlan-id` range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1-4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]  
vlan-tagging;  
unit number {  
    vlan-id-range 1-4094;  
}  
  
[edit interfaces interface-name]  
unit 0;
```

VLAN ID 0 is reserved for tagging the priority of frames.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Binding a Range of VLAN IDs to a Logical Interface on page 54</li></ul>



## vlan-ranges

```
Syntax  vlan-ranges {
        access-profile profile-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                mac-address;
                option-82;
                radius-realm radius-realm-string;
                user-prefix user-prefix-string;
            }
        }
        dynamic-profile profile-name {
            accept (any | dhcp-v4 | inet);
            ranges (any | low-tag)—(any | high-tag);
        }
        override;
    }
```

**Hierarchy Level** [edit interfaces *interface-name* dynamic-profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.

**Options** **any**—Any valid VLAN ID number.

***vlan-id-low***—Specify the first VLAN ID number for the group of VLANs.

***vlan-id-high***—Specify the last VLAN ID number for the group of VLANs.

**Range:** 1 through 4094

The remaining statements are explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing—control—To add this statement to the configuration.

**Related Documentation**

- Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles
- Configuring Dynamic Mixed VLAN Ranges

## vlan-rewrite

---

<b>Syntax</b>	<code>vlan-rewrite translate (200 500   201 501)</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>number</i> family bridge interface-mode trunk]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Translates an incoming VLAN to a bridge-domain VLAN, corresponding counter translation at egress. Supports translation of VLAN 200 to VLAN 500 and VLAN 201 to VLAN 501. Other valid VLANs pass through without translation.
<b>Options</b>	<b>translate 200 500</b> —Translates incoming packets with VLAN 200 to 500. <b>translate 201 501</b> —Translates incoming packets with VLAN 201 to 501. <b>translate 202 502</b> —Translates incoming packets with VLAN 202 to 502.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Rewriting a VLAN Tag and Adding a New Tag on page 133</a></li></ul>

## vlan-rule (100-Gigabit Ethernet)

---

<b>Syntax</b>	<code>vlan-rule (high-low   odd-even);</code>
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot</i> pic <i>slot</i> forwarding-mode <b>vlan-steering</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure the interoperation mode of the 100-Gigabit Ethernet PIC when interoperating with 100 gigabit Ethernet interfaces from other vendors.  If no VLAN rule is configured, all tagged packets are distributed to PFE0.
<b>Options</b>	<b>high-low</b> —VLAN IDs 1 through 2047 are distributed to PFE0 and VLAN IDs 2048 through 4096 are distributed to PFE1.  <b>odd-even</b> —Odd number VLAN IDs are distributed to PFE1 and even number VLAN IDs are distributed to PFE0.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring 100-Gigabit Ethernet PIC VLAN Steering Mode</a></li><li>• <a href="#">forwarding-mode (100-Gigabit Ethernet) on page 375</a></li><li>• <a href="#">vlan-steering (100-Gigabit Ethernet) on page 447</a></li></ul>

## vlan-steering (100-Gigabit Ethernet)

---

<b>Syntax</b>	<pre>vlan-steering {     vlan-rule (high-low   odd-even); }</pre>
<b>Hierarchy Level</b>	[edit chassis fpc slot pic slot forwarding-mode]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	<p>Configure the 100-Gigabit Ethernet PIC to interoperate with 100 gigabit Ethernet interfaces from other vendors.</p> <p>See <b>sa-multicast</b> regarding interoperability with 100-Gigabit Ethernet PICs from Juniper Networks.</p> <p>The other statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring 100-Gigabit Ethernet PIC VLAN Steering Mode</li><li>• <b>forwarding-mode (100-Gigabit Ethernet)</b> on page 375</li><li>• <b>sa-multicast (100-Gigabit Ethernet)</b> on page 422</li><li>• <b>vlan-rule (100-Gigabit Ethernet)</b> on page 446</li></ul>

## vlan-tagging

---

<b>Syntax</b>	vlan-tagging;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• 802.1Q VLANs Overview on page 47</li><li>• vlan-id</li><li>• Configuring a Layer 3 Subinterface (CLI Procedure)</li><li>• Configuring Tagged Aggregated Ethernet Interfaces</li><li>• Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch</li></ul>

## vlan-tags

---

See the following sections:

- **vlan-tags (Dual-Tagged Logical Interface) on page 450**
- **vlan-tags (Stacked VLAN Tags) on page 452**

## vlan-tags (Dual-Tagged Logical Interface)

<b>Syntax</b>	<code>vlan-tags inner-list [vlan-id vlan-id–vlan-id ] outer &lt;tpid.&gt;vlan-id;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	(MX Series routers only) Binds a dual-tag logical interface to a list of VLAN IDs. Configures the logical interface to receive and forward any dual-tag frame whose inner VLAN ID tag matches the list of VLAN IDs you specify.



---

### NOTE:

To create a circuit cross-connect (CCC) using VLAN-bundled dual-tag logical interfaces on Layer 2 VPN routing instances, you must include the `encapsulation-type` statement and specify the value `ethernet-vlan` at the one of the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn]

For more information about the `encapsulation-type` configuration statement and the Layer 2 encapsulation types `ethernet` and `ethernet-vlan`, see the [Junos OS VPNs Configuration Guide](#).

---

**Options** `inner-list [vlan-id vlan-id vlan-id–vlan-id]`—A list of valid VLAN ID numbers. Specify the VLAN IDs individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both.

**Range:** 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

`outer <tpid.>vlan-id`—An optional Tag Protocol ID (TPID) and a valid VLAN ID.

**Range:** For TPID, specify a hexadecimal value in the format `0xnnnn`.

**Range:** For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.



---

**NOTE:** Configuring `inner-list` with the entire `vlan-id` range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs of inner tag (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1 through 4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]  
vlan-tagging;  
unit number {  
    vlan-tags outer vid inner-list 1-4094;  
}  
  
[edit interfaces interface-name]  
vlan-tagging;  
unit number {  
    vlan-id vid;  
}
```

---

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Binding VLAN IDs to Logical Interfaces on page 53
- encapsulation (Logical Interface)
- encapsulation (Physical Interface)
- encapsulation-type (Layer 2 VPN routing instance), see the [Junos OS VPNs Configuration Guide](#).
- flexible-vlan-tagging
- vlan-id-list (Ethernet VLAN Circuit) on page 442
- vlan-tagging on page 448

## vlan-tags (Stacked VLAN Tags)

<b>Syntax</b>	<code>vlan-tags inner <i>tpid.vlan-id</i> inner-range <i>vid1—vid2</i> outer <i>tpid.vlan-id</i>;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Gigabit Ethernet IQ and IQE interfaces only, binds TPIDs and 802.1Q VLAN tag IDs to a logical interface. You must include the <b>stacked-vlan-tagging</b> statement at the <code>[edit interfaces <i>interface-name</i>]</code> hierarchy level.



**NOTE:** The inner-range *vid1—vid2* option is supported on MX Series with IQE PICs only.

<b>Options</b>	<p><b>inner <i>tpid.vlan-id</i></b>—A TPID and a valid VLAN identifier.</p> <p><b>Range:</b> For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.</p> <p><b>inner-range <i>vid1—vid2</i></b>—For MX Series routers with Enhanced IQ (IQE) PICs only; specify a range of VLAN IDs where <i>vid1</i> is the start of the range and <i>vid2</i> is the end of the range.</p> <p><b>Range:</b> For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.</p> <p><b>outer <i>tpid.vlan-id</i></b>—A TPID and a valid VLAN identifier.</p> <p><b>Range:</b> For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames.</p>
----------------	--



**NOTE:** Configuring inner-range with the entire *vlan-id* range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs of inner tag (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1-4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup table entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name

    stacked-vlan-tagging;
    unit number {
        vlan-tags outer vid inner-range 1-4094;
    }

[edit interfaces interface-name
vlan-tagging;
```



```

unit number {
    vlan-id vid;
}

```

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Dual VLAN Tags on page 124
- stacked-vlan-tagging

## vlan-tags-outer

**Syntax** `vlan-tags-outer vlan-tag;`

**Hierarchy Level** [edit interfaces *interface-set* *interface-set-name* interface *interface-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** The S-VLAN outer tag that belongs to a set of interfaces used to configure hierarchical CoS schedulers.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Junos OS Class of Service Configuration Guide](#)

## vlan-vci-tagging

**Syntax** `vlan-vci-tagging;`

**Hierarchy Level** [edit interfaces *interface-name*],  
[edit logical-systems *logical-system-name* interfaces *interface-name*]

**Release Information** Statement introduced in Junos OS Release 9.0.

**Description** Enable the ATM-to-Ethernet interworking cross-connect function on a Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interface.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring ATM-to-Ethernet Interworking

## wavelength

---

<b>Syntax</b>	<code>wavelength <i>nm</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> optics-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For 10-Gigabit Ethernet DWDM interfaces only, configure full C-band ITU-Grid tunable optics.
<b>Options</b>	<p><i>nm</i>—Wavelength value. It can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>1528.77</b>—1528.77 nanometers (nm), corresponds from 50 through 100 gigahertz (GHz)</li><li>• <b>1529.16</b>—1529.16 nm, corresponds to 50 GHz</li><li>• <b>1529.55</b>—1529.55 nm, corresponds from 50 through 100 GHz</li><li>• <b>1529.94</b>—1529.94 nm, corresponds to 50 GHz)</li><li>• <b>1530.33</b>—1530.33 nm, corresponds to 50 to 100 GHz</li><li>• <b>1530.72</b>—1530.72 nm, corresponds to 50 GHz</li><li>• <b>1531.12</b>—1531.12 nm, corresponds from 50 through 100 GHz</li><li>• <b>1531.51</b>—1531.51 nm, corresponds to 50 GHz</li><li>• <b>1531.90</b>—1531.90 nm, corresponds from 50 through 100 GHz</li><li>• <b>1532.29</b>—1532.29 nm, corresponds to 50 GHz</li><li>• <b>1532.68</b>—1532.68 nm, corresponds from 50 through 100 GHz</li><li>• <b>1533.07</b>—1533.07 nm, corresponds to 50 GHz</li><li>• <b>1533.47</b>—1533.47 nm, corresponds from 50 through 100 GHz</li><li>• <b>1533.86</b>—1533.86 nm, corresponds to 50 GHz</li><li>• <b>1534.25</b>—1534.25 nm, corresponds from 50 through 100 GHz</li><li>• <b>1534.64</b>—1534.64 nm, corresponds to 50 GHz</li><li>• <b>1535.04</b>—1535.04 nm, corresponds from 50 through 100 GHz</li><li>• <b>1535.43</b>—1535.43 nm, corresponds to 50 GHz</li><li>• <b>1535.82</b>—1535.82 nm, corresponds from 50 through 100 GHz</li><li>• <b>1536.22</b>—1536.22 nm, corresponds to 50 GHz</li><li>• <b>1536.61</b>—1536.61 nm, corresponds from 50 through 100 GHz</li><li>• <b>1537.00</b>—1537.00 nm, corresponds to 50 GHz</li><li>• <b>1537.40</b>—1537.40 nm, corresponds from 50 through 100 GHz</li><li>• <b>1537.79</b>—1537.79 nm, corresponds to 50 GHz</li></ul>

- **1538.19**—1538.19 nm, corresponds from 50 through 100 GHz
- **1538.58**—1538.58 nm, corresponds to 50 GHz
- **1538.98**—1538.98 nm, corresponds from 50 through 100 GHz
- **1539.37**—1539.37 nm, corresponds to 50 GHz
- **1539.77**—1539.77 nm, corresponds from 50 through 100 GHz
- **1540.16**—1540.16 nm, corresponds to 50 GHz
- **1540.56**—1540.56 nm, corresponds from 50 through 100 GHz
- **1540.95**—1540.95 nm, corresponds to 50 GHz
- **1541.35**—1541.35 nm, corresponds from 50 through 100 GHz
- **1541.75**—1541.75 nm, corresponds to 50 GHz
- **1542.14**—1542.14 nm, corresponds from 50 through 100 GHz
- **1542.54**—1542.54 nm, corresponds to 50 GHz
- **1542.94**—1542.94 nm, corresponds from 50 through 100 GHz
- **1543.33**—1543.33 nm, corresponds to 50 GHz
- **1543.73**—1543.73 nm, corresponds to 50 to 100 gGHz
- **1544.13**—1544.13 nm, corresponds to 50 GHz
- **1544.53**—1544.53 nm, corresponds from 50 through 100 GHz
- **1544.92**—1544.92 nm, corresponds to 50 GHz
- **1545.32**—1545.32 nm, corresponds from 50 through 100 GHz
- **1545.72**—1545.72 nm, corresponds to 50 GHz
- **1546.12**—1546.12 nm, corresponds from 50 through 100 GHz
- **1546.52**—1546.52 nm, corresponds to 50 GHz
- **1546.92**—1546.92 nm, corresponds from 50 through 100 GHz
- **1547.32**—1547.32 nm, corresponds to 50 GHz
- **1547.72**—1547.72 nm, corresponds from 50 through 100 GHz
- **1548.11**—1548.11 nm, corresponds to 50 GHz
- **1548.51**—1548.51 nm, corresponds from 50 through 100 GHz
- **1548.91**—1548.91 nm, corresponds to 50 GHz
- **1549.32**—1549.32 nm, corresponds from 50 through 100 GHz
- **1549.72**—1549.72 nm, corresponds to 50 GHz
- **1550.12**—1550.12 nm, corresponds from 50 through 100 GHz
- **1550.52**—1550.52 nm, corresponds to 50 GHz
- **1550.92**—1550.92 nm, corresponds from 50 through 100 GHz

- **1551.32**—1551.32 nm, corresponds to 50 GHz
- **1551.72**—1551.72 nm, corresponds from 50 through 100 GHz
- **1552.12**—1552.12 nm, corresponds to 50 GHz
- **1552.52**—1552.52 nm, corresponds from 50 through 100 GHz
- **1552.93**—1552.93 nm, corresponds to 50 GHz
- **1553.33**—1554.33 nm, corresponds from 50 through 100 GHz
- **1553.73**—1554.73 nm, corresponds to 50 GHz
- **1554.13**—1554.13 nm, corresponds from 50 through 100 GHz
- **1554.54**—1554.54 nm, corresponds to 50 GHz
- **1554.94**—1554.94 nm, corresponds from 50 through 100 GHz
- **1555.34**—1555.34 nm, corresponds to 50 GHz
- **1555.75**—1555.75 nm, corresponds from 50 through 100 GHz
- **1556.15**—1556.15 nm, corresponds to 50 GHz
- **1556.55**—1556.55 nm, corresponds from 50 through 100 GHz
- **1556.96**—1556.96 nm, corresponds to 50 GHz
- **1557.36**—1557.36 nm, corresponds from 50 through 100 GHz
- **1557.77**—1557.77 nm, corresponds to 50 GHz
- **1558.17**—1558.17 nm, corresponds from 50 through 100 GHz
- **1558.58**—1558.58 nm, corresponds to 50 GHz
- **1558.98**—1558.98 nm, corresponds from 50 through 100 GHz
- **1559.39**—1559.39 nm, corresponds to 50 GHz
- **1559.79**—1559.79 nm, corresponds from 50 through 100 GHz
- **1560.20**—1560.20 nm, corresponds to 50 GHz
- **1560.61**—1560.61 nm, corresponds to 50 to 100 GHz
- **1561.01**—1561.01 nm, corresponds to 50 GHz
- **1561.42**—1561.42 nm, corresponds from 50 through 100 GHz
- **1561.83**—1561.83 nm, corresponds to 50 GHz
- **1562.23**—1562.23 nm, corresponds from 50 through 100 GHz
- **1562.64**—1562.64 nm, corresponds to 50 GHz
- **1563.05**—1563.05 nm, corresponds from 50 through 100 GHz
- **1563.45**—1563.45 nm, corresponds to 50 GHz
- **1563.86**—1563.86 nm, corresponds from 50 through 100 GHz
- **Default: 1550.12**—1550.12 nm, corresponds from 50 through 100 GHz

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- 10-Gigabit Ethernet DWDM Interface Wavelength Overview on page 297

## west-interface

**Syntax**

```
west-interface {
    node-id mac-address;
    control-channel channel-name {
        ring-protection-link-end;
    }
}
```

**Hierarchy Level** [edit protocols **protection-group** ethernet-ring *ring-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define one of the two interface ports for Ethernet ring protection, the other being defined by the **east-interface** statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.



**NOTE:** Always configure this port second, after configuring the **east-interface** statement.

The statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Ring Protection Switching Overview on page 339
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- east-interface
- **ethernet-ring** on page 370

## working-circuit

---

<b>Syntax</b>	<code>working-circuit <i>group-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> sonet-options aps]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the working router in an APS circuit pair.
<b>Options</b>	<i>group-name</i> —Circuit's group name.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Basic APS Support</li><li>protect-circuit</li></ul>

## PART 4

# Index

- Index on page 461
- Index of Statements and Commands on page 471





# Index

## Symbols

- #, comments in configuration statements.....xxxiv
- ( ), in syntax descriptions.....xxxiv
- 10-Gigabit Ethernet interfaces.....37
  - 802.3ah OAM.....260
  - DWDM.....297
  - framing.....299
- 10-Gigabit Ethernet IQ PIC.....299
- 10-Gigabit Ethernet LAN/WAN PIC
  - caveats.....289
  - control queue disable.....292
  - features.....289
  - handling oversubscription.....295
  - line rate mode.....292
  - oversubscribed Ethernet mode
    - control queue disable.....292
  - oversubscribed mode.....292
  - overview.....289
- 10-port 10-Gigabit Ethernet OSE PIC
  - caveats.....289
  - features.....289
  - overview.....289
- 100-Gigabit Ethernet
  - configuration
    - forwarding-mode.....375
    - sa-multicast.....422
    - vlan-rule.....446
    - vlan-steering.....447
  - forwarding-options
    - sa-multicast.....422
    - vlan-steering.....447
  - vlan-steering
    - vlan-rule.....446
- 802.1ag Ethernet OAM for VPLS.....198
- 802.1ag OAM
  - configuring Ethernet interfaces.....159
- 802.1Q VLANs
  - mixed VLAN tagging.....52
  - VLAN IDs.....439, 444
    - values, listed by Ethernet interface
      - type.....49
  - VLAN tagging.....47, 143, 448
- 802.3ad statement.....359
  - usage guidelines.....77
- 802.3ah OAM
  - configuring Ethernet interfaces.....253
  - example configuration.....260
- < >, in syntax descriptions.....xxxiii
- [ ], in configuration statements.....xxxiv
- { }, in configuration statements.....xxxiv
- | (pipe), in syntax descriptions.....xxxiv

## A

- accept-source-mac statement
  - usage guidelines.....268
- access interface
  - interface-mode statement.....69
- access-concentrator statement
  - usage guidelines.....317
- active statement
  - usage guidelines.....102
- active-active bridging.....80, 88
- ADSL
  - example configuration.....321, 322
- aggregate statement
  - usage guidelines.....265, 266
- aggregated Ethernet interfaces.....77
  - configuring.....75
  - example configuration.....354
- LACP.....102
  - example configuration.....107
  - interval.....103
  - traceoptions.....106
- link speed.....109
- minimum links.....110
- multicast statistics.....111
- VLAN IDs.....49

aggregated-ether-options statement.....	361
usage guidelines.....	29
aging timer	
ARP.....	43
all (tracing flag)	
VRRP.....	43
ARP	
aging timer.....	43
ARP proxy, unrestricted	
Ethernet interfaces.....	149
arp statement	
usage guidelines.....	147
ARP table, static	
Ethernet interfaces.....	147
ATM-for-ADSL	
example configuration.....	321
ATM-to-Ethernet interworking.....	453
VLAN tagging.....	382, 439
auto-negotiation statement	
Gigabit Ethernet.....	363
usage guidelines.....	277
J Series uPIM.....	36
auto-reconnect statement	
usage guidelines.....	317
autonegotiation	
configuring manually.....	277
<b>B</b>	
backup routers	
VRRP.....	261
bandwidth-limit statement	
policer for Gigabit Ethernet interface.....	364
usage guidelines.....	266
braces, in configuration statements.....	xxxiv
brackets	
angle, in syntax descriptions.....	xxxiii
square, in configuration statements.....	xxxiv
Bridge Domain.....	163
bridge network	
trunk interface.....	71
bridge-domain.....	163
burst-size-limit statement	
policer for Gigabit Ethernet interface.....	364
usage guidelines.....	266

## C

CCC	
encapsulation	
VLAN-bundled dual-tag logical	
interfaces.....	450
VLAN-bundled single-tag logical	
interfaces.....	442
channelized STM1 interfaces	
example configuration.....	305
interface naming.....	305
virtual tributary mapping.....	305
circuit cross-connect (CCC)	
encapsulation	
VLAN-bundled dual-tag logical	
interfaces.....	450
VLAN-bundled single-tag logical	
interfaces.....	442
classifier statement.....	365
usage guidelines.....	267
comments, in configuration statements.....	xxxiv
Configuring a Layer 2 Circuit on a VLAN-Bundled	
Logical Interface.....	65
Configuring a VLAN-Bundled Logical	
Interface.....	64, 65
Configuring Logical Link-Layer Encapsulation to	
Support CCCs.....	62
Configuring VLAN ID List-Bundled Logical Interfaces	
That Connect CCCs.....	62
connections	
configuration statements.....	23, 26
continuity measurement	
displaying statistics and frame counts.....	238
conventions	
text and syntax.....	xxxiii
curly braces, in configuration statements.....	xxxiv
customer support.....	xxxiv
contacting JTAC.....	xxxiv

## D

database (tracing flag).....	43
discovery stage	
PPPoE.....	309
documentation	
comments on.....	xxxiv
dot1x	
configuration statements.....	24
dual-tag framing	
VLAN ID list.....	450

dynamic PPPoE statements	
pppoe-underlying-options.....	414
dynamic subscribers	
pppoe-underlying-options statement.....	414

## E

E-LMI.....	173
el-options statement	
usage guidelines.....	305
em0	
configuring.....	285
management Ethernet interface.....	285
encapsulation	
extended VLAN CCC.....	60, 143
ETH-DM	
configuring routers to support.....	215, 223, 238
displaying statistics and frame	
counts.....	218, 228, 238
overview.....	202
starting an ETH-DM session.....	216, 226, 238
ETH-LM	
displaying statistics and frame counts.....	231
overview.....	208
Ethernet bridging.....	141, 142
Ethernet configurations, example.....	353
Ethernet continuity measurement	
displaying statistics and frame counts.....	238
Ethernet frame delay measurement	
configuring routers to support.....	215, 223, 238
displaying statistics and frame	
counts.....	218, 228, 238
overview.....	202
starting an ETH-DM session.....	216, 226, 238
Ethernet frame loss measurement	
displaying statistics and frame counts.....	231
overview.....	208
Ethernet interfaces.....	141
802.1ag OAM.....	159
802.3ah OAM.....	253
configuration statements.....	29
example configuration.....	353
Fast Ethernet interfaces.....	29
Gigabit Ethernet interfaces.....	29
gratuitous ARP.....	42
management Ethernet interface.....	285
mixed VLAN tagging.....	52
multicast statistics.....	45
passive monitoring.....	155
proxy ARP, unrestricted.....	149

static ARP table entries.....	147
VLAN IDs.....	439
VLAN tagging.....	47, 143, 448
VRRP.....	261
Ethernet link aggregation.....	77
Ethernet Local Management Interface See E-LMI	
Ethernet Ring Protection	
configuration statements.....	27
Ethernet Ring Protection Switching,	
Configuring.....	339
Ethernet Service OAM .....	201
ethernet statement.....	366
Ethernet switching.....	141, 142
Ethernet switching interfaces.....	36
Ethernet TCC	
applying.....	144
encapsulation.....	143
example configuration.....	145
Ethernet VLAN circuit	
VLAN ID list.....	442
ethernet-policer-profile statement.....	369
usage guidelines.....	265, 266
ethernet-ring statement.....	370
ethernet-switch-profile statement.....	270, 371
usage guidelines.....	123, 265
event statement	
port-status-tlv statement.....	411
extended VLAN	
CCC	
applying.....	60
example configuration.....	61
TCC	
applying.....	143
encapsulation.....	143

## F

failover-delay statement	
usage guidelines.....	261
family bridge	
VLAN ID list.....	443
VLAN IDs.....	438
Fast Ethernet interfaces	
configuration statements.....	29
Ethernet link aggregation.....	77
example configuration.....	353
ignoring Layer 3 incomplete errors.....	41
ingress rate-limit.....	44
link modes.....	41
link protection.....	100

loopback mode.....	40
MAC address filtering.....	38
physical interface properties.....	29
proxy ARP, unrestricted.....	149
speed.....	44
static ARP table entries.....	147
usage guidelines.....	143
VLAN IDs.....	49, 439
VLAN tagging.....	47, 143, 448
VRRP.....	261
fastether-options statement.....	372
usage guidelines.....	29
flow control.....	41
flow-control statement.....	373
usage guidelines.....	41
flow-control-options statement.....	374
font conventions.....	xxxiii
forwarding-class statement	
usage guidelines.....	267
forwarding-mode statement.....	375
frame delay, Ethernet See Ethernet frame delay	
measurement	
frame loss, Ethernet See Ethernet frame loss	
measurement	
framing statement	
10-Gigabit Ethernet interfaces.....	376
usage guidelines.....	299
fxp0 interface	
configuring.....	285
management Ethernet interface.....	285
<b>G</b>	
ge interface	
configuring otn-options.....	283
general (tracing flag).....	43
Gigabit Ethernet interfaces.....	37, 141
802.1ag .....	159
802.3ah .....	253
autonegotiation.....	277
configuration statements.....	29
Ethernet link aggregation.....	77
example configuration.....	353
flow control.....	41
ignoring Layer 3 incomplete errors.....	41
link protection.....	100
loopback mode.....	40
MAC address filtering.....	38
proxy ARP, unrestricted.....	149
static ARP table entries.....	147
usage guidelines.....	143
VLAN IDs.....	49, 439, 444
VLAN tagging.....	47, 143, 382, 439, 448
VRRP.....	261
Gigabit Ethernet IQ interfaces	
configuring.....	263
MAC address accounting.....	274
MAC address filtering.....	269
policer	
example configuration.....	270
rate limiting.....	265, 266
Gigabit Ethernet OTN.....	283
Gigabit Ethernet uPIM interfaces	
speed.....	44
Gigabit Ethernet, IQ, IQ2 and IQ2-E interfaces	
VLAN tag stacking and rewriting.....	119
gether-options statement.....	377
usage guidelines.....	29
gratuitous ARP.....	42
gratuitous-arp-reply statement.....	378
usage guidelines.....	42
<b>I</b>	
iccp	
configuration statements.....	24
ICL-PL configuration.....	89
icons defined, notice.....	xxxii
IEEE 802.1p policer profile	
usage guidelines.....	266
ieee802.1p statement.....	379
IGMP snooping for active-active MC-LAG	
configuration.....	92
ignore-l3-incompletes statement.....	379
ignoring Layer 3 incomplete errors.....	41
ingress-rate-limit statement.....	380
usage guidelines.....	44
inner-tag-protocol-id statement.....	380
usage guidelines.....	124
inner-vlan-id statement.....	381
usage guidelines.....	124
inner-vlan-id-range statement.....	382
input-priority-map statement.....	382
usage guidelines.....	266
input-vlan-map statement.....	383
usage guidelines.....	119
instance.....	163
Instance.....	163
integrated routing and bridging interfaces See IRB	

interface statement  
     usage guidelines.....71  
 interface-mode statement  
     usage guidelines.....69, 70  
 interfaces  
     10-Gigabit Ethernet DWDM.....297  
     10-Gigabit Ethernet framing.....299  
     aggregated Ethernet.....75  
     configuration statements.....3, 359  
     Gigabit Ethernet  
         configuring.....277  
     Gigabit Ethernet IQ .....263  
     Gigabit Ethernet IQ policer  
         example configuration.....270  
     mixed VLAN tagging.....52  
 interfaces (tracing flag).....43  
 interfaces statement.....384  
 IP addresses  
     management Ethernet interface.....285  
     mapping to MAC address.....147, 149  
 IQ interfaces  
     channelized STM1.....305  
     Gigabit Ethernet.....263  
 IQE interfaces  
     channelized STM1.....305  
 Iterator  
     example configuration.....246  
 Iterator profile  
     configuration.....211  
 iterator statistics.....233  
 iterators  
     VPLS connections.....214  
 ITU-T Recommendation Y.1731.....201  
 ITU-T standards  
     Y.1731 ETH-DM.....202  
     Y.1731 ETH-LM.....208  
 ITU-Y.1731  
     VPLS connections.....214

## J

J Series Routers.....36  
 jitter, Ethernet frame See Ethernet frame delay  
     measurement

## L

LACP  
     Ethernet aggregation.....102  
         example configuration.....107  
         interval.....103  
         traceoptions.....106  
         tracing operations.....106  
 lacp statement  
     802.3ad.....385  
     Aggregated Ethernet.....386  
     usage guidelines.....102  
 LAN PHY.....299  
 Layer 2 bridging  
     Ethernet.....142  
 Layer 2.5 VPNs  
     Ethernet.....60, 143, 144  
 Layer 3 incomplete errors.....379  
 line-vlan-id statement  
     usage guidelines.....119  
 link aggregation.....77  
 link modes.....41  
 link protection  
     aggregated Ethernet interfaces  
         configuring.....100  
         configuring primary and backup links.....101  
         disabling.....101  
         reverting traffic to primary link.....101  
 link speed  
     Ethernet aggregation.....109  
 link-discovery statement.....387  
 link-fault-management statement.....388  
 link-mode statement.....389  
     usage guidelines.....41  
 link-protection statement.....390  
 link-speed statement  
     usage guidelines.....109  
 log files  
     number of PPPoE.....335  
     size of PPPoE.....335  
 logical interfaces  
     static ARP table entries.....147, 149  
     VLAN IDs.....439, 444  
     VLAN-bundled  
         dual-tag.....450  
         single-tag.....442  
 logical systems  
     configuration statements.....19  
 loopback mode.....40

loopback statement	
Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet.....	392
Fast Ethernet interfaces	
usage guidelines.....	40
Gigabit Ethernet interfaces	
usage guidelines.....	40
loss-priority statement.....	392
usage guidelines.....	267
<b>M</b>	
MAC address accounting	
Gigabit Ethernet IQ interfaces.....	274
MAC address filtering	
Fast Ethernet interfaces.....	38
Gigabit Ethernet interfaces.....	38
Gigabit Ethernet IQ interfaces.....	269
MAC addresses	
management Ethernet interface.....	38, 286
mapping to IP addresses.....	147, 149
MAC flush.....	192
mac statement	
usage guidelines.....	286
mac-learn-enable statement.....	393
usage guidelines.....	274
Maintenance Intermediate Points.....	162
Bridge Domain.....	163
Instance.....	163
MIP.....	162
MIP Half Function.....	163
maintenance-domain statement	
mip-half-function.....	396
management Ethernet interface	
configuring.....	285
IP address.....	285
link modes.....	41
MAC address.....	286
speed.....	44
manuals	
comments on.....	xxxiv
master routers	
VRRP.....	261
master-only statement	
usage guidelines.....	285
MC-LAG configuration.....	89
mep statement.....	394
minimum links for aggregation	
Ethernet links.....	110

minimum-links statement.....	395
usage guidelines.....	110
MIP Half Function.....	163
mip-half-function.....	163
mip-half-function statement.....	396
mixed VLAN tagging.....	52
mpls statement.....	397
multicast-statistics statement	
usage guidelines	
aggregated Ethernet.....	111
Ethernet.....	45
multichassis link aggregation	
active-active bridging.....	80, 88
VRRP over integrated routing and bridging.....	80, 88
multichassis link aggregation (MC-LAG).....	78
multiple chassis configuration.....	90
MX Series Routers.....	37

## N

negotiate-address statement	
usage guidelines.....	317
no-auto-mdix statement.....	397
no-auto-negotiation statement	
Gigabit Ethernet	
usage guidelines.....	277
J Series uPIM.....	36
no-flow-control statement.....	373
usage guidelines.....	41
no-gratuitous-arp-reply statement.....	378
usage guidelines.....	42
no-gratuitous-arp-request statement.....	398
usage guidelines.....	42
no-loopback statement.....	392
usage guidelines.....	40
no-mac-learn-enable statement.....	393
usage guidelines.....	274
no-source-filtering statement.....	424
usage guidelines.....	38, 269
normal (tracing flag)	
arp aging timer.....	43
notice icons defined.....	xxii

## O

OAM	
configuration statements.....	24
E-LMI.....	173
oam statement.....	399

optics-options statement.....	401
usage guidelines.....	297
output-priority-map statement.....	402
usage guidelines.....	267
output-vlan-map statement	
usage guidelines.....	119

## P

packets (tracing flag).....	43
parentheses, in syntax descriptions.....	xxxiv
passive monitoring flow	
Ethernet interfaces.....	155
passive statement	
usage guidelines.....	102
passive-monitor-mode statement	
usage guidelines.....	155
pdu-interval statement.....	402
pdu-threshold statement.....	403
periodic statement.....	404
usage guidelines.....	103
physical interfaces	
Ethernet link aggregation.....	77
flow control.....	41
link modes.....	41
loopback mode.....	40
MAC address filtering.....	38
mixed VLAN tagging.....	52
VLAN tagging.....	47, 143, 448
policer statement	
CFM firewall.....	405
CFM global level.....	406
CFM session level.....	407
CoS.....	408
interface MAC.....	409
usage guidelines.....	265
policing	
Gigabit Ethernet IQ interfaces.....	265, 266
pop statement	
Gigabit Ethernet IQ interfaces.....	410
Gigabit Ethernet, IQ, IQ2 and IQ2-E interfaces	
usage guidelines.....	119
usage guidelines.....	128
pop-pop statement	
Gigabit Ethernet IQ interfaces.....	410
usage guidelines.....	128
pop-swap statement	
Gigabit Ethernet IQ interfaces.....	411
usage guidelines.....	129
Port-Based Network Access Control Protocol	
IEEE 802.1x	
dot1x.....	249
port-status-tlv statement.....	411
ppp-options statement.....	412
PPPoE	
discovery stage.....	309
example configuration.....	321, 322
flags for tracing operations.....	336
log file access for tracing operations.....	335
log file size and number.....	335
log filenames for tracing operations.....	335
regular expressions for tracing	
operations.....	335
service name tables	
about.....	309
ACI/ARI pair configuration.....	328
ACI/ARI pairs.....	311
any service configuration.....	325
assigning to underlying interface.....	331
benefits.....	314
configuration example.....	331
configuration overview.....	323
configuration troubleshooting.....	336
creating.....	324
dynamic PPPoE interfaces.....	312
empty service configuration.....	324
enabling PADO advertisement.....	331
evaluation order for matching client	
information.....	314
maximum sessions limit.....	312, 329
named service configuration.....	326
PADO advertisement.....	313
service entries and actions.....	310
static interfaces, reserving.....	330
static PPPoE interfaces.....	313
verifying the configuration.....	338
tracing operations.....	334
PPPoE client	
example configuration.....	321
reserving static interfaces for.....	330
PPPoE server	
example configuration.....	322
pppoe-options statement.....	413
usage guidelines.....	317
pppoe-underlying-options statement	
static and dynamic PPPoE.....	414
premium	
policer.....	416

premium statement	
hierarchical policer.....	415
output priority map.....	416
usage guidelines.....	265, 266, 267
Proactive mode	
overview.....	210
protection-group	
configuration statements.....	27
protection-group statement.....	417
protocol-down statement.....	418
protocols connections	
configuration statements.....	23, 26
protocols dot1x	
configuration statements.....	24
protocols Ethernet Ring Protection	
configuration statements.....	27
protocols iccp	
configuration statements.....	24
protocols OAM	
configuration statements.....	24
protocols VRRP	
configuration statements.....	24
proxy statement	
usage guidelines.....	144
proxy-arp statement	
usage guidelines.....	149
push statement	
Gigabit Ethernet IQ interfaces.....	418
Gigabit Ethernet, IQ, IQ2 and IQ2-E interfaces	
usage guidelines.....	119
usage guidelines.....	127
push-push statement	
Gigabit Ethernet IQ interfaces.....	419
usage guidelines.....	129

## R

remote MEP with iterator profile	
configuration.....	213
remote statement	
usage guidelines.....	60, 143, 144
remote-mep statement.....	420
request statement.....	420
rewrite VLAN tag on untagged frame	
usage guidelines.....	131
rewrite-on-egress statement	
usage guidelines.....	119
rewrite-on-ingress statement	
usage guidelines.....	119
ring-protection-link-end statement.....	421

ring-protection-link-owner statement.....	421
---	-----

## S

sa-multicast statement.....	422
service ID configuration.....	90
service name tables	
PPPoE	
about.....	309
ACI/ARI pair configuration.....	328
ACI/ARI pairs.....	311
any service configuration.....	325
assigning to underlying interface.....	331
benefits.....	314
configuration example.....	331
configuration overview.....	323
configuration troubleshooting.....	336
creating.....	324
dynamic PPPoE interfaces.....	312
empty service configuration.....	324
enabling PADO advertisement.....	331
evaluation order for matching client	
information.....	314
maximum sessions limit.....	312, 329
named service configuration.....	326
PADO advertisement.....	313
service entries and actions.....	310
static interfaces, reserving.....	330
static PPPoE interfaces.....	313
verifying the configuration.....	338
service-level agreement measurement	
overview.....	202
service-name statement	
usage guidelines.....	317
sla-iterator-profile statement	
usage guidelines.....	213
sonet-options statement	
usage guidelines.....	305
source address filtering	
Fast Ethernet interfaces.....	38, 39
Gigabit Ethernet interfaces.....	38, 39
source-address-filter statement.....	423
usage guidelines.....	39
source-filtering statement.....	424
usage guidelines.....	38, 269
Specifying the Interface Over Which VPN Traffic	
Travels to the CE Router.....	64
Specifying the Interface to Handle Traffic for a	
CCC.....	64



Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit.....	66
speed statement	
Ethernet.....	425
MX Series DPC.....	426
usage guidelines.....	44
stacked VLAN-tag framing	
VLAN ID list.....	452
stacked-vlan-tagging statement	
usage guidelines.....	119
startup-silent-period statement	
usage guidelines.....	261
state (tracing flag).....	43
static ARP table entries	
Ethernet interfaces.....	147, 149
example configuration.....	148
static PPPoE statements	
pppoe-underlying-options.....	414
static subscribers	
pppoe-underlying-options statement.....	414
STM1 interfaces	
example configuration.....	305
subscriber interface statements	
pppoe-underlying-options.....	414
support, technical See technical support	
swap statement	
Gigabit Ethernet IQ interfaces.....	427
Gigabit Ethernet, IQ, IQ2 and IQ2-E interfaces	
usage guidelines.....	119
swap-push statement	
Gigabit Ethernet IQ interfaces.....	427
usage guidelines.....	133
swap-swap statement	
Gigabit Ethernet IQ interfaces.....	428
usage guidelines.....	134
switch-options statement.....	428
switch-port statement	
access switching.....	429
Symmetrical Load Balancing	
on 802.3ad Link Aggregation on MX Series.....	112
syntax conventions.....	xxxiii
<b>T</b>	
tag-protocol-id statement.....	430
TPID to rewrite.....	431
TPIDs expected to be sent or received.....	430
usage guidelines.....	119, 124
technical support	
contacting JTAC.....	xxxiv
timer (tracing flag)	
Ethernet interface speed.....	43
trace operations	
VRRP.....	43
traceoptions (LACP) statement	
usage guidelines.....	106
traceoptions statement	
VRRP	
usage guidelines.....	43
tracing operations	
LACP.....	106
PPPoE.....	334
Tri-Rate Ethernet copper interfaces	
speed.....	44
trunk interface	
interface-mode statement.....	70
usage guidelines.....	71
vlan-id-list statement.....	70
trunk port.....	70
VLAN ID list.....	443
<b>U</b>	
unit statement.....	432
unnumbered-interface statement	
usage guidelines.....	317
uPIM Ethernet interfaces.....	36
<b>V</b>	
Virtual Router Redundancy Protocol See VRRP	
VLAN	
Configuring a Layer 2 Circuit on a	
VLAN-Bundled Logical Interface.....	65
Configuring a VLAN-Bundled Logical	
Interface.....	65
Configuring Logical Link-Layer Encapsulation	
to Support CCCs.....	62
Configuring VLAN ID List-Bundled Logical	
Interfaces That Connect CCCs.....	62
Specifying the Interface Over Which VPN	
Traffic Travels to the CE Router.....	64
Specifying the Interface to Handle Traffic for a	
CCC.....	64
VLAN CCC	
configuration guidelines.....	59
example configuration.....	60
VLAN IDs.....	444
values, listed by Ethernet interface type.....	49

VLAN tag stacking and rewriting	
Gigabit Ethernet, IQ, IQ2 and IQ2-E	
interfaces.....	119
VLAN tagging.....	47, 143, 448
VLAN VPLS	
configuration guidelines.....	59
example configuration.....	60
vlan-id statement.....	438
802.IQ VLANs.....	439
ATM-to-Ethernet cross-connect.....	439
Ethernet interfaces.....	439
usage guidelines.....	47, 143
Fast Ethernet interfaces	
usage guidelines.....	47, 143
Gigabit Ethernet interfaces	
usage guidelines.....	53, 58
interface in bridge domain.....	438
rewriting at ingress or egress.....	440
usage guidelines.....	119
vlan-id-list.....	441
vlan-id-list statement	
bridge domain.....	443
Ethernet VLAN circuit.....	442
Gigabit Ethernet interfaces	
usage guidelines.....	53
usage guidelines.....	70
vlan-id-range statement.....	444
Ethernet interfaces.....	444
Gigabit Ethernet interfaces	
usage guidelines.....	53
vlan-ranges statement.....	445
vlan-rewrite statement.....	446
vlan-rule statement.....	446
vlan-steering statement.....	447
vlan-tagging statement.....	448
Ethernet interfaces	
usage guidelines.....	47, 143
Fast Ethernet interfaces	
usage guidelines.....	47, 143
Gigabit Ethernet interfaces	
usage guidelines.....	47
vlan-tags statement	
dual-tag framing.....	450
Gigabit Ethernet interfaces	
usage guidelines.....	58
stacked VLAN tags.....	452
usage guidelines.....	124
vlan-tags-outer statement.....	453
vlan-vci-tagging statement.....	453
VLANs	
configuring VLAN ranges.....	445
VPLS	
statistical frame loss measurement.....	214
VRRP.....	261
configuration statements.....	24
trace operations.....	43
tracing flag.....	43
VRRP over integrated routing and bridging.....	80, 88
<b>W</b>	
WAN PHY	
configuring.....	299
wavelength statement.....	454
usage guidelines.....	297
weighted random early detection.....	45
west-interface statement.....	457
working-circuit statement.....	458
WRED.....	45

# Index of Statements and Commands

## Symbols

802.3ad statement.....359

## A

aggregated-ether-options statement.....361

auto-negotiation statement

    Gigabit Ethernet.....363

## B

bandwidth-limit statement

    policer for Gigabit Ethernet interface.....364

burst-size-limit statement

    policer for Gigabit Ethernet interface.....364

## C

classifier statement.....365

## D

dynamic PPPoE statements

    pppoe-underlying-options.....414

## E

ethernet statement.....366

ethernet-policer-profile statement.....369

ethernet-ring statement.....370

ethernet-switch-profile statement.....270, 371

event statement

    port-status-tlv statement.....411

## F

fastether-options statement.....372

flow-control statement.....373

flow-control-options statement.....374

forwarding-mode statement.....375

framing statement

    10-Gigabit Ethernet interfaces.....376

## G

gether-options statement.....377

gratuitous-arp-reply statement.....378

## I

ieee802.1p statement.....379

ignore-l3-incompletes statement.....379

ingress-rate-limit statement.....380

inner-tag-protocol-id statement.....380

inner-vlan-id statement.....381

inner-vlan-id-range statement.....382

input-priority-map statement.....382

input-vlan-map statement.....383

interfaces statement.....384

## L

lacp statement

    802.3ad.....385

    Aggregated Ethernet.....386

link-discovery statement.....387

link-fault-management statement.....388

link-mode statement.....389

link-protection statement.....390

loopback statement

    Aggregated Ethernet, Fast Ethernet, and Gigabit

    Ethernet.....392

loss-priority statement.....392

## M

mac-learn-enable statement.....393

maintenance-domain statement

    mip-half-function.....396

mep statement.....394

minimum-links statement.....395

mip-half-function statement.....396

mpls statement.....397

## N

no-auto-mdix statement.....397

no-flow-control statement.....373

no-gratuitous-arp-reply statement.....378

no-gratuitous-arp-request statement.....398

no-loopback statement.....392

no-mac-learn-enable statement.....393

no-source-filtering statement.....424

## O

oam statement.....399

optics-options statement.....401

output-priority-map statement.....402

## P

pdu-interval statement.....402

pdu-threshold statement.....403

periodic statement.....404

policer statement

    CFM firewall.....405

    CFM global level.....406

    CFM session level.....407

    CoS.....408

    interface MAC.....409

pop statement

    Gigabit Ethernet IQ interfaces.....410

pop-pop statement

    Gigabit Ethernet IQ interfaces.....410

pop-swap statement

    Gigabit Ethernet IQ interfaces.....411

port-status-tlv statement.....411

ppp-options statement.....412

pppoe-options statement.....413

pppoe-underlying-options statement

    static and dynamic PPPoE.....414

premium

    policer.....416

premium statement

    hierarchical policer.....415

    output priority map.....416

protection-group statement.....417

protocol-down statement.....418

push statement

    Gigabit Ethernet IQ interfaces.....418

push-push statement

    Gigabit Ethernet IQ interfaces.....419

## R

remote-mep statement.....420

request statement.....420

ring-protection-link-end statement.....421

ring-protection-link-owner statement.....421

## S

sa-multicast statement.....422

sla-iterator-profile statement

    usage guidelines.....213

source-address-filter statement.....423

source-filtering statement.....424

speed statement

    Ethernet.....425

    MX Series DPC.....426

static PPPoE statements

    pppoe-underlying-options.....414

subscriber interface statements

    pppoe-underlying-options.....414

swap statement

    Gigabit Ethernet IQ interfaces.....427

swap-push statement

    Gigabit Ethernet IQ interfaces.....427

swap-swap statement

    Gigabit Ethernet IQ interfaces.....428

switch-options statement.....428

switch-port statement

    access switching.....429

## T

tag-protocol-id statement.....430

    TPID to rewrite.....431

    TPIDs expected to be sent or received.....430

## U

unit statement.....432

## V

vlan-id statement.....438

    802.1Q VLANs.....439

    ATM-to-Ethernet cross-connect.....439

    Ethernet interfaces.....439

    interface in bridge domain.....438

    rewriting at ingress or egress.....440

vlan-id-list.....441

vlan-id-list statement

    bridge domain.....443

    Ethernet VLAN circuit.....442

vlan-id-range statement.....444

vlan-ranges statement.....445

vlan-rewrite statement.....446

vlan-rule statement.....446

vlan-steering statement.....447

vlan-tagging statement.....448

vlan-tags statement

    dual-tag framing.....450

    stacked VLAN tags.....452

vlan-tags-outer statement.....	453
vlan-vci-tagging statement.....	453

## W

wavelength statement.....	454
west-interface statement.....	457
working-circuit statement.....	458

