THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
• To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

• To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.

• To submit a service request, visit Cisco Support.

• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

• To obtain general networking, training, and certification titles, visit Cisco Press.

• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

© 2019 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## P R E F A C E

Preface  xxii  
Changes to This Document  xxii  
Communications, Services, and Additional Information  xxii

## C H A P T E R  1

Dense Wavelength Division Multiplexing Commands  1  
admin-state  3  
controller dwdm  5  
g709 bdi-to-client-gais  7  
g709 enable  8  
g709 fec  9  
g709 odu overhead tti  11  
g709 odu report disable  12  
g709 otu overhead tti  13  
g709 otu report disable  15  
g709 otu threshold  17  
g709 tim-to-client-gais  18  
g709 tti-processing  19  
log signal  20  
loopback (DWDM)  21  
network connection id  22  
network port id  23  
fm fec report enable  24  
fm fec threshold  25  
fm optics report enable  26  
fm optics threshold  28  
fm otn report enable  30
show lldp neighbors 101
show lldp traffic 104
show mac-accounting (Ethernet) 106
small-frame-padding 108
speed (Fast Ethernet) 109
transport-mode (UDLR) 111

CHAPTER 3

Ethernet OAM Commands 113
action capabilities-conflict 117
action critical-event 119
action discovery-timeout 121
action dying-gasp 123
action high-threshold 125
action remote-loopback 127
action session-down 129
action session-up 131
action uni-directional link-fault 133
action wiring-conflict 135
aggregate 137
ais transmission 139
ais transmission up 141
buckets archive 143
buckets size 144
clear error-disable 146
clear ethernet cfm ccm-learning-database location 147
clear ethernet cfm interface statistics 148
clear ethernet cfm local meps 149
clear ethernet cfm offload 151
clear ethernet cfm peer meps 152
clear ethernet cfm traceroute-cache 153
clear ethernet lmi interfaces 154
clear ethernet oam statistics 155
clear ethernet sla statistics all 156
clear ethernet sla statistics on-demand 157
Frame Relay Commands 361

clear frame-relay multilink interface 362

clear frame-relay lmi interface 364

encap (PVC) 365

encapsulation frame-relay 366
frame-relay intf-type 368
frame-relay lmi disable 369
frame-relay lmi-n391dte 370
frame-relay lmi-n392dce 371
frame-relay lmi-n392dte 372
frame-relay lmi-n393dce 373
frame-relay lmi-n393dte 374
frame-relay lmi-t391dte 375
frame-relay lmi-t392dce 376
frame-relay lmi-type 377
frame-relay multilink ack 378
frame-relay multilink bandwidth-class 380
frame-relay multilink bid 382
frame-relay multilink hello 384
frame-relay multilink lid 386
frame-relay multilink retry 388
pvc (frame relay) 390
show frame-relay lmi 391
show frame-relay lmi-info 393
show frame-relay multilink 396
show frame-relay pvc 409
show frame-relay vcm-info interface 412
show interfaces (frame relay) 414
snmp-server traps frame-relay pvc 418

CHAPTER 5

Global Interface Commands 421
bandwidth (global) 422
bundle wait-while 423
clear interface 424
dampening 425
interface (global) 427
lacp system 429
mlacp reset priority 430
mlacp switchback 431
m lacp switchover maximize  
mlacp switchover type  
mtu  
show im dampening  
show interfaces  
show m lacp inconsistencies  
shutdown (global)  

 CHAPTER 6  
**Internal Ethernet Control Network Commands**  
clear controller backplane ethernet location statistics  
show controllers backplane ethernet local brief  
show controllers backplane ethernet local clients  
show controllers backplane ethernet local detail  
show controllers backplane ethernet local multicast groups  
show controllers backplane ethernet location brief  
show controllers backplane ethernet location clients  
show controllers backplane ethernet location detail  
show controllers backplane ethernet location multicast groups  

 CHAPTER 7  
**Integrated Routing and Bridging Commands**  
interface bvi  
routed interface bvi  
show interfaces bvi  

 CHAPTER 8  
**Link Bundling Commands**  
backbone interface  
bundle lacp delay  
bundle-hash  
bundle id  
bundle load-balancing hash  
bundle load-balancing hash (EFP)  
bundle maximum-active links  
bundle minimum-active bandwidth  
bundle minimum-active links
bundle port-priority 505
bundle wait-while 507
clear lacp counters 508
interface (bundle) 509
isolation recovery-delay 510
lacp cisco enable 511
lacp churn logging 513
lacp collector-max-delay 514
lacp fast-switchover 515
lacp non-revertive 516
lacp packet-capture 517
lacp period short 519
lacp system priority 522
member neighbor 524
mlacp connect 525
mlacp iccp-group 526
mlacp node 527
mlacp port-priority 528
mlacp system mac 529
mlacp system priority 530
redundancy iccp group 531
redundancy one-way 532
show bundle 533
show bundle brief 548
show bundle load-balancing 551
show bundle replication bundle-ether 555
show iccp group 556
show lacp bundle 558
show lacp counters 560
show lacp io 562
show lacp packet-capture 565
show lacp port 568
show lacp system-id 570
show mlacp 572
show mlacp counters 574

---

### Management Ethernet Interface Commands 577

- duplex (Management Ethernet) 578
- interface MgmtEth 580
- ipv6 address autoconfig 581
- mac-address (Management Ethernet) 583
- speed (Management Ethernet) 584

---

### Multilink Commands 587

- bundle 588
- controller MgmtMultilink 589
- interface multilink 591
- multilink 593
- multilink fragment 594
- multilink group 595
- show controllers mgmtmultilink 596
- show interfaces multilink 599

---

### Packet-over-SONET Interface Commands 601

- crc (POS) 602
- encapsulation (POS) 603
- interface pos 604
- keepalive (POS) 606
- pos 608
- show interfaces pos 610
- transmit-delay 613

---

### PPP Commands 615

- clear ppp sso state 617
- clear ppp statistics 618
- encapsulation ppp 619
- group 620
- multi-router aps 621
Serial Interface Commands 669

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands

Serial Interface Commands
SONET Controller Commands  715
ais-shut (SONET)  717
ais-shut (SONET path)  718
aps group  719
aps group (global)  722
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>au</td>
<td>724</td>
</tr>
<tr>
<td>authenticate (PGP)</td>
<td>726</td>
</tr>
<tr>
<td>b3-ber-prdi</td>
<td>728</td>
</tr>
<tr>
<td>channel local</td>
<td>729</td>
</tr>
<tr>
<td>channel remote</td>
<td>731</td>
</tr>
<tr>
<td>clear counters sonet</td>
<td>733</td>
</tr>
<tr>
<td>clock source (SONET)</td>
<td>735</td>
</tr>
<tr>
<td>controller (SONET)</td>
<td>736</td>
</tr>
<tr>
<td>delay clear</td>
<td>738</td>
</tr>
<tr>
<td>delay trigger</td>
<td>739</td>
</tr>
<tr>
<td>down-when-looped</td>
<td>740</td>
</tr>
<tr>
<td>framing (SONET)</td>
<td>741</td>
</tr>
<tr>
<td>line delay clear</td>
<td>742</td>
</tr>
<tr>
<td>line delay trigger</td>
<td>743</td>
</tr>
<tr>
<td>lockout</td>
<td>744</td>
</tr>
<tr>
<td>loopback (SONET)</td>
<td>745</td>
</tr>
<tr>
<td>mode (SONET)</td>
<td>746</td>
</tr>
<tr>
<td>overhead (SONET)</td>
<td>748</td>
</tr>
<tr>
<td>overhead (SONET path)</td>
<td>750</td>
</tr>
<tr>
<td>path delay clear</td>
<td>752</td>
</tr>
<tr>
<td>path delay trigger</td>
<td>753</td>
</tr>
<tr>
<td>path (SONET)</td>
<td>754</td>
</tr>
<tr>
<td>report (SONET)</td>
<td>756</td>
</tr>
<tr>
<td>report (SONET path)</td>
<td>758</td>
</tr>
<tr>
<td>revert</td>
<td>760</td>
</tr>
<tr>
<td>scrambling disable (SONET path)</td>
<td>762</td>
</tr>
<tr>
<td>show aps</td>
<td>763</td>
</tr>
<tr>
<td>show aps agents</td>
<td>765</td>
</tr>
<tr>
<td>show aps group</td>
<td>767</td>
</tr>
<tr>
<td>show controllers pos</td>
<td>769</td>
</tr>
<tr>
<td>show controllers sonet</td>
<td>775</td>
</tr>
<tr>
<td>show sonet-local trace frr</td>
<td>782</td>
</tr>
<tr>
<td>shutdown (SONET)</td>
<td>783</td>
</tr>
<tr>
<td>signalling</td>
<td>784</td>
</tr>
</tbody>
</table>
T3, E3, T1, E1 Controller Commands on the Cisco ASR 9000 Series Router

bert e1 799
bert e3 801
bert error 803
bert interval 805
bert pattern 807
bert t1 810
bert t3 812
cablelength 814
channel-group 815
clear controller lnm 817
clear controller t1 820
clear controller t3 822
clock source (T1/E1) 824
clock source (T3/E3) 826
controller e1 828
controller e3 830
controller t1 832
controller t3 834
delay clear (T1/E1) 836
delay clear (T3/E3) 837
delay trigger (T1/E1) 838
delay trigger (T3/E3) 839
description (T1/E1) 840
description (T3/E3) 841
clear monitor-session counters 909
destination interface 910
destination pseudowire 911
mirror first 912
mirror interval 913
monitor-session 914
monitor-session (interface) 915
show monitor-session status 917
show monitor-session counters 918

CHAPTER 17 VLAN Subinterface Commands 919
dot1q vlan 920
interface (VLAN) 922

CHAPTER 18 10-Gigabit Ethernet WAN PHY Controller Commands 925
clear controller wanphy 926
clear counters wanphy 927
controller wanphy 928
report sd-ber 930
report sf-ber disable 931
show controllers wanphy 932
threshold sd-ber 938
threshold sf-ber 939
Preface

This command reference describes the Cisco IOS XR Interfaces commands. The preface for the *Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers* contains the following sections:

- Changes to This Document, on page xxi
- Communications, Services, and Additional Information, on page xxi

Changes to This Document

This table lists the technical changes made to this document since it was first released.

*Table 1: Changes to This Document*

<table>
<thead>
<tr>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 2017</td>
<td>Initial release of the cumulative command reference document that covers all updates from Release 4.3.0 onwards.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.3.2.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.4.1.</td>
</tr>
<tr>
<td>July 2018</td>
<td>Republished for Release 6.5.1.</td>
</tr>
<tr>
<td>January 2019</td>
<td>Republished for Release 6.5.2.</td>
</tr>
<tr>
<td>May 2019</td>
<td>Republished for Release 6.6.25.</td>
</tr>
</tbody>
</table>

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
• To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
Dense Wavelength Division Multiplexing Commands

This module provides command line interface (CLI) commands for configuring dense wavelength division multiplexing (DWDM) on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- admin-state, on page 3
- controller dwdm, on page 5
- g709 bdi-to-client-gais, on page 7
- g709 enable, on page 8
- g709 fec, on page 9
- g709 odu overhead tti, on page 11
- g709 odu report disable, on page 12
- g709 otu overhead tti, on page 13
- g709 otu report disable, on page 15
- g709 otu threshold, on page 17
- g709 tim-to-client-gais, on page 18
- g709 tti-processing, on page 19
- log signal, on page 20
- loopback (DWDM), on page 21
- network connection id, on page 22
- network port id, on page 23
- pm fec report enable, on page 24
- pm fec threshold, on page 25
- pm optics report enable, on page 26
- pm optics threshold, on page 28
- pm otn report enable, on page 30
- pm otn threshold, on page 33
- proactive, on page 36
- proactive revert threshold, on page 38
- proactive revert window, on page 40
- proactive trigger threshold, on page 42
• proactive trigger window, on page 44
• show controller dwdm, on page 46
• show controller dwdm pm, on page 52
• show vtp-monitored ports, on page 57
• transport-mode (WAN/OTN), on page 58
• wavelength, on page 61
admin-state

To configure the transport administration state on a DWDM port, use the `admin-state` command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the `no` form of this command.

---

**ASR 9000 64-bit (eXR) does not support the `admin-state in-service` and `admin-state out-of-service` commands.**

```
admin-state  {in-service | out-of-service}
```

**Syntax Description**

- `in-service` Places the DWDM port in In Service (IS) state, to support all normal operation.
- `out-of-service` Places the DWDM port in Out of Service (OOS) state. The laser is turned off and all traffic flow is stopped. This is the default.

**Command Default**

Out-of-service is the default transport administration state.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure `admin-state out-of-service`, the DWDM port is placed in OOS state. The laser is turned off, traffic flow is stopped, and proactive protection is disabled. However, configuration changes can still be made on the port.

**Examples**

The following example shows how to turn on the laser and place a DWDM port in In Service (IS) state:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# admin-state in-service
```

---

**Note**

This is a required configuration. The DWDM cards will not operate without this configuration.
RP/0/RSP0/CPU0:router(config-dwdm)# commit

The following example shows how to stop all operation on a DWDM port:

RP/0/RSP0/CPU0:router(config-dwdm)# commit
RP/0/RSP0/CPU0:router(config-dwdm)# admin-state out-of-service
controller dwdm

To configure a DWDM controller, use the controller dwdm command in Global Configuration mode. To return to the default state, use the no form of this command.

controller dwdm interface-path-id [vtxp-monitor]

Syntax Description

<table>
<thead>
<tr>
<th>interface-path-id</th>
<th>Physical interface or virtual interface.</th>
</tr>
</thead>
</table>

**Note**

Use the show interfaces command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

| vtxp-monitor | Enables VTXP (virtual transponder) attribute on the interface. The purpose of VTXP attribute tagging is to easily identify a set of interfaces (on which VTXP is enabled) and use them for further configuration or monitoring. |

Command Default

No default behavior or values

Command Modes

Global Configuration mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For the interface-path-id argument, use the following guidelines:

- If specifying a physical interface, the naming notation is rack/slot/module/port/subport. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number.
  - **port**: Physical port number of the interface.
  - **subport**: Physical port number of the sub-interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>
## controller dwdm

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure a DWDM controller in slot 6:

```
RP/0/RSP0/CPU0:router (config) # controller dwdm 0/6/0/0
```

```
RP/0/RSP0/CPU0:router (config) # controller dwdm 0/6/0/0 vtxn-monitor
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
<tr>
<td>show vtxn-monitored ports, on page 57</td>
<td>Displays ports on which VTXP attribute is enabled.</td>
</tr>
</tbody>
</table>
g709 bdi-to-client-gais

To insert a Generic Alarm Indication Signal (GAIS) pattern to client on the detection of a backward defect indication (BDI), use the `g709 bdi-to-client-gais` command in DWDM configuration mode. To disable this feature, use the `no` form of this command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

By default, no GAIS to client is inserted.

### Command Modes

DWDM configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure sending a Generic Alarm Indication Signal (GAIS) pattern signal to client when a BDI is received:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/6/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 bdi-to-client-gais
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 enable

To enable the ITU-T G.709 wrapper, use the **g709 enable** command in DWDM configuration mode. To disable the ITU-T G.709 wrapper, use the **no** form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The G.709 wrapper is disabled.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable the G.709 wrapper on an interface:

```
RP/0/RP0/CPU0:Router(config)# controller dwdm 0/5/0/0
RP/0/RP0/CPU0:Router(config-dwdm)# g709 enable
RP/0/RP0/CPU0:Router(config-dwdm)# admin-state in-service
```
g709 fec

To configure the Forward Error Correction (FEC) mode for the DWDM controller, use the `g709 fec` command in DWDM configuration mode. To return to the default state, use the `no` form of this command.

**Note**
ASR 9000 64-bit (eXR) does not support the `g709 disable`, `g709 enhanced<1.4>`, and `g709 standard` commands.

```
g709 fec  { [disable] | enhanced | standard | ci-bch | high-gain-sd-fec | long-haul-sd-fec }
```

**Syntax Description**
- `disable` Disables FEC.
- `enhanced` Enables ITU-T G.975.1 I.4 FEC.
- `standard` Enables standard FEC mode. This is the default.
- `ci-bch` Continuously Interleaved BCH FEC
- `high-gain-sd-fec` 7% CISCO SD FEC.
- `long-haul-sd-fec` 20% CISCO SD FEC.

**Command Default**
Standard FEC mode is enabled by default.

**Command Modes**
DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.1</td>
<td>The <code>ci-bch</code> keyword was introduced.</td>
</tr>
<tr>
<td>Release 5.3.2</td>
<td>The high-gain-sd-fec and long-haul-sd-fec keywords were introduced on the A9K-400G-DWDM-TR line card.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**
The enhanced FEC mode supported on the Cisco CRS Router (ITU-T G.975.1 I.7) and the Cisco ASR 9000 Series Router (ITU-T G.975.1 I.4) are different and therefore, incompatible. To support interoperability of DWDM between these routers, standard FEC must be configured.

The `g709 fec` command can be used only when the DWDM controller port is in the out-of-service administrative state. You stop operation using the `admin-state out-of-service` command.

The G.709 wrapper must be enabled to enable forward error correction (FEC) mode on the controller.

Standard FEC is the default mode; therefore, if you use the `no g709 fec` command, standard FEC is used.
To display the FEC mode, use the `show controller dwdm` command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure the FEC mode on a DWDM controller:

```plaintext
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/6/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# admin-state out-of-service
RP/0/RSP0/CPU0:router(config-dwdm)# commit

RP/0/RSP0/CPU0:router(config-dwdm)# g709 fec standard
RP/0/RSP0/CPU0:router(config-dwdm)# commit
RP/0/RSP0/CPU0:router(config-dwdm)# admin-state in-service
RP/0/RSP0/CPU0:router(config-dwdm)# commit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-state, on page 3</td>
<td>Configures the transport administration state on a DWDM port.</td>
</tr>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
<tr>
<td>g709 bdi-to-client-gais, on page 7</td>
<td>Inserts a GAIS pattern to client on the detection of a BDI.</td>
</tr>
</tbody>
</table>
To configure the Trail Trace Identifier (TTI) level for an Optical Channel Data Unit (ODU), use the `g709 odu overhead tti` command in DWDM configuration mode. To return to the default, use the `no` form of this command.

```
g709 odu overhead tti {expected | sent} {ascii | hex} tti-string
```

**Syntax Description**
- **expected**: Configures the expected TTI string.
- **sent**: Configures the transmit TTI string.
- **ascii**: Indicates that the string is in ASCII format.
- **hex**: Indicates that the string is in hexadecimal format.
- **tti-string**: The TTI level string. You can configure the TTI level string in ASCII string format or hexadecimal format. The ASCII text string can be a maximum of 64 characters. The hexadecimal string length must be an even number and can be a maximum of 128 bytes.

**Command Default**
No TTI level string is configured.

**Command Modes**
DWDM configuration

**Command History**
- **Release 3.9.0**: This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Examples**
The following example shows how to configure the expected TTI string:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 odu overhead tti expected test OTU 5678
```

**Related Commands**
- **Command**: `show controller dwdm`, on page 46
- **Description**: Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.
g709 odu report disable

To disable the logging of selected Optical Channel Data Unit (ODU) alarms to the console for a DWDM controller, use the `g709 odu report disable` command in DWDM configuration mode. To return to the default state, use the `no` form of this command.

```
g709 odu report {ais | bdi | lck | oci | ptim | tim} disable
```

**Syntax Description**
- `ais`  Alarm indication signal reporting status.
- `bdi`  Backward defect indication reporting status.
- `lck`  Upstream connection locked reporting status.
- `oci`  Open connection indication error reporting status.
- `ptim` Payload type identifier mismatch reporting status.
- `tim`  Set Trace Identifier Mismatch reporting status.

**Command Default**
Reporting is enabled for all keywords.

**Command Modes**
- DWDM configuration

**Command History**
- **Release** Modification
  - Release 3.9.0  This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
| Task ID | Operations 
|---------|---------------
| dwdm    | read, write  |

**Examples**
This example shows how to disable ODU reporting for OCI:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 odu report oci disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller dwdm</code>, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 otu overhead tti

To configure the OTU Trail Trace Identifier (TTI) buffer for a DWDM controller, use the **g709 otu overhead tti** command in DWDM configuration mode. To return to the default state, use the **no** form of this command.

**Note**

ASR 9000 64-bit (eXR) does not support the **g709 otu overhead tti sent ascii LINE** and **g709 otu overhead tti sent hex LINE** commands.

```
g709 otu overhead tti {expected | sent} {ascii | hex} tti-string
```

**Syntax Description**

- expected: Configures the expected TTI string.
- sent: Configures the transmit TTI string.
- ascii: Indicates that the string is in ASCII format.
- hex: Indicates that the string is in hexadecimal format.
- tti-string: The TTI string. A maximum of 64 characters is allowed.

**Command Default**

No TTI string is configured

**Command Modes**

DWDM configuration

**Command History**

- **Release 3.9.0**: This command was introduced.

**Usage Guidelines**

To display the TTI strings, use the **show controller dwdm g709** command.

**Task ID**

- **Task ID**: read, write

**Examples**

The following example shows how to configure the expected TTI string:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 otu overhead tti expected test OTU 5678
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 otu report disable

To disable the logging of selected Optical Channel Transport Unit (OTU) alarms to the console for a DWDM controller, use the `g709 otu report disable` command in DWDM configuration mode. To return to the default state, use the `no` form of this command.

```
g709 otu report {bdi | fecmismatch | iae | lof | lom | los | sd-ber | sf-ber | tim} disable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bdi</td>
<td>Backward defect indication reporting status.</td>
</tr>
<tr>
<td>fecmismatch</td>
<td>FEC mismatch alarm reporting status.</td>
</tr>
<tr>
<td>iae</td>
<td>Incoming alignment error reporting status.</td>
</tr>
<tr>
<td>lof</td>
<td>OTU loss of frame reporting status.</td>
</tr>
<tr>
<td>lom</td>
<td>Loss of multiple frame reporting status.</td>
</tr>
<tr>
<td>los</td>
<td>Loss of signal reporting status.</td>
</tr>
<tr>
<td>sd-ber</td>
<td>SM bit error rate (BER) is in excess of the signal degradation BER threshold.</td>
</tr>
<tr>
<td>sf-ber</td>
<td>SM BER is in excess of the signal failure BER threshold.</td>
</tr>
<tr>
<td>tim</td>
<td>Trace Identifier Mismatch reporting status.</td>
</tr>
</tbody>
</table>

**Note**

FEC mismatch alarm is deprecated.

**Command Default**

Reporting is enabled for all keywords.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configuring two ends of an OTN link with different FEC modes is not supported. Even if different FEC modes are configured, the FEC mismatch alarm will not be raised. Interface may experience continuous port flap in addition to continuous bit interleaved parity (BIP) errors at both OTN and LAN level.

**Task ID**

```
Task ID  Operations
dwdm     read, write
```

**Examples**

The following example shows how to disable OTU reporting for IAE:
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 otu report iae disable

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 otu threshold

To configure thresholds for selected Optical Channel Transport Unit (OTU) bit error rate (BER) alarms, use the `g709 otu threshold` command in DWDM configuration mode. To return to the default state, use the no form of this command.

```
g709 otu threshold {sd-ber | sf-ber} bit-error-rate
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sd-ber bit-error-rate</strong></td>
<td>Signal degradation bit error rate (BER) in the range 1 to 9, where <code>bit-error-rate</code> specifies a negative exponent of base 10 (10–bit-error-rate). The default is 6 (10–6).</td>
</tr>
<tr>
<td><strong>sf-ber bit-error-rate</strong></td>
<td>Signal failure BER above threshold in the range 1 to 9, where <code>bit-error-rate</code> specifies a negative exponent of base 10 (10–bit-error-rate). The default is 3 (10–3).</td>
</tr>
</tbody>
</table>

**Command Default**

The default bit error rate for `sd-ber` is 6.
The default bit error rate for `sf-ber` is 3.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the signal fail BER rate to be 5:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 otu threshold sf-ber 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller dwdm</code>, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 tim-to-client-gais

To insert a Generic Alarm Indication Signal (GAIS) on the client side when a Trace Identifier Mismatch (TIM) is detected, use the **g709 tim-to-client-gais** command in DWDM configuration mode. To disable this feature, use the **no** form of this command.

**g709 tim-to-client-gais**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

By default, no GAIS to client is inserted.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a GAIS to client when a TIM is received:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# g709 tim-to-client-gais
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show controller dwdm, on page 46</strong></td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
g709 tti-processing

To enable Trace Identifier Mismatch (TIM) alarms, use the **g709 tti-processing** command in DWDM configuration mode. To disable TIM alarms, use the **no** form of this command.

---

**Note**

ASR9000 64-bit (eXR) does not support the **g709 tti-processing** command.

---

**g709 tti-processing**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

By default, trace identifier mismatch (TIM) alarms are disabled.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Trace identifier mismatch (TIM) alarms can be set only when TTI processing is enabled.

---

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the expected TTI string:

```
RP/0/RSP0/CPU0:router(config) # controller dwdm 0/1/0/0
RP/0/RSP0/CPU0:router(config-dwdm) # g709 tti-processing
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
log signal

To enable 10 millisecond proactive monitoring of Forward Error Correction-Fast Re-Route (FEC-FRR), use the log signal command in DWDM configuration mode. To disable proactive monitoring, use the no form of this command.

```
log signal file-name
```

**Syntax Description**

`file-name` Specifies the name of the log file.

**Command Default**

No default behavior or values

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

**Note**

The log signal command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the `show controller dwdm proactive status` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable 10 millisecond proactive monitoring of Forward Error Correction-Fast Re-Route (FEC-FRR).

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# log signal LogFile1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
loopback (DWDM)

To configure the DWDM controller for loopback mode, use the `loopback` command in DWDM configuration mode. To remove the loopback DWDM command from the configuration file, use the `no` form of this command.

**Note**

ASR 9000 64-bit (eXR) does not support the `loopback` command.

```
loopback {internal | line}
```

**Syntax Description**

- **internal**: Specifies that all the packets be looped back to the router.
- **line**: Specifies that the incoming network packets be looped back to the DWDM network.

**Command Default**

This command is disabled by default.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The DWDM controller supports two loopback operation modes for diagnostic purposes: internal and line. The terminal (internal) loopback mode allows the received data from the Layer 2 Framer (for example, a SONET/SDH framer for POS or Ethernet MAC for 10GE) of the PLIM to be looped back to the ingress side of the Framer. This allows the packets to be looped back to the PLIM. The line loopback mode allows the received trunk/DWDM line Rx to be connected to the trunk/DWDM line Tx towards the line. This is used for line diagnostics.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, all packets are looped back to the DWDM controller:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# loopback internal
```
network connection id

To configure a connection identifier for the Multi Service Transport Protocol (MSTP), use the `network connection id` command in DWDM configuration mode. To remove a connection identifier, use the no form of this command.

```
network connection id  id-number
```

**Syntax Description**
- `id-number` Connection identifier.

**Command Default**
No default behavior or values

**Command Modes**
DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure a connection identifier for the Multi Service Transport Protocol (MSTP).

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# network connection id 1/1/1/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network port id, on page 23</td>
<td>Assigns an identifier number to a port for the MSTP.</td>
</tr>
</tbody>
</table>
network port id

To assign an identifier number to a port for the Multi Service Transport Protocol (MSTP), use the `network port id` command in DWDM configuration mode. To remove an identifier number from a port, use the no form of this command.

```
network port id id-number
```

**Syntax Description**

- `id-number` Port identifier.

**Command Default**

No default behavior or values

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID Operations
-------- --------
dwdm    read, write
```

**Examples**

The following example shows how to assign an identifier number to a port for the Multi Service Transport Protocol (MSTP):

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# network port id 1/0/1/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network connection id, on page 22</td>
<td>Configures a connection identifier for the MSTP.</td>
</tr>
</tbody>
</table>
pm fec report enable

To enable Threshold Crossing Alert (TCA) generation for FEC, use the `pm fec report enable` command in DWDM configuration mode. To disable TCAs, use the `no` form of this command.

```
pm {15-min | 24-hour} fec report {ec-bits | uc-words} enable
```

**Syntax Description**

- **15-min**: Configures the TCA generation for 15-minute intervals.
- **24-hour**: Configures TCA generation for 24-hour intervals.
- **ec-bits**: Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
- **uc-words**: Uncorrectable words. This is the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.

**Command Default**

TCA is not enabled.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display FEC performance measurement information, use the `show controller dwdm pm fec` command.

**Examples**

The following example shows how to enable TCAs in FEC reporting for uncorrectable words:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min fec report uc-words enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller dwdm</code>, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
**pm fec threshold**

To configure performance monitoring thresholds on the FEC layer, use the `pm fec threshold` command in DWDM configuration mode. To return to the default state, use the `no` form of this command.

```
pm {15-min | 24-hour} fec threshold {ec-bits | uc-words} threshold
```

**Syntax Description**

- **pm 15-min fec threshold ec-bits threshold**: Configures the performance monitoring thresholds for 15-minute intervals. Denotes the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
- **pm 24-hour fec threshold uc-words threshold**: Configures performance monitoring thresholds for 24-hour intervals. Denotes the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
- **threshold**: Threshold for the performance monitoring parameter in the range 1–4294967295.

**Command Default**

No threshold is configured.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display performance measurement information for the FEC layer, use the `show controller dwdm pm fec` command.

**Task ID**

- **Task ID**
  - **Operations**
    - **dwdm**: read, write

**Examples**

The following example shows how to configure an FEC layer performance monitoring threshold for uncorrectable words:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min fec threshold uc-words 2000000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controller dwdm pm</code>, on page 52</td>
<td>Displays performance monitoring information for a DWDM controller.</td>
</tr>
</tbody>
</table>
pm optics report enable

To enable Threshold Crossing Alert (TCA) generation on the optics layer, use the `pm optics report enable` command in DWDM configuration mode. To disable TCA reporting, use the `no` form of this command.

```
pm {15-min | 24-hour} optics report {lbc | opr | opt} {max-tca | min-tca} enable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-min</td>
<td>Configures TCA generation for 15-minute intervals.</td>
</tr>
<tr>
<td>24-hour</td>
<td>Configures TCA generation for 24-hour intervals.</td>
</tr>
<tr>
<td>lbc</td>
<td>Laser bias current.</td>
</tr>
<tr>
<td>opr</td>
<td>Optical power on the unidirectional port.</td>
</tr>
<tr>
<td>opt</td>
<td>Transmit optical power in dBm.</td>
</tr>
<tr>
<td>max-tca</td>
<td>Indicates that the maximum value of the parameter is compared against the threshold to determine if a TCA should be generated.</td>
</tr>
<tr>
<td>min-tca</td>
<td>Indicates that the minimum value of the parameter is compared against the threshold to determine if a TCA should be generated.</td>
</tr>
</tbody>
</table>

**Command Default**

TCA reporting is not enabled.

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display performance monitoring information for the optics, use the `show controller dwdm pm optics` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable TCA reporting on the optics layer reporting for the maximum OPT:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min optics report opt max-tca enable
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show controller dwdm pm</code>, on page 52</td>
<td>Displays performance monitoring information for a DWDM controller.</td>
</tr>
</tbody>
</table>
pm optics threshold

To configure performance monitoring thresholds on the optics layer, use the pm optics threshold command in DWDM configuration mode. To return to the default state, use the no form of this command.

```
pm {15-min | 24-hour} optics threshold {lbc | opr | opt} {max | min} threshold
```

**Syntax Description**
- **15-min**: Configures the performance monitoring thresholds for 15-minute intervals.
- **24-hour**: Configures performance monitoring thresholds for 24-hour intervals.
- **lbc**: Laser bias current.
- **opr**: Optical power on the unidirectional port.
- **opt**: Transmit optical power in dBm.
- **max**: Indicates that the threshold is for the maximum value of the parameter.
- **min**: Indicates that the threshold is for the minimum value of the parameter.
- **threshold**: Threshold for the performance monitoring parameter.

**Command Default**
No thresholds are configured.

**Command Modes**
DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To display performance monitoring information for the optics layer, use the `show controller dwdm pm optics` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure an optics layer performance monitoring threshold for maximum OPT:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min optics threshold opt max 2000000
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show controller dwdm pm, on page 52</code></td>
<td>Displays performance monitoring information for a DWDM controller.</td>
</tr>
</tbody>
</table>
pm otn report enable

To enable Threshold Crossing Alert (TCA) generation on the Optical Transport Network (OTN) layer, use the `pm otn report enable` command in DWDM configuration mode. To disable TCA reporting, use the `no` form of this command.

```
pm {15-min | 24-hour} otn report otn-parameter enable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-min</td>
<td>Configures TCA generation for 15-minute intervals.</td>
</tr>
<tr>
<td>24-hour</td>
<td>Configures TCA generation for 24-hour intervals.</td>
</tr>
</tbody>
</table>

**otn-parameter** Specific parameter for which to configure the threshold. OTN parameters can be as follows:

- **bbe-pm-fe**—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval.
- **bbe-pm-ne**—Near-end path monitoring background block errors (BBE-PM).
- **bbe-sm-fe**—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval.
- **bbe-sm-ne**—Near-end section monitoring background block errors (BBE-SM).
- **bber-pm-fe**—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval.
- **bber-pm-ne**—Near-end path monitoring background block errors ratio (BBER-PM).
- **bber-sm-fe**—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval.
- **bber-sm-ne**—Near-end section monitoring background block errors ratio (BBER-SM)
- **es-pm-fe**—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval.
- **es-pm-ne**—Near-end path monitoring errored seconds (ES-PM).
- **es-sm-fe**—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval.
- **es-sm-ne**—Near-end section monitoring errored seconds (ES-SM).
- **esr-pm-fe**—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.
- **esr-pm-ne**—Near-end path monitoring errored seconds ratio (ESR-PM).
- **esr-sm-fe**—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
- **esr-sm-ne**—Near-end section monitoring errored seconds ratio (ESR-SM).
- **fc-pm-fe**—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval.
- **fc-pm-ne**—Near-end path monitoring failure counts (FC-PM).
- **fc-sm-fe**—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval.
- **fc-sm-ne**—Near-end section monitoring failure counts (FC-SM).
- **ses-pm-fe**—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval.
- **ses-pm-ne**—Far-end path monitoring severely errored seconds (SES-PM).
- **ses-sm-fe**—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval.
- **ses-sm-ne**—Near-end section monitoring severely errored seconds (SES-SM).
- **sesr-pm-fe**—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval.
- **sesr-pm-ne**—Near-end path monitoring severely errored seconds ratio (SESR-PM).
- **sesr-sm-fe**—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval.
- **sesr-sm-ne**—Near-end section monitoring severely errored seconds ratio (SESR-SM).
- **uas-pm-fe**—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval.
- **uas-pm-ne**—Near-end path monitoring unavailable seconds (UAS-PM).
- **uas-sm-fe**—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval.
- **uas-sm-ne**—Near-end section monitoring unavailable seconds (UAS-SM).

### Command Default

TCA generation is not enabled.

### Command Modes

DWDM configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To display performance measurement information for the OTN layer, use the `show controller dwdm pm otn` command.
The following example shows how to enable TCA generation on the OTN layer reporting for the path monitoring errored seconds ratio (ESR-PM):

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min otn report esr-pm-fe enable
```
pm otn threshold

To configure performance monitoring thresholds on the optical transport network (OTN) layer, use the `pm otn threshold` command in DWDM configuration mode. To disable TCA reporting, use the `no` form of this command.

`pm {15-min | 24-hour} otn threshold otn-parameter enable`

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-min</td>
<td>Configures performance monitoring thresholds for 15-minute intervals.</td>
</tr>
<tr>
<td>24-hour</td>
<td>Configures performance monitoring thresholds for 24-hour intervals.</td>
</tr>
</tbody>
</table>

**otn-parameter**

Specific parameter for which to configure the threshold. OTN parameters can be as follows:

- **bbe-pm-fe**—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval.
- **bbe-pm-ne**—Near-end path monitoring background block errors (BBE-PM).
- **bbe-sm-fe**—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval.
- **bbe-sm-ne**—Near-end section monitoring background block errors (BBE-SM).
- **bber-pm-fe**—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval.
- **bber-pm-ne**—Near-end path monitoring background block errors ratio (BBER-PM).
- **bber-sm-fe**—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval.
- **bber-sm-ne**—Near-end section monitoring background block errors ratio (BBER-SM)
- **es-pm-fe**—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval.
- **es-pm-ne**—Near-end path monitoring errored seconds (ES-PM).
- **es-sm-fe**—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval.
- **es-sm-ne**—Near-end section monitoring errored seconds (ES-SM).
• **esr-pm-fe**—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.

• **esr-pm-ne**—Near-end path monitoring errored seconds ratio (ESR-PM).

• **esr-sm-fe**—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval.

• **esr-sm-ne**—Near-end section monitoring errored seconds ratio (ESR-SM).

• **fc-pm-fe**—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval.

• **fc-pm-ne**—Near-end path monitoring failure counts (FC-PM).

• **fc-sm-fe**—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval.

• **fc-sm-ne**—Near-end section monitoring failure counts (FC-SM).

• **ses-pm-fe**—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval.

• **ses-pm-ne**—Far-end path monitoring severely errored seconds (SES-PM).

• **ses-sm-fe**—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval.

• **ses-sm-ne**—Near-end section monitoring severely errored seconds (SES-SM).

• **sesr-pm-fe**—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval.

• **sesr-pm-ne**—Near-end path monitoring severely errored seconds ratio (SESR-PM).

• **sesr-sm-fe**—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval.

• **sesr-sm-ne**—Near-end section monitoring severely errored seconds ratio (SESR-SM).

• **uas-pm-fe**—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval.

• **uas-pm-ne**—Near-end path monitoring unavailable seconds (UAS-PM).

• **uas-sm-fe**—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval.

• **uas-sm-ne**—Near-end section monitoring unavailable seconds (UAS-SM).

**Threshold for the performance monitoring parameter.**

**Command Default**
No thresholds are configured.

**Command Modes**
DWDM configuration
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To display performance measurement information for the OTN layer, use the `show controller dwdm pm otn` command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure an OTN layer performance monitoring threshold for path monitoring errored seconds ratio (ESR-PM):

```
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/0/0/0
RP/0/RSP0/CPU0:router(config-dwdm)# pm 15-min otn threshold esr-pm-ne 500000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm pm, on page 52</td>
<td>Displays performance monitoring information for a DWDM controller.</td>
</tr>
</tbody>
</table>
**proactive**

To enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR), use the `proactive` command in DWDM configuration mode. To disable automatic triggering, use the `no` form of this command.

---

**Note**

ASR 9000 64-bit (eXR) does not support the `proactive` command.

---

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
| Release 4.2.3 | Support for Proactive protection feature was included on these Modular Port Adaptors (MPAs):  
  - A9K-MPA-2X40GE  
  - A9K-MPA-1X40GE |

**Usage Guidelines**

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

---

**Note**

The `proactive` command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the `show controller dwdm proactive status` command.

---

**Task ID**

**Task ID**

<table>
<thead>
<tr>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR):

```plaintext
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# proactive
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show controller dwdm, on page 46</code></td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
proactive revert threshold

To configure the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route, use the proactive revert threshold command in DWDM configuration mode. To remove the revert threshold, use the no form of this command.

Note

ASR 9000 64-bit (eXR) does not support the proactive revert threshold <1-9> <3-10> command.

Syntax Description

proactive revert threshold  x-coefficient  y-power

x-coefficient  Bit error rate coefficient (x of xE-y). The range is 1 to 9. Default is 1.

y-power  Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

No default behavior or values

Command Modes

DWDM configuration

Command History

Release 4.0.0  This command was introduced.

Release 4.2.3  Support for proactive revert threshold command was included on these Modular Port Adaptors (MPAs):

- A9K-MPA-2X40GE
- A9K-MPA-1X40GE

Usage Guidelines

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

Note

The proactive revert threshold command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the show controller dwdm proactive status command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure the revert threshold for FEC-FRR:
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# proactive revert threshold 1 9

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
**proactive revert window**

To configure the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered, use the **proactive revert window** command in DWDM configuration mode. To remove the revert window, use the **no** form of this command.

**Note**

ASR 9000 64-bit (eXR) does not support the **proactive revert window <500-100000>** command.

**Syntax Description**

```
proactive revert window  window
```

- **window** The length of time (in milliseconds) of the window in which reverting from FEC-FRR may be triggered. The range is 2000 to 100000.

**Command Default**

No default behavior or values

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Support for proactive protection was included on these Modular Port Adaptors (MPAs):</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-2X40GE</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-1X40GE</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

**Note**

The **proactive revert window** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the window in which reverting from FEC-FRR may be triggered:
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# proactive revert window 100000

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
<td></td>
</tr>
</tbody>
</table>
proactive trigger threshold

To configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive trigger threshold** command in DWDM configuration mode. To remove the trigger threshold, use the no form of this command.

**Note**

ASR 9000 64-bit (eXR) does not support the **proactive trigger threshold** <1-9> <2-9> command.

**proactive trigger threshold** x-coefficient y-power

**Syntax Description**

- **x-coefficient** Bit error rate coefficient (x of xE-y). The range is 1 to 9. Default is 1.
- **y-power** Bit error rate exponent (y of xE-y). The range is 3 to 9.

**Command Default**

No default behavior or values

**Command Modes**

DWDM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Support for <strong>proactive trigger threshold</strong> command was included on these Modular Port Adaptors (MPAs):</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-2X40GE</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-1X40GE</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

**Note**

The **proactive trigger threshold** command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the **show controller dwdm proactive status** command.

**Task ID**

| Task ID Operations |
|-------------------|------------------|
| dwdm read,        | write            |

**Examples**

The following example shows how to configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR)
Dense Wavelength Division Multiplexing Commands

RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# proactive trigger threshold 1 9

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
**proactive trigger window**

To configure the trigger window (in milliseconds) in which Fast Re-Route may be triggered, use the `proactive trigger window` command in DWDM configuration mode. To remove the trigger window, use the no form of this command.

---

**Note**

ASR 9000 64-bit (eXR) does not support the `proactive trigger window <10-10000>` command.

---

**Syntax Description**

| window | The length of time (in milliseconds) of the window in which FEC-FRR may be triggered. The range is 10 to 10000. |

---

**Command Default**

No default behavior or values

---

**Command Modes**

DWDM configuration

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Support for <code>proactive trigger window</code> command was included on these Modular Port Adaptors (MPAs):</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-2X40GE</td>
</tr>
<tr>
<td></td>
<td>• A9K-MPA-1X40GE</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The proactive feature is used to trigger Forward Error Correction-Fast Re-Route (FEC-FRR).

---

**Note**

The `proactive trigger window` command is supported on the legacy line cards but does not function on the A9K-8X100GE-SE line cards though it is supported on them.

To see the proactive status, use the `show controller dwdm proactive status` command.

---

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to configure the trigger window (in milliseconds) in which triggering of Fast Re-Route may happen:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller dwdm 0/1/0/1
RP/0/RSP0/CPU0:router(config-dwdm)# proactive trigger window 10000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller dwdm, on page 46</td>
<td>Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.</td>
</tr>
</tbody>
</table>
show controller dwdm

To display optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller, use the show controller dwdm command in EXEC mode.

```
show controller dwdm interface-path-id [g709 [registers] | log | optics | wavelength-map]
```

**Syntax Description**
- `interface-path-id` Physical interface or virtual interface.
- `g709` (Optional) Displays the G.709 Optical Transport Network (OTN) protocol alarms and counters for bit errors, along with the FEC statistics and threshold-based alerts. g709 mode and g709 fec set to enhanced by default.
- `log` (Optional) Displays information about signal logging.
- `optics` (Optional) Displays optical related information about the interface, such as output power level and wavelength.
- `registers` (Optional) For g709, displays platform-specific OTN framer registers; for optics, displays transponder registers.
- `tdc` (Optional) Displays tunable dispersion compensator (TDC) information.
- `wavelength-map` (Optional) Displays the wavelength information.

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**
- **Release 3.9.0** This command was introduced.
- **Release 5.3.1** g709 standard FEC mode is enabled by default.

**Usage Guidelines**
DWDM interfaces with g709 capability(enabled) and FEC(enabled) would report with Threshold Crossing Alerts (TCA) for Error Correction based PREFEC version of SD and SF BER. The thresholds act independent of FRR thresholds. If FRR is also enabled, then PREFEC thresholds are expected to be manually tuned to provide an early warning before the protection is triggered. The information regarding PREFEC_SD and PREFEC_SF are made available for the show controller dwdm interface-path-id g709 command. 10 GigE and 40 GigE DWDM interfaces support standard FEC and enhanced i.4 and i.7 FEC modes while 100GigE supports standard FEC.
**Examples**

This example shows sample output from the `show controllers dwdm g709` command when FEC and g709 are both active:

```
RP/RSP0/CPU0:Router# show controller dwdm 0/5/0/0 g709
Mon Feb 10 13:12:00.268 IST

G709 Status

OTU
- LOS = 0
- LOF = 0
- LOM = 0
- BDI = 0
- IAE = 1
- BIP = 0
- BEI = 0
- TIM = 0

ODU
- AIS = 0
- BDI = 0
- OCI = 0
- LCK = 0
- BIP = 0
- BEI = 0
- PTIM = 0
- TIM = 0

FEC Mode: Enhanced (Default)
- EC (current second) = 0
- EC = 0
- UC = 0
- PREFEC BER < 9.01E-11
- Q > 6.46
- Q Margin > 7.26

Detected Alarms: None
Asserted Alarms: None
Alarm Reporting Enabled for: LOS LOF LOM IAE OTU-BDI OTU-TIM OTU_SD_BER PREFEC_SD_BER PREFEC_SF_BER ODU-AIS ODU-BDI OCI LCK PTIM ODU-TIM ODU_SF_BER ODU_SD_BER
FECMISMATCH

BER Thresholds: preFEC-SF = E-9 preFEC-SD = E-11
- OTU-SF = E-3
- OTU-SD = E-6
- ODU-SF = E-3
- ODU-SD = E-6

Connectivity Info
- Network Port ID: Not Configured
- Network Connection ID: Not Configured

OTU TTI Sent  String ASCII : Tx TTI Not Configured
OTU TTI Received String ASCII : Rx TTI Not Received
OTU TTI Expected String ASCII : Exp TTI Not Configured

ODU TTI Sent  String ASCII : Tx TTI Not Configured
ODU TTI Received String ASCII : Rx TTI Not Received
ODU TTI Expected String ASCII : Exp TTI Not Configured
```
This table describes selected fields from the `show controllers dwdm` command output.

**Table 2: show controllers dwdm Command Output Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Number of alarm indication signal (AIS) alarms. AIS is a signal sent downstream as an indication that an upstream defect has been detected.</td>
</tr>
<tr>
<td>Alarm reporting enabled for</td>
<td>Lists the alarms that are enabled for reporting.</td>
</tr>
<tr>
<td>Asserted Alarms</td>
<td>Alarms indicated to be reported by the user.</td>
</tr>
<tr>
<td>BDI</td>
<td>Number of backward defect indication (BDI) alarms. The BDI is a single bit that conveys information regarding signal failure in the upstream direction.</td>
</tr>
<tr>
<td>BER thresholds</td>
<td>Values of the configured bit error rate thresholds.</td>
</tr>
<tr>
<td>BIP</td>
<td>Number of bit interleaved parity alarms. The BIP is comprised of one byte and is used for error detection. It is computed over the entire optical channel payload unit (OPU).</td>
</tr>
<tr>
<td>Controller State</td>
<td>Status of the controller.</td>
</tr>
<tr>
<td>Detected Alarms</td>
<td>Alarms detected by the hardware.</td>
</tr>
<tr>
<td>EC</td>
<td>Corrected code words. This is the number of words corrected by the FEC and is displayed as a per second rate.</td>
</tr>
<tr>
<td>FEC Mode</td>
<td>Indicates the forward error correction (FEC) mode for the controller. This can be Disabled, Enhanced FEC G.975.1 1.4, or Standard FEC (Default).</td>
</tr>
<tr>
<td>IAE</td>
<td>Number of incoming alignment errors (IAE).</td>
</tr>
<tr>
<td>LCK</td>
<td>Number of upstream connection locked alarms. LCK is a signal sent downstream as an indication that upstream the connection is locked, and no signal is passed through.</td>
</tr>
<tr>
<td>LOF</td>
<td>Number of OTU loss of frame (LOF) alarms.</td>
</tr>
<tr>
<td>LOM</td>
<td>Number of OTU loss of multiframe (LOM) alarms.</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status. Indicates whether or not loopback is enabled and the type of loopback enabled.</td>
</tr>
<tr>
<td>LOS</td>
<td>Number of OTU loss of signal (LOS) alarms. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.</td>
</tr>
<tr>
<td>OCI</td>
<td>Number of open connection indication alarms. OCI is a signal sent downstream as an indication that upstream the signal is not connected to a trail termination source.</td>
</tr>
<tr>
<td>ODU</td>
<td>Optical channel data unit alarms.</td>
</tr>
<tr>
<td>OTU</td>
<td>Optical transport unit overhead alarms.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
OTU TTI Expected | Value of the expected TTI.
OTU TTI Received | Value of the received TTI.
OTU TTI Sent | Value of the transmit trail trace identifier (TTI).
PTIM | Number of payload type identifier mismatch alarms. This occurs when there is a mismatch between the way the ITU-T G.709 option is configured on the PLIM at each end of the optical span.
TDC Info | Tunable Dispersion Compensator (TDC) information.
Transport Admin State | Current status of the port as set by the admin-state command. Possible values are: IS (In-Service) and OOS (Out-of-Service).
UC | Uncorrectable code words. This is a raw counter.
Pre-FEC BER | Pre - bit error rate (BER) forward error correction (FEC). The pre-FEC BER is calculated using pre-forward error correction (FEC) error counts.
Q | The general signal quality bit error rate (BER) per voltage. The Q and Q margin are calculated using the Pre-FEC BER.
Q Margin | The general signal quality bit error rate (BER) per voltage. The Q and Q margin are calculated using the Pre-FEC BER.
Operational Mode | Indicates whether the tunable dispersion compensator (TDC) operational mode option is set to Auto or Manual.
Status | Indicates whether the tunable dispersion compensator (TDC) is in the acquiring state or locked state. The status is invalid if there is a major alarm.
Dispersion Setting | Indicates a value between –700 and +700 packets per second (pps). The dispersion setting is read from the optics module after the tunable dispersion compensator (TDC) has locked.
Reroute Control | Not used.
Reroute BER | Not used.

See Table 3: show controllers dwdm optics Command Output Field Descriptions, on page 50 for a description of the optics fields.

The following example shows the output from the `show controllers dwdm` command with the `optics` keyword:

```
RP0/RSP0/CPU0:router# show controllers dwdm 0/2/0/0 optics
Mon Jul 12 21:04:29.254 UTC
Optics Status

  Optics Type: 10GBASE-ZR,
  Wavelength Info: C-Band, MSA ITU Channel= N/A, Frequency=192THz, Wavelength=1558nm
```
TX Power = 1.50 dBm  
RX Power = -11.86 dBm

This table describes selected fields from the `show controllers dwdm` command output with the `optics` keyword.

### Table 3: `show controllers dwdm optics` Command Output Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optics Type</td>
<td>Indicates the optics type: GE or OC-768c/STM-256c DWDM.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Indicates whether the clock is internal or line.</td>
</tr>
<tr>
<td>Wavelength Band</td>
<td>Indicates the wavelength band: C-band or L-band.</td>
</tr>
<tr>
<td>MSA ITU Channel</td>
<td>Multi Source Agreement (MSA) ITU channel number.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Frequency of the channel in terahertz.</td>
</tr>
<tr>
<td>Wavelength</td>
<td>Wavelength corresponding to the channel number in nanometers.</td>
</tr>
<tr>
<td>TX power</td>
<td>Value of the transmit power level.</td>
</tr>
<tr>
<td>RX Power</td>
<td>Actual optical power at the RX port.</td>
</tr>
<tr>
<td>RX LOS Threshold</td>
<td>Receive loss of signal threshold. If the receive optical power is less than or equal to this threshold, the optical LOS alarm is raised.</td>
</tr>
</tbody>
</table>

This example shows sample output from the `show controllers dwdm` command with the `wavelength-map` keyword on a Gigabit Ethernet controller:

```
RP/0/RSP0/CPU0:router# show controller dwdm 0/5/0/3 wavelength-map
Wavelength band: C-band
MSA ITU channel range supported: 3-84

Wavelength map table
-------------------------------
<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (THz)</th>
<th>Wavelength (nm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>196.00</td>
<td>1529.553</td>
</tr>
<tr>
<td>04</td>
<td>195.95</td>
<td>1529.944</td>
</tr>
<tr>
<td>05</td>
<td>195.90</td>
<td>1530.334</td>
</tr>
<tr>
<td>06</td>
<td>195.85</td>
<td>1530.725</td>
</tr>
<tr>
<td>07</td>
<td>195.80</td>
<td>1531.116</td>
</tr>
<tr>
<td>08</td>
<td>195.75</td>
<td>1531.507</td>
</tr>
<tr>
<td>09</td>
<td>195.70</td>
<td>1531.898</td>
</tr>
<tr>
<td>10</td>
<td>195.65</td>
<td>1532.290</td>
</tr>
<tr>
<td>11</td>
<td>195.60</td>
<td>1532.681</td>
</tr>
</tbody>
</table>
```

Dense Wavelength Division Multiplexing Commands
This table describes selected fields from the `show controllers dwdm` command output with the `wavelength-map` keyword.

### Table 4: `show controllers dwdm wavelength` Command Output Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channelNum</td>
<td>Channel number.</td>
</tr>
<tr>
<td>frequency(THz)</td>
<td>Frequency of the wavelength in terahertz.</td>
</tr>
<tr>
<td>wavelength(nm)</td>
<td>Wavelength in nanometers.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-state, on page 3</td>
<td>Configures the transport administration state on a DWDM port.</td>
</tr>
</tbody>
</table>
show controller dwdm pm

To display performance monitoring information for a DWDM controller, use the `show controller dwdm pm` command in EXEC mode.

```
show controller dwdm  instance  pm history  [{15-min | 24-hour | fec | optics | otn}]
show controller dwdm  instance  pm interval  [{15-min | 24-hour}][{fec | optics | otn}]  index
```

**Syntax Description**

- **instance**  Physical interface instance. Naming notation is `rack/slot/module/port` and a slash between values is required as part of the notation.
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.
  - `port`: Physical port number of the interface.

For more information about the syntax for the router, use the question mark (?) online help function.

- **history**  Displays all performance monitoring data.
- **interval**  Displays specific performance monitoring data in a particular interval.
- **15-min**  Displays performance monitoring data in a 15-minute interval.
- **24-hour**  Displays performance monitoring data in a 24-hour interval.
- **fec**  Displays FEC performance parameters, such as bit errors corrected (BIEC) and uncorrectable words.
- **optics**  Displays optics performance parameters, such as optical power.
- **otn**  Displays OTN performance parameters, such as path monitoring failure counts (FC-PM) and section monitoring unavailable seconds (UAS-SM).
- **index**  Interval for which to display the performance monitoring information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read</td>
</tr>
</tbody>
</table>
Examples

The following examples show sample output for a DWDM controller:

```
RP/0/RSP0/CPU0:Router# show controller dwdm 0/5/0/0 pm interval 15-min fec 0
Thu Jul 1 18:58:09.353 UTC

G709 FEC in the current interval [18:45:00 - 18:58:09 Thu Jul 1 2010]
EC-BITS : 0  Threshold : 0  TCA(enable) : NO
UC-WORDS : 0  Threshold : 0  TCA(enable) : NO

RP/0/RSP0/CPU0:Router# show controller dwdm 0/5/0/0 pm history 15-min
Thu Jul 1 18:59:04.585 UTC

G709 OTN in the current interval [18:45:00 - 18:59:04 Thu Jul 1 2010]
ES-SM-NE : 0  Threshold : -1  TCA(enable) : NO
ESR-SM-NE : 0  Threshold : -1  TCA(enable) : NO
SES-SM-NE : 0  Threshold : -1  TCA(enable) : NO
SESR-SM-NE : 0  Threshold : -1  TCA(enable) : NO
UAS-SM-NE : 0  Threshold : -1  TCA(enable) : NO
BBE-SM-NE : 0  Threshold : -1  TCA(enable) : NO
BBER-SM-NE : 0  Threshold : -1  TCA(enable) : NO
FC-SM-NE : 0  Threshold : -1  TCA(enable) : NO
ES-PM-NE : 0  Threshold : -1  TCA(enable) : NO
ESR-PM-NE : 0  Threshold : -1  TCA(enable) : NO
SES-PM-NE : 0  Threshold : -1  TCA(enable) : NO
SESR-PM-NE : 0  Threshold : -1  TCA(enable) : NO
UAS-PM-NE : 0  Threshold : -1  TCA(enable) : NO
BBE-PM-NE : 0  Threshold : -1  TCA(enable) : NO
BBER-PM-NE : 0  Threshold : -1  TCA(enable) : NO
FC-PM-NE : 0  Threshold : -1  TCA(enable) : NO
ES-SM-FE : 0  Threshold : -1  TCA(enable) : NO
ESR-SM-FE : 0  Threshold : -1  TCA(enable) : NO
SES-SM-FE : 0  Threshold : -1  TCA(enable) : NO
SESR-SM-FE : 0  Threshold : -1  TCA(enable) : NO
UAS-SM-FE : 0  Threshold : -1  TCA(enable) : NO
BBE-SM-FE : 0  Threshold : -1  TCA(enable) : NO
BBER-SM-FE : 0  Threshold : -1  TCA(enable) : NO
FC-SM-FE : 0  Threshold : -1  TCA(enable) : NO
ES-PM-FE : 0  Threshold : -1  TCA(enable) : NO
ESR-PM-FE : 0  Threshold : -1  TCA(enable) : NO
SES-PM-FE : 0  Threshold : -1  TCA(enable) : NO
SESR-PM-FE : 0  Threshold : -1  TCA(enable) : NO
UAS-PM-FE : 0  Threshold : -1  TCA(enable) : NO
BBE-PM-FE : 0  Threshold : -1  TCA(enable) : NO
BBER-PM-FE : 0  Threshold : -1  TCA(enable) : NO
FC-PM-FE : 0  Threshold : -1  TCA(enable) : NO

G709 FEC in the current interval [18:45:00 - 18:59:04 Thu Jul 1 2010]
EC-BITS : 0  Threshold : 0  TCA(enable) : NO
UC-WORDS : 0  Threshold : 0  TCA(enable) : NO

Optics in the current interval [18:45:00 - 18:59:04 Thu Jul 1 2010]
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
show controller dwdm pm

This table describes selected fields from the `show controllers dwdm pm` command output.

### Table 5: `show controllers dwdm pm` Command Output Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC-BITS</td>
<td>Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.</td>
</tr>
<tr>
<td>UC-WORDS</td>
<td>Uncorrectable words. This is the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.</td>
</tr>
<tr>
<td>LBC</td>
<td>Laser bias current.</td>
</tr>
<tr>
<td>OPR</td>
<td>Optical power on the unidirectional port.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OPT</td>
<td>Transmit optical power in dBm.</td>
</tr>
<tr>
<td>MAX</td>
<td>Indicates the maximum value of the parameter.</td>
</tr>
<tr>
<td>AVG</td>
<td>Indicates the average value of the parameter.</td>
</tr>
<tr>
<td>MIN</td>
<td>Indicates the minimum value of the parameter.</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>Indicates the parameter’s configured threshold.</td>
</tr>
<tr>
<td>TCA</td>
<td>Indicates if TCA reporting is enabled or not.</td>
</tr>
<tr>
<td>BBE-PM-FE</td>
<td>Far-end path monitoring background block errors (BBE-PM)—Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>BBE-PM-NE</td>
<td>Near-end path monitoring background block errors (BBE-PM).</td>
</tr>
<tr>
<td>BBE-SM-FE</td>
<td>Far-end section monitoring background block errors (BBE-SM)—Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>BBE-SM-NE</td>
<td>Near-end section monitoring background block errors (BBE-SM).</td>
</tr>
<tr>
<td>BBER-PM-FE</td>
<td>Far-end path monitoring background block errors ratio (BBER-PM)—Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>BBER-PM-NE</td>
<td>Near-end path monitoring background block errors ratio (BBER-PM).</td>
</tr>
<tr>
<td>BBER-SM-FE</td>
<td>Far-end section monitoring background block errors ratio (BBER-SM)—Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>BBER-SM-NE</td>
<td>Near-end section monitoring background block errors ratio (BBER-SM).</td>
</tr>
<tr>
<td>ES-PM-FE</td>
<td>Far-end path monitoring errored seconds (ES-PM)—Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>ES-PM-NE</td>
<td>Near-end path monitoring errored seconds (ES-PM).</td>
</tr>
<tr>
<td>ES-SM-FE</td>
<td>Far-end section monitoring errored seconds (ES-SM)—Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>ES-SM-NE</td>
<td>Near-end section monitoring errored seconds (ES-SM).</td>
</tr>
<tr>
<td>ESR-PM-FE</td>
<td>Far-end path monitoring errored seconds ratio (ESR-PM)—Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>ESR-PM-NE</td>
<td>Near-end path monitoring errored seconds ratio (ESR-PM).</td>
</tr>
<tr>
<td>ESR-SM-FE</td>
<td>Far-end section monitoring errored seconds ratio (ESR-SM)—Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ESR-SM-NE</td>
<td>Near-end section monitoring errored seconds ratio (ESR-SM).</td>
</tr>
<tr>
<td>FC-PM-FE</td>
<td>Far-end path monitoring failure counts (FC-PM)—Indicates the failure counts recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>FC-PM-NE</td>
<td>Near-end path monitoring failure counts (FC-PM).</td>
</tr>
<tr>
<td>FC-SM-FE</td>
<td>Far-end section monitoring failure counts (FC-SM)—Indicates the failure counts recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>FC-SM-NE</td>
<td>Near-end section monitoring failure counts (FC-SM).</td>
</tr>
<tr>
<td>SES-PM-FE</td>
<td>Far-end path monitoring severely errored seconds (SES-PM)—Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>SES-PM-NE</td>
<td>Near-end path monitoring severely errored seconds (SES-PM).</td>
</tr>
<tr>
<td>SES-SM-FE</td>
<td>Far-end section monitoring severely errored seconds (SES-SM)—Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>SES-SM-NE</td>
<td>Near-end section monitoring severely errored seconds (SES-SM).</td>
</tr>
<tr>
<td>SESR-PM-FE</td>
<td>Far-end path monitoring severely errored seconds ratio (SESR-PM)—Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>SESR-PM-NE</td>
<td>Near-end path monitoring severely errored seconds ratio (SESR-PM).</td>
</tr>
<tr>
<td>SESR-SM-FE</td>
<td>Far-end section monitoring severely errored seconds ratio (SESR-SM)—Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>SESR-SM-NE</td>
<td>Near-end section monitoring severely errored seconds ratio (SESR-SM).</td>
</tr>
<tr>
<td>UAS-PM-FE</td>
<td>Far-end path monitoring unavailable seconds (UAS-PM)—Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval.</td>
</tr>
<tr>
<td>UAS-PM-NE</td>
<td>Near-end path monitoring unavailable seconds (UAS-PM).</td>
</tr>
<tr>
<td>UAS-SM-FE</td>
<td>Far-end section monitoring unavailable seconds (UAS-SM)—Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval.</td>
</tr>
<tr>
<td>UAS-SM-NE</td>
<td>Near-end section monitoring unavailable seconds (UAS-SM).</td>
</tr>
</tbody>
</table>
show vtxp-monitored ports

To display the list of DWDM controller interfaces on which VTXP attribute is enabled, use the `show vtxp-monitored ports` command in Global Configuration mode.

```
show vtxp-monitored ports
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to view the interfaces on which the VTXP attribute is enabled:

```
RP/0/RSP0/CPU0:router# show vtxp-monitored ports
Thu Jan 8 17:01:29.931 IST
dwdm ifName : dwdm0/1/0/0
dwdm ifName : dwdm0/1/0/1
dwdm ifName : dwdm0/1/0/2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller dwdm, on page 5</td>
<td>Configures a DWDM controller.</td>
</tr>
</tbody>
</table>
transport-mode (WAN/OTN)

To specify the transport mode for a 10-Gigabit Ethernet interface, use the transport-mode command in interface configuration mode. To return to the default mode, use the no form of this command.

transport-mode {wan | otn bit-transparent {opu1e | opu2e}}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan</td>
<td>Configures the interface for 10GBASE-W WAN SONET/SDH (9.95328Gb/s) transport.</td>
</tr>
<tr>
<td>otn bit-transparent</td>
<td>Configures the interface for 10-Gigabit Ethernet over Optical Transport Network (ITU-T G.709) with 10GBASE-R transparently mapped into OTU-2.</td>
</tr>
<tr>
<td>opu1e</td>
<td>Configures the interface for 10GBASE-R over OPU1e without fixed stuffing (11.0491Gb/s).</td>
</tr>
<tr>
<td>opu2e</td>
<td>Configures the interface for 10GBASE-R over OPU2e with fixed stuffing (11.0957Gb/s).</td>
</tr>
</tbody>
</table>

Command Default

The interface is in LAN mode. Neither WAN mode or OTN mode is configured.

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Three modes are supported for a 10-Gigabit Ethernet interface: LAN, WAN, or OTN on these Ethernet line cards and Modular Port Adaptors (MPAs):

- 2-Port 10-Gigabit Ethernet, 20-Port Gigabit Ethernet Combination line card (A9K-2T20GE-B and A9K-2T20GE-L)
- 8-Port 10-Gigabit Ethernet line card (A9K-8T-L, -B, or -E)
- 16-Port 10-Gigabit Ethernet SFP+ line card (A9K-16T/8-B and A9K-16T/8-B+AIP)
- 24-Port 10-Gigabit Ethernet line card (A9K-24X10GE-SE/TR)
- 36-Port 10-Gigabit Ethernet line card (A9K-36X10GE-SE/TR)
- 2-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-2x10GE)
- 4-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-4x10GE)
- 8-Port 10-Gigabit Ethernet Modular Port Adaptor (A9K-MPA-8x10GE)

Limitation:

On TenGig breakout interface of Cisco ASR 9000 High Density 100GE Ethernet (8x100G and 4x100G) line cards, configure same transport mode (OPU1E or OPU2E) on both ends of the interface. Different transport modes at both ends results in flapping of the interface status and the router console displays continuous interface UP/DOWN messages.
If you want to configure the interface for DWDM support, configure the 10-Gigabit Ethernet interface for OTN transport mode.

These 40GE MPAs support LAN and OTU3 modes:

- A9K-MPA-1x40GE
- A9K-MPA-2x40GE

Note

Before Cisco IOS XR Software Release 4.2.0, only transport-mode wan was used under the interface configuration mode to set WAN PHY controller. Then, both Operational Mode and Configuration Mode would be changed to WAN Mode.

After Cisco IOS XR Software Release 4.2.0, you can use transport-mode wan under the interface configuration mode to use basic function of WAN PHY. In addition, we can use wanmode on under the wanphy controller mode to use alarm function and BIP counter.

Note

On the Cisco A9K-4T16GE-TR and Cisco A9K-4T16GE-SE line cards, mixed use of LAN and WAN transport modes is not supported due to hardware limitation. In other words, WAN PHY is configured on all the four 10GigE ports to be operated either in LAN mode or WAN mode for 10 GigE ports 16, 17, 18 and 19.

On applying the configuration change from LAN to WAN or back on port 16, the same configuration shall be applied on all the other 10 GigE ports 17, 18, and 19. The ports 17, 18 or 19 cannot be used to make configuration changes using the transport-mode command. Also, the running configuration shows the configuration change only on port 16.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

This example shows how to configure the interface for WAN PHY mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface 10gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# transport-mode wan
RP/0/RSP0/CPU0:router(config-if)# commit
```

The following configuration is needed to operate in WAN PHY mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller wanphy <>
RP/0/RSP0/CPU0:router(config)# wanmode on
RP/0/RSP0/CPU0:router(config)# commit
```

This example shows how to configure a DWDM interface using OTN transport:

```
RP/0/RSP0/CPU0:router# config
```
The following additional configuration is also needed:

```
RP/0/RSP0/CPU0:router(config)# controller dwdm <>
RP/0/RSP0/CPU0:router(config)# admin-state in-service
RP/0/RSP0/CPU0:router(config)# commit
```

This example shows how to return the interface configuration to its default LAN mode from OTN or WAN PHY mode:

```
RP/0/RSP0/CPU0:router(config)# interface 10gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# no transport-mode
RP/0/RSP0/CPU0:router(config-if)# commit
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>controller wanphy, on page 928</td>
<td>Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
**wavelength**

To set the wavelength on a DWDM controller to a specific ITU channel or to define a specific frequency or wavelength to a DWDM controller, use the **wavelength** command in DWDM configuration mode. To return the wavelength to its default value, use the **no** form of this command.

---

**Note**

ASR 9000 64-bit (eXR) does not support the **wavelength 100MHz-Grid frequency** command.

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wavelength</strong> {50GHz-grid }channel-number</td>
<td>Specifies 50-GHz frequency grid.</td>
<td>channel-number 1, frequency 19580</td>
</tr>
<tr>
<td><strong>wavelength</strong> {100MHz-grid }channel-number</td>
<td>Specifies 100-GHz frequency grid.</td>
<td>channel-number 2, frequency 19580</td>
</tr>
<tr>
<td><strong>channel-number</strong></td>
<td>ITU channel number. ITU channel numbers have predefined frequencies as defined by Multi Source Agreement (MSA) International Telecommunication Union (ITU) grid.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The range is 1 to 100 for conventional band (C-band)</td>
<td></td>
</tr>
<tr>
<td><strong>frequency</strong></td>
<td>Keyword that specifies the frequency for the DWDM controller.</td>
<td>frequency 19580</td>
</tr>
<tr>
<td><strong>update wavelength</strong></td>
<td>Keyword that defines a specific wavelength for the DWDM controller.</td>
<td>update wavelength 1532290</td>
</tr>
<tr>
<td><strong>update</strong></td>
<td>Keyword that defines a specific wavelength for the DWDM controller.</td>
<td>frequency 1532290</td>
</tr>
<tr>
<td><strong>frequency</strong></td>
<td>Keyword that specifies the frequency for the DWDM controller.</td>
<td>frequency 19580</td>
</tr>
<tr>
<td><strong>update</strong></td>
<td>Keyword that defines a specific wavelength for the DWDM controller.</td>
<td>update wavelength 1532290</td>
</tr>
</tbody>
</table>

---

**Command Default**

The default channel is 96.

**Command Modes**

DWDM configuration

**Command History**

| Release | Modification                                                                 |
|---------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| 4.3.0   | This command was introduced.                                                |
| 5.3.2   | 50 GHZ or 100 GHZ options were introduced.                                 |

**Usage Guidelines**

You can set the wavelength to a specific ITU channel, that is represented by a channel number in the Multi Source Agreement (MSA) ITU grid.

The spacing between wavelengths is 50 GHZ or 100 GHZ. Use the **show controllers dwdm** command with the **wavelength-map** keyword to view the channel numbers and wavelengths that are supported for a particular controller.
The controller must be in the out-of-service state before you can use the `wavelength` command.

### Examples

The following example shows how to set the DWDM wavelength to ITU channel 10.

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# wavelength 50GHz-grid 10
```

The following example shows how to set the frequency of ITU channel 10 to 195.8 THz.

```
RP/0/RP0/CPU0:router(config)# controller dwdm 0/1/0/0
RP/0/RP0/CPU0:router(config-dwdm)# wavelength 50GHz-grid frequency 19580
```
Ethernet Interface Commands

This module provides command line interface (CLI) commands for configuring Ethernet interfaces on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- carrier-delay, on page 64
- clear lldp, on page 66
- clear mac-accounting (Ethernet), on page 68
- flow-control, on page 70
- interface (Ethernet), on page 72
- lldp, on page 74
- lldp (interface), on page 75
- lldp holdtime, on page 76
- lldp reinit, on page 77
- lldp timer, on page 78
- lldp tlv-select disable, on page 79
- loopback (Ethernet), on page 80
- mac-accounting, on page 81
- mac-address (Ethernet), on page 83
- negotiation auto, on page 84
- packet-gap non-standard, on page 85
- show controllers (Ethernet), on page 86
- show lldp, on page 94
- show lldp entry, on page 96
- show lldp errors, on page 98
- show lldp interface, on page 99
- show lldp neighbors, on page 101
- show lldp traffic, on page 104
- show mac-accounting (Ethernet), on page 106
- small-frame-padding, on page 108
- speed (Fast Ethernet), on page 109
- transport-mode (UDLR), on page 111
carrier-delay

To delay the processing of hardware link down notifications, use the carrier-delay command in interface configuration mode.

Note

- The carrier-delay command is active only when both up and down are configured from the host.
- If this configuration is not used, the default value is determined by the underlying driver, and may vary depending on whether auto-negotiation is enabled. The default value is chosen to provide enough time for the hardware link to stabilize after state change and to protect the system from excessive link flaps.
- If a value of 0 is set, carrier-delay is disabled in that direction.
- The range of carrier-delay on access port of ASR 9000v is 1 to 60000 msec. If a value of 0 is set, the default value of 100 msec is applied. A value greater than 60000 msec will be ignored and show interfaces output will display the previously configured msec.

carrier-delay {down milliseconds [up milliseconds] | up milliseconds [down milliseconds]}

Syntax Description

down milliseconds Length of time, in milliseconds, to delay the processing of hardware link down notifications. Range is from 0 through 2147483648.

up milliseconds Length of time, in milliseconds, to delay the processing of hardware link up notifications. Range is from 0 through 2147483648.

Command Default

No carrier-delay is manually configured, there is a default carrier-delay setting of 10 msec up and 0 msec down.

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>The default value used when there is no carrier-delay configuration changed from 0 to being defined by each driver.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>The range for both down and up was increased to 0 through 2147483648.</td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When you delay the processing of hardware link down notifications, the higher layer routing protocols are unaware of a link until that link is stable.

If the carrier-delay down milliseconds command is configured on a physical link that fails and cannot be recovered, link down detection is increased, and it may take longer for the routing protocols to re-route traffic around the failed link.

In the case of very small interface state flaps, running the carrier-delay down milliseconds command prevents the routing protocols from experiencing a route flap.
Enter the `show interface` command to see the current state of the carrier-delay operation for an interface. When no carrier-delay is manually configured, carrier-delay displays the default information of 10 msec up.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to delay the processing of hardware link down notifications:

```
RP/0/RSP0/CPU0:router(config-if)# carrier-delay down 10
```

The following example shows how to delay the processing of hardware link up and down notifications:

```
RP/0/RSP0/CPU0:router(config-if)# carrier-delay up 100 down 100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dampening, on page 425</td>
<td>Turns on event dampening.</td>
</tr>
</tbody>
</table>
clear lldp

To reset Link Layer Discovery Protocol (LLDP) traffic counters or LLDP neighbor information, use the clear lldp command in EXEC mode.

clear lldp {counters | table}

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>Specifies that LLDP traffic counters are cleared.</td>
</tr>
<tr>
<td>table</td>
<td>Specifies that LLDP information in the neighbor table is cleared.</td>
</tr>
</tbody>
</table>

Command Default

LLDP traffic counters are not reset, and LLDP neighbor information is not cleared.

Command Modes

EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To reset counters from the show lldp traffic command, use the clear lldp counters command. To clear neighbor information displayed by the show lldp neighbors command, use the clear lldp table command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to clear the LLDP counters and display LLDP traffic. The output from the show lldp traffic command shows that all the traffic counters have been reset to zero.

```
RP/0/RSP0/CPU0:router# clear lldp counters
RP/0/RSP0/CPU0:router# show lldp traffic
LLDP traffic statistics:
    Total frames out: 0
    Total entries aged: 0
    Total frames in: 0
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs discarded: 0
    Total TLVs unrecognized: 0
```

The following example shows how to clear the LLDP table. The output of the show lldp neighbors command shows that all information has been deleted from the table.

```
RP/0/RSP0/CPU0:router# clear lldp table
RP/0/RSP0/CPU0:router# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (F) Repeater, (S) Station, (O) Other
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lldp neighbors, on page 101</code></td>
<td>Displays information about LLDP neighbors.</td>
</tr>
<tr>
<td><code>show lldp traffic, on page 104</code></td>
<td>Displays statistics for LLDP traffic.</td>
</tr>
</tbody>
</table>
clear mac-accounting (Ethernet)

To clear Media Access Control (MAC) accounting statistics, use the clear mac-accounting command in EXEC mode.

```
clear mac-accounting {GigabitEthernet | TenGigE} interface-path-id [location node-id]
```

**Syntax Description**

- **{GigabitEthernet | TenGigE}**
  - Type of Ethernet interface whose MAC accounting statistics you want to clear. Enter GigabitEthernet, TenGigE.

- **interface-path-id**
  - Physical interface or virtual interface.
  - **Note**
    - Use the show interfaces command to see a list of all interfaces currently configured on the router.

  - For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id**
  - (Optional) Clears MAC accounting statistics for the designated node. The node-id argument is entered in the rack/slot/module notation.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear all MAC accounting statistics for the TenGigE port at 1/0/0/1:

```
RP/0/RSP0/CPU0:router# clear mac-accounting TenGigE 0/1/5/0 location 1/0/0/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-accounting, on page 81</td>
<td>Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show mac-accounting (Ethernet), on page 106</td>
<td>Displays MAC accounting statistics for an interface.</td>
</tr>
</tbody>
</table>
flow-control

To enable the sending of flow-control pause frames, use the `flow-control` command in interface configuration mode. To disable flow control, use the `no` form of this command.

```
flow-control {bidirectional | egress | ingress}
```

### Syntax Description

- **bidirectional**: Enables flow-control for egress and ingress direction.
- **egress**: Pauses egress traffic if IEEE 802.3x PAUSE frames are received.
- **ingress**: Sends IEEE 802.3x PAUSE frames in case of congestion with ingress traffic.

### Command Default

- If auto-negotiate is enabled on the interface, then the default is negotiated.
- If auto-negotiate is disabled on the interface, then the sending of flow-control pause frames is disabled for both egress and ingress traffic.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was first introduced.</td>
</tr>
<tr>
<td>Release 4.2.3</td>
<td>This command was supported on 1 Gigabit Ethernet optical and copper SFPs.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

**Note**

When you explicitly enable the sending of flow-control pause frames, the value you configured with the `flow-control` command overrides any auto-negotiated value. This prevents a link from coming up if the value you set with the `flow-control` command conflicts with the allowable settings on the other end of the connection.

**Note**

The `flow-control` command is supported on Gigabit Ethernet, TenGigE interfaces only; the `flow-control` command is not supported on Management Ethernet Interfaces.

**Note**

The `flow-control` command syntax options may vary, depending on the type of PLIM or SPA that is installed in your router.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

This example shows how to enable the sending of flow-control pause frames for ingress traffic on the TenGigE interface 0/3/0/0:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-if)# flow-control ingress
```
interface (Ethernet)

To specify or create an Ethernet interface and enter interface configuration mode, use the `interface (Ethernet)` command in Global Configuration mode. Use the `no` form of the command to remove the configuration.

```
interface {GigabitEthernet | TenGigE} interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet</td>
<td>Specifies or creates a Gigabit Ethernet (1000 Mbps) interface.</td>
</tr>
<tr>
<td>TenGigE</td>
<td>Specifies or creates a Ten Gigabit Ethernet (10 Gbps) interface.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To specify a physical interface, the notation for the `interface-path-id` is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:

- **rack**: Chassis number of the rack.
- **slot**: Physical slot number of the line card.
- **module**: Module number. A physical layer interface module (PLIM) is always 0.
- **port**: Physical port number of the interface.

**Note**

Ten GigE interfaces will not show egress statistics when loopback line is configured because the loopback is closed at the interface controller level, before the Network Processor (NP). But on One GigE interfaces the line loopback is closed in the NP.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>
This example shows how to enter interface configuration mode for a Ten Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface (Ethernet), on page 72</code></td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
lldp

To enable the Link Layer Discovery Protocol (LLDP) globally for both transmit and receive operation on the system, use the lldp command in Global Configuration mode. To disable LLDP, use the no form of this command.

**lldp**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
LLDP is disabled.

**Command Modes**
Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.1</td>
<td>The lldp subinterfaces enable was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
When you enable LLDP globally using the lldp command, LLDP is not enabled on subinterfaces or bundle subinterfaces by default. This is to prevent the LLDP process from consuming high CPU cycles. In order to enable LLDP on subinterfaces and bundle subinterfaces as well, the lldp subinterfaces enable command is introduced.

**Note**
When you use this command, you must remember that as the scale of interfaces (with subinterfaces and bundle subinterfaces) becomes higher, it might cause the LLDP process to hog the CPU.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enable LLDP globally on the router:

```
RP/0/RSP0/CPU0:router(config)# lldp
```

This example shows how to enable LLDP on subinterfaces:

```
RP/0/RSP0/CPU0:router(config)# lldp subinterfaces enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp, on page 94</td>
<td>Displays the global LLDP operational characteristics on the system.</td>
</tr>
</tbody>
</table>
lldp (interface)

To enter LLDP configuration mode, use the **lldp (interface)** command.

**lldp**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to enter LLDP configuration mode from Ethernet interface configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lldp
RP/0/RSP0/CPU0:router(config-lldp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (Ethernet), on page 72</td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
</tbody>
</table>
lldp holdtime

To specify the length of time that information from a Link Layer Discovery Protocol (LLDP) packet should be held by the receiving device before aging and removing it, use the **lldp holdtime** command in Global Configuration mode. To return to the default, use the **no** form of this command.

**Syntax**

```
lldp holdtime  seconds
```

**Syntax Description**

- **seconds**: Number from 0 to 65535 that specifies the amount of time (in seconds) to hold the packet information. The default is 120.

**Command Default**

The packet hold time is 120 seconds (2 minutes).

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to change the default hold time to 1 minute:

```
RP/0/RSP0/CPU0:router(config)# lldp holdtime 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>show lldp, on page 94</td>
<td>Displays the global LLDP operational characteristics on the system.</td>
</tr>
</tbody>
</table>
**lldp reinit**

To specify the length of time to delay initialization of the Link Layer Discovery Protocol (LLDP) on an interface, use the `lldp reinit` command in Global Configuration mode. To return to the default, use the `no` form of this command.

```
lldp reinit  seconds
```

**Syntax Description**

| seconds | Number from 2 to 5 that specifies the length of time (in seconds) that LLDP should delay initialization. The default is 2. |

**Command Default**

Initialization of LLDP is delayed for 2 seconds on an interface.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

| ethernet-services | read, write |

The following example shows how to change the default initialization delay from 2 to 4 seconds:

```
RP/0/RSP0/CPU0:router# lldp reinit 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>show lldp, on page 94</td>
<td>Displays the global LLDP operational characteristics on the system.</td>
</tr>
</tbody>
</table>
lldp timer

To specify the Link Layer Discovery Protocol (LLDP) packet rate, use the `lldp timer` command in Global Configuration mode. To return to the default, use the `no` form of this command.

```
lldp timer  seconds
```

**Syntax Description**

`seconds`  Number from 5 to 65534 that specifies the rate (in seconds) at which to send LLDP packets. The default is 30.

**Command Default**

LLDP packets are sent every 30 seconds.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to change the default LLDP packet rate from 30 seconds to 1 minute:

```
RP/0/RSP0/CPU0:router(config)# lldp timer 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>show lldp, on page 94</td>
<td>Displays the global LLDP operational characteristics on the system.</td>
</tr>
</tbody>
</table>
**Ildp tlv-select disable**

To disable transmission of the selected Type Length Value (TLV) in Link Layer Discovery Protocol (LLDP) packets, use the `ildp tlv-select disable` command in Global Configuration mode. To return to the default, use the `no` form of this command.

```
Ildp tlv-select tlv-name disable
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tlv-name</code></td>
<td>Name of the TLV to be suppressed from LLDP packets. The <code>tlv-name</code> can be one of the following LLDP TLV types:</td>
</tr>
<tr>
<td></td>
<td>• management-address</td>
</tr>
<tr>
<td></td>
<td>• port-description</td>
</tr>
<tr>
<td></td>
<td>• system-capabilities</td>
</tr>
<tr>
<td></td>
<td>• system-description</td>
</tr>
<tr>
<td></td>
<td>• system-name</td>
</tr>
</tbody>
</table>

**Command Default**

All TLVs are sent in LLDP packets.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Release 4.1.0

**Usage Guidelines**

Certain TLVs are classified as mandatory in LLDP packets, such as the Chassis ID, Port ID, and Time to Live (TTL) TLVs. These TLVs must be present in every LLDP packet. You can use the `ildp tlv-select disable` command to suppress transmission of certain other optional TLVs in LLDP packets.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to disable transmission of the System Capabilities TLV from LLDP packets:

```
RP/0/RSP0/CPU0:router(config)# ildp tlv-select system-capabilities disable
```
loopback (Ethernet)

To configure an Ethernet controller for loopback mode, use the `loopback` command in interface configuration mode. To disable loopback, use the `no` form of this command.

```
loopback  {external | internal | line}
```

**Syntax Description**
- `external` All IPv4 self-ping packets are sent out of the interface and looped back externally before being received on the ingress path.
- `internal` All packets are looped back internally within the router before reaching an external cable.
- `line` Incoming network packets are looped back through the external cable.

**Command Default**
Loopback mode is disabled.

**Command Modes**
Interface configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was first introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `loopback` command is available for all Ethernet interface types (Gigabit Ethernet, 10-Gigabit Ethernet).

Two loopback operation modes are supported for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

**Tip**
Use the `loopback external` command when an external loopback connector is attached to the interface.

**Examples**
In the following example, all packets are looped back to the TenGigE controller:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-if)# loopback internal
```
mac-accounting

To generate accounting information for IP traffic based on the source and destination Media Access Control (MAC) addresses on LAN interfaces, use the `mac-accounting` command in interface configuration mode. To disable MAC accounting, use the `no` form of this command.

```
mac-accounting {egress | ingress}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>egress</td>
<td>Generates accounting information for IP traffic based on the destination MAC addresses (egress direction).</td>
</tr>
<tr>
<td>ingress</td>
<td>Generates accounting information for IP traffic based on the source MAC addresses (ingress direction).</td>
</tr>
</tbody>
</table>

**Command Default**

MAC accounting is disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mac-accounting` command calculates the total packet and byte counts for a LAN interface that receives or sends IPv4 packets to or from a unique MAC address.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable MAC accounting for the source MAC address on the ingress direction:

```
RP/0/RSP0/CPU0:router(config)
RP/0/RSP0/CPU0:router(config)
interface bundle-ether <bundle-id>
RP/0/RSP0/CPU0:router(config-if)# mac-accounting ingress
```

This example shows how to enable MAC accounting for the source MAC address on the egress direction:

```
RP/0/RSP0/CPU0:router(config)
RP/0/RSP0/CPU0:router(config)
interface bundle-ether <bundle-id>
RP/0/RSP0/CPU0:router(config-if)# mac-accounting egress
```
In order to view the mac-accounting statistics for the configured bundle interface, use the `show mac-accounting bundle-ether <bundle id>` command.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mac-accounting (Ethernet), on page 68</td>
<td>Clears MAC accounting statistics for an interface.</td>
<td></td>
</tr>
<tr>
<td>show mac-accounting (Ethernet), on page 106</td>
<td>Displays MAC accounting statistics for an interface.</td>
<td></td>
</tr>
</tbody>
</table>
mac-address (Ethernet)

To set the MAC layer address of an Ethernet interface, use the `mac-address` command in interface configuration mode. To return the device to its default MAC address, use the `no` form of this command.

```
mac-address  value1.value2.value3
```

**Syntax Description**

- `value1`: High 2 bytes of the MAC address in hexadecimal format. Range is from 0 to ffff.
- `value2`: Middle 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
- `value3`: Low 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.

**Command Default**
The default MAC address is read from the hardware burned-in address (BIA).

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was first introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).
The `mac-address` command is available for all types of line card Ethernet interfaces (Gigabit Ethernet, 10-Gigabit Ethernet) and for the Management Ethernet interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the MAC address of a Ten Gigabit Ethernet interface located at 0/3/0/0:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```
**negotiation auto**

To enable link autonegotiation on Gigabit Ethernet interfaces, use the **negotiation auto** command in interface configuration mode. To disable link autonegotiation, use the **no** form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Link auto-negotiation is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was first introduced.</td>
</tr>
<tr>
<td>Release 4.2.3</td>
<td>The <strong>negotiation auto</strong> command was supported on 1 Gigabit Ethernet interfaces.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **negotiation auto** command is available on Gigabit Ethernet interfaces only.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable link autonegotiation on an interface:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RSP0/CPU0:router(config-if)# negotiation auto
```

This example shows how to disable link autonegotiation on an interface:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RSP0/CPU0:router(config-if)# no negotiation auto
```
packet-gap non-standard

To change the packet interval for traffic on an interface for improved interoperability with Cisco Catalyst 6000 series switches, use the `packet-gap non-standard` command in interface configuration mode. To use the standard packet interval as defined by the IEEE 802.ae specification, use the `no` form of this command.

```
packet-gap non-standard
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
The interface uses the standard packet interval as defined by the IEEE 802.ae specification.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was first introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An interface that is connected to a Cisco Catalyst 6000 series switch may experience packet loss problems that can be resolved by changing the packet interval of traffic from standard (as defined by the IEEE 802.ae specification) to nonstandard using the `packet-gap non-standard` command.

**Note**
The `packet-gap non-standard` command is available on 10-Gigabit Ethernet interfaces only.

**Task ID**
```
Task ID Operations
interface  read, write
```

**Examples**
This example shows how to change the packet interval for traffic on an interface from standard to nonstandard:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-if)# packet-gap non-standard
```
# show controllers (Ethernet)

To display status and configuration information about the Ethernet interfaces on a specific node, use the `show controllers` command in EXEC mode.

```
show controllers {GigabitEthernet | GigabitEthCtrlr | HundredGigE | HundredGigECtrlr | TenGigE | TenGigECtrlr} interface-path-id [{all | bert | control | internal | mac | periodic | phy | pm | regs | stats | xgxs}]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{GigabitEthernet</td>
<td>GigabitEthCtrlr</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

### Note
Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (```?)``` online help function.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays detailed information for the specified interface.</td>
</tr>
<tr>
<td>bert</td>
<td>Displays BERT status information for the interface.</td>
</tr>
<tr>
<td>control</td>
<td>Displays configuration and control information.</td>
</tr>
<tr>
<td>internal</td>
<td>Displays internal information for the interface.</td>
</tr>
<tr>
<td>periodic</td>
<td>Displays performance monitoring data periodically.</td>
</tr>
<tr>
<td>phy</td>
<td>Displays physical information for the interface.</td>
</tr>
<tr>
<td>pm</td>
<td>Displays Ethernet performance monitoring.</td>
</tr>
<tr>
<td>regs</td>
<td>Displays register information.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays statistical information for the interface.</td>
</tr>
<tr>
<td>xgxs</td>
<td>Displays information about the 10 Gigabit Ethernet Extended Sublayer (XGXS).</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values

## Command Modes

EXEC mode

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was first introduced.</td>
</tr>
</tbody>
</table>
Release 6.0.x This command was modified. The `GigabitCtrlr`, `TenGigECtrlr`, and `HundredGigECtrlr` keywords were added.

Release 6.2.1 The command was updated to display receiving optical power threshold value configured, and the minimum and maximum threshold values, as part of Early Indication of Link Loss Change feature.

Usage Guidelines

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

For controllers, use the following keywords only.

- `all`
- `periodic`
- `pm`
- `stats`

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
</tbody>
</table>

**Note** Required in addition to the interface (read) task ID to use the `control` keyword only.

<table>
<thead>
<tr>
<th>dwdm</th>
<th>read</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read</td>
</tr>
<tr>
<td>sonet-sdh</td>
<td>read</td>
</tr>
</tbody>
</table>

This example shows the receiving optical power alarm status on HuGigE0/1/2/3:

```
RP/0/RSP0/CPU0:router# show controllers GigabitEthernet0/0/0/4
Operational data for interface HuGigE0/1/2/3:
State:
   Administrative state: Enabled
   Operational state: Up,
   LED state: Green On
```
Phy:
Media type: 100GBASE-LR4, fiber over 4 Lane optics (long reach),
Optics:
Vendor: CISCO-AVAGO
Part number: 10-2134-01 (ver.: V01)
Serial number: IPUIALJRAA

Digital Optical Monitoring:
Transceiver Temp: 98.781 C
Transceiver Voltage: 3.283 V

<table>
<thead>
<tr>
<th>Lane</th>
<th>Wavelength (nm)</th>
<th>Tx Power (dBm)</th>
<th>Rx Power (mW) (H)</th>
<th>Laser Bias (mA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>1270</td>
<td>-1.6</td>
<td>0.699 (H)</td>
<td>9.408</td>
</tr>
<tr>
<td>02</td>
<td>1290</td>
<td>-1.6</td>
<td>0.493</td>
<td>9.406</td>
</tr>
<tr>
<td>03</td>
<td>1310</td>
<td>-1.6</td>
<td>0.501 (H)</td>
<td>9.407</td>
</tr>
<tr>
<td>04</td>
<td>1330</td>
<td>-1.6</td>
<td>0.400</td>
<td>9.399</td>
</tr>
</tbody>
</table>

DOM alarms:
Transceiver Temp: Alarm high
Transmit Power: Warning high
Receive Power: Alarm low

<table>
<thead>
<tr>
<th>Thresholds</th>
<th>Alarm</th>
<th>Warning</th>
<th>Warning</th>
<th>Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp (C)</td>
<td>90.000</td>
<td>85.000</td>
<td>-5.000</td>
<td>-10.000</td>
</tr>
<tr>
<td>Voltage (V)</td>
<td>3.630</td>
<td>3.470</td>
<td>3.140</td>
<td>2.970</td>
</tr>
<tr>
<td>Laser Bias (mA)</td>
<td>15.000</td>
<td>15.000</td>
<td>2.000</td>
<td>2.000</td>
</tr>
<tr>
<td>Transmit Power (mW)</td>
<td>1.000</td>
<td>0.501</td>
<td>0.112</td>
<td>0.045</td>
</tr>
<tr>
<td>Receive Power (mW)</td>
<td>1.995</td>
<td>1.000</td>
<td>0.020</td>
<td>0.008</td>
</tr>
</tbody>
</table>

Alarms:
Current:
SD-BER
SF-BER
Previous:
No alarms

Statistics:
Sync Header Error Count: <count>
PCS BIP Error count: <count>
FEC:
Corrected Codeword Count: <count>
Uncorrected Codeword Count: <count>

MAC address information:
Operational address: 0003.6cff.0c00
Burnt-in address: 0003.6cff.0c00
1 unicast address(es) in filter:
0012.3456.7890
Operating in multicast promiscuous mode

Autonegotiation disabled

Priority Flow Control:
Total Rx PFC Frames: 1030
Total Tx PFC Frames: 4440
CoS Status Rx Frames Tx Frames
---  ------  ------------  ------
Operational values:
- Speed: 10 Gbps,
- Bandwidth utilization: 19.73%,
- Duplex: Full Duplex,
- Flowcontrol: None,
- Priority flow control: On,
- Loopback: None (or external),
- MTU: 1514 bytes,
- MRU: 1514 bytes,
- Inter-packet gap: standard (12),
- Forward error correction: Standard (Reed-Solomon)

This example shows the receiving optical power degrade threshold value configured on GigabitEthernet interface location 0/0/0/4:

```
RP/0/RSP0/CPU0:router# show controllers GigabitEthernet0/0/0/4 control
Management information for interface GigabitEthernet0/0/0/4:

Port number: 4
Interface handle: 0x08000400

Config:
- Auto-negotiation: Off
- Carrier delay (up): None
- Carrier delay (down): None
- Duplex: Not configured
- Flow Control: None
- Priority Flow Control: None
- Forward Error Correction: Standard (Reed-Solomon)
- IPG: Standard (12)
- Loopback: None
- MTU: Not configured
- Speed: Not configured
- Soft BW: Not configured
- MAC Address: Not configured

Rx Optical Power Degrade Threshold: -10db

Driver constraints:
- Min MTU: 64 bytes
- Max MTU: 9000 bytes
- Max speed: 1Gbps
- Interface type: Gigabit Ethernet
- Mgmt interface: No
- Allowed config mask: 0x26f

Cached driver state:
- MTU: 1514 bytes
- Burnt-in MAC Address: 0001.0203.0404

Not a member of a bundle interface.

Port FSM state:
- Port is disabled due to an admin down condition.

Complete FSM state:
Admin down
Bundle admin up
Client admin up
Client admin tx up
Port disabled
Port tx disabled
HW link down

IDB interface state information:
IDB bundle admin up
IDB client admin up
IDB client tx admin up
IDB error disable not set

0 Unicast MAC Addresses:
0 Multicast MAC Addresses:

The following example shows sample output from the `show controllers hundredGigE phy` command for A9K-2x100GE line card:

```
RP/0/RSP0/CPU0:router# show controller hundredGigE 0/9/0/0 phy

PHY data for interface: HundredGigE0/9/0/0:

<table>
<thead>
<tr>
<th>Rx</th>
<th>64B66B</th>
<th>Lane</th>
<th>Sync</th>
<th>PCS</th>
<th>Virt</th>
<th>PCS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Service</td>
<td>Block</td>
<td>Marker</td>
<td>Header</td>
<td>Lane</td>
<td>BIP Errors</td>
</tr>
<tr>
<td></td>
<td>Lane</td>
<td>Lock</td>
<td>Sync</td>
<td>Err Cnt</td>
<td>Lane</td>
<td>Lane</td>
</tr>
</tbody>
</table>
| -- | --------- | -------- | -------- | ---------- | ----- | ----- | ------
| 0 | Locked | Locked | 0 | 0 | Clean | 0 |
| 1 | Locked | Locked | 0 | 0 | Clean | 10 |
| 2 | Locked | Locked | 0 | 3 | Clean | 11 |
| 3 | Locked | Locked | 0 | 0 | Clean | 12 |
| 4 | Locked | Locked | 0 | 0 | Clean | 2 |
| 5 | Locked | Locked | 0 | 0 | Clean | 3 |
| 6 | Locked | Locked | 0 | 0 | Clean | 13 |
| 7 | Locked | Locked | 0 | 0 | Clean | 14 |
| 8 | Locked | Locked | 0 | 0 | Clean | 4 |
| 9 | Locked | Locked | 0 | 0 | Clean | 15 |
| 10 | Locked | Locked | 0 | 0 | Clean | 5 |
| 11 | Locked | Locked | 0 | 0 | Clean | 6 |
| 12 | Locked | Locked | 0 | 0 | Clean | 16 |
| 13 | Locked | Locked | 0 | 0 | Clean | 17 |
| 14 | Locked | Locked | 0 | 0 | Clean | 7 |
| 15 | Locked | Locked | 0 | 0 | Clean | 8 |
| 16 | Locked | Locked | 0 | 0 | Clean | 18 |
| 17 | Locked | Locked | 0 | 0 | Clean | 9 |
| 18 | Locked | Locked | 0 | 0 | Clean | 19 |

CFP EEPROM port: 0
Xcvr Type: CFP
Ext Type: 8W,
Connector Type: MPO
Ethernet Application Codes: 100GE-SR10,
Number of Lanes: Network 10, Host 10
Max Bit Rate: Network Lane 10.4Gbit/s, Host Lane 10.4Gbit/s
Link Reaches: SM Fiber 0KM, MM Fiber: 100M, Copper: 0M
Device Tech1: VCSEL, DML,
Device Tech2: No WL, Uncool XmtX, Xmt not tunable, No VOA, PIN detector, No EDC,
Encoding: NRZ, Non-PSK,
Vendor Name: Reflex Photonics
Vendor OUI: 00.00.00
Vendor Part Number: CF-X12-C11801
Vendor Serial Number: X000A906
Date Code (yyyymmdd): 20110527, Lot Code 25
Module DDM Type: RX Avg Power, TX OMA,
Per Lane DDM: Laser Temp,
Enhanced Options:
MSA Data (CFP NVR 1 Table - addr 0x8000-0x807F)
0x0000: 0e 30 09 03 00 00 00 00 : 08 aa 4a 34 34 00 00 00
0x0010: 0a 01 83 40 86 60 4e 20 : 00 04 40 3c 50 26 fa 46
0x0020: 00 52 65 66 6c 65 78 20 : 50 68 6f 74 6f 6e 69 63
0x0030: 73 00 00 00 43 46 2d 58 : 31 32 2d 43 31 31 38 30
0x0040: 31 20 20 20 58 30 30 30 : 20 20 20 20 20 20 20 20
0x0050: 20 20 20 20 20 20 20 20 : 20 20 20 20 20 20 20 20
0x0060: 20 20 20 20 20 20 20 20 : 20 20 20 20 20 20 20 20
0x0070: 01 00 01 01 01 01 01 01 : 40 00 00 00 00 00 00 17

Part Number: (ver.: )
Product ID:
Vendor Specific Data (Vendor Cisco NVR 1 Table - address 0x8400-0x847F)
0x0100: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0110: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0120: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0130: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0140: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0150: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0160: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00
0x0170: 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00

Module Thresholds:
Temperature: +0.273 C +0.253 C +0.019 C +0.000
Voltage: 5.031 Volt 5.338 Volt 0.013 Volt 2.879

Temperature: +45.132 C
Voltage: 3.355 Volt

Lanes
Thresholds:
Temperature: +0.273 C +0.253 C +0.019 C
Bias: 0.000 mAmps 0.000 mAmps 0.000 mAmps

Transmit Power: 0.000 mW (<-40.00 dBm) 0.000 mW (<-40.00 dBm) 0.000 mW (<-40.00 dBm)
Receive Power: 0.000 mW (<-40.00 dBm) 0.000 mW (<-40.00 dBm) 0.000 mW (<-40.00 dBm)

<table>
<thead>
<tr>
<th>Lane</th>
<th>Temp</th>
<th>Bias</th>
<th>Tx Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>+42.640 C</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>+42.640 C</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>+42.640 C</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>+42.640 C</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The following examples show sample output from the `show controllers hundredGigE phy` command for A9K-400G-DWDM-TR line card:

```
RP/0/RSP0/CPU0:router# show controller hundredGigE0/2/0/20/0 phy

<table>
<thead>
<tr>
<th>Rx</th>
<th>Service Block</th>
<th>64B66B Lane</th>
<th>Sync Marker</th>
<th>PCS Header</th>
<th>PCS Lane</th>
<th>Virt PCS Lane</th>
<th>PCS Error Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Locked</td>
<td>Locked</td>
<td>0</td>
<td>0</td>
<td>Clean 19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*** PHY PCS PMA Statistics ***

<table>
<thead>
<tr>
<th>Rx</th>
<th>Service Block</th>
<th>Rx Alignement</th>
<th>PCS Lane</th>
<th>PCS Lane</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>Status 1</td>
<td>Status 2</td>
<td>Offset</td>
<td>Length</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>6</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>Locked</td>
<td>Locked</td>
<td>367</td>
<td>0</td>
</tr>
</tbody>
</table>
show lldp

To display the global Link Layer Discovery Protocol (LLDP) operational characteristics on the system, use the `show lldp` command in EXEC mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `show lldp` command displays the LLDP operational characteristics when LLDP is enabled globally on the system using the `lldp` command. The settings for the following commands are displayed:

- lldp timer
- lldp holdtime
- lldp reinit

**Example 1**
The following example shows the default LLDP operational characteristics when LLDP is enabled globally on the system:

```
RP/0/RSP0/CPU0:router# show lldp
Wed Apr 13 06:16:45.510 DST
Global LLDP information:
  Status: ACTIVE
  LLDP advertisements are sent every 30 seconds
  LLDP hold time advertised is 120 seconds
  LLDP interface reinitialisation delay is 2 seconds
```

**Example 2**
The following example shows the output when LLDP is not enabled globally on the system:
show lldp

% LLDP is not enabled

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>lldp timer, on page 78</td>
<td>Specifies the LLDP packet rate.</td>
</tr>
<tr>
<td>lldp holdtime, on page 76</td>
<td>Specifies the length of time that information from an LLDP packet should be held by the receiving device before aging and removing it.</td>
</tr>
<tr>
<td>lldp reinit, on page 77</td>
<td>Specifies the length of time to delay initialization of LLDP on an interface.</td>
</tr>
</tbody>
</table>
show lldp entry

To display detailed information about LLDP neighbors, use the `show lldp entry` command in EXEC mode.

```
show lldp entry { * name }
```

**Syntax Description**

* Displays detailed information about all LLDP neighbors.

`name` Name of a specific LLDP neighbor for which detailed information is displayed.

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows sample output for all LLDP neighbor table entries on the system:

```
RP/0/RSP0/CPU0:router# show lldp entry *
Wed Apr 13 10:29:40.342 UTC
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

------------------------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8
Port Description: GigabitEthernet0/0/0/8
System Name: asr9k-5
System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 102 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
    IPv4 address: 10.5.173.110

------------------------------------------------
```

```
Local Interface: GigabitEthernet0/0/0/8
```
Chassis id: 0026.9815.c3e6
Port id: G10/0/0/8.1
Port Description: GigabitEthernet0/0/0/8.1
System Name: asr9k-5

System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 96 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110

Total entries displayed: 2

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
</tbody>
</table>
**show lldp errors**

To display Link Layer Discovery Protocol (LLDP) error and overflow statistics, use the `show lldp errors` command in EXEC mode.

```
show lldp errors  [location  location]
```

**Syntax Description**

- `location  location` (Optional) Displays information about LLDP neighbors for the specified location. The `location` argument is entered in the `rack/slot/module` notation.

**Command Default**

Totals of LLDP error and overflow statistics for the system are displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows sample output for the `show lldp errors` command:

```
RP/0/RSP0/CPU0:router# show lldp errors
Wed Apr 13 06:17:08.321 DST
LLDP errors/overflows:
  Total memory allocation failures: 0
  Total encapsulation failures: 0
  Total input queue overflows: 0
  Total table overflows: 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>show lldp traffic, on page 104</td>
<td>Displays statistics for LLDP traffic.</td>
</tr>
</tbody>
</table>
show lldp interface

To display Link Layer Discovery Protocol (LLDP) configuration and status information on an interface, use the `show lldp interface` command in EXEC mode.

```
show lldp interface [type interface-path-id | location location]
```

**Syntax Description**

- **type**: (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id**: Physical interface or virtual interface.
- **location**: (Optional) Displays information about LLDP neighbors for the specified location. The `location` argument is entered in the `rack/slot/module` notation.

**Command Default**

LLDP configuration and status information for all interfaces is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When LLDP is enabled globally on the system, all supported interfaces are automatically enabled for both LLDP receive and transmit operations. You can individually disable interfaces for either LLDP receive or transmit operations using the `receive disable` command or `transmit disable` command in LLDP configuration mode under the interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows sample output for the `show lldp interface` command for the Gigabit Ethernet interface at 0/1/0/7:

```
RP/0/RSP0/CPU0:router# show lldp interface gigabitethernet 0/1/0/7
Wed Apr 13 13:22:30.501 DST

GigabitEthernet0/1/0/7:
  Tx: enabled
  Rx: enabled
  Tx state: IDLE
  Rx state: WAIT FOR FRAME
```
Table 6: show lldp interface Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx:</td>
<td>Configuration status of the interface to transmit LLDP advertisements.</td>
</tr>
<tr>
<td>Rx:</td>
<td>Configuration status of the interface to receive LLDP advertisements.</td>
</tr>
<tr>
<td>Tx state:</td>
<td>Status of the LLDP transmit process on the interface.</td>
</tr>
<tr>
<td>Rx state:</td>
<td>Status of the LLDP receive process on the interface.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>lldp (interface), on page 75</td>
<td>Enters LLDP configuration mode.</td>
</tr>
</tbody>
</table>
show lldp neighbors

To display information about Link Layer Discovery Protocol (LLDP) neighbors, use the `show lldp neighbors` command in EXEC mode.

```bash
show lldp neighbors [type interface-path-id | location location] [detail]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

- **location** (Optional) Displays information about LLDP neighbors for the specified location. The `location` argument is entered in the `rack/slot/module` notation.

- **detail** (Optional) Displays all available information about LLDP neighbors.

**Command Default**

Basic device information for LLDP neighbors is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To clear the neighbor information displayed by the `show lldp neighbors` command, use the `clear lldp table` command.

**Task ID**

- **Task ID** Operation
  - ethernet-services read

The following example show sample output for the `show lldp neighbors` command:

```
RP/0/RSP0/CPU0:router# show lldp neighbors
Capability codes:
   (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
   (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID   Local Intf   Hold-time Capability Port ID
R1          Et1/0       150      R          Et1/0

Total entries displayed: 1
```
### Table 7: show lldp neighbors Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>Name of the neighbor device. <strong>Note</strong>: If the device ID has more than 20 characters, the ID will be truncated to 20 characters in command output because of display constraints.</td>
</tr>
<tr>
<td>Local Intf</td>
<td>Local interface through which this neighbor is connected.</td>
</tr>
<tr>
<td>Hold-time</td>
<td>Amount of time (in seconds) that the local device will hold the LLDP advertisement from a sending device before discarding it.</td>
</tr>
<tr>
<td>Capability</td>
<td>The device type of the neighbor, whose values correspond to the characters and definition displayed in the &quot;Capability codes&quot; section.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Interface and port number of the neighboring device.</td>
</tr>
</tbody>
</table>

The following example shows sample output for the `show lldp neighbors detail` command:

```
RP/0/RSP0/CPU0:router# show lldp neighbors detail
Wed Apr 13 10:29:40.342 UTC
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

----------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8
Port Description: GigabitEthernet0/0/0/8
System Name: asr9k-5
System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
Copyright (c) 2011 by Cisco Systems, Inc.
Time remaining: 102 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
    IPv4 address: 10.5.173.110

----------------------------------
Local Interface: GigabitEthernet0/0/0/8
Chassis id: 0026.9815.c3e6
Port id: Gi0/0/0/8.1
Port Description: GigabitEthernet0/0/0/8.1
System Name: asr9k-5
System Description:
Cisco IOS XR Software, Version 4.1.0.32I[Default]
```
Copyright (c) 2011 by Cisco Systems, Inc.

Time remaining: 96 seconds
Hold Time: 120 seconds
System Capabilities: R
Enabled Capabilities: R
Management Addresses:
  IPv4 address: 10.5.173.110

Total entries displayed: 2

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>clear lldp, on page 66</td>
<td>Resets LLDP traffic counters or LLDP neighbor information.</td>
</tr>
</tbody>
</table>
show lldp traffic

To display statistics for Link Layer Discovery Protocol (LLDP) traffic, use the `show lldp traffic` command in EXEC mode.

`show lldp traffic [location  location]`

**Syntax Description**

| location  | location | (Optional) Displays LLDP statistics for traffic at the specified location. The location argument is entered in the rack/slot/module notation. |

**Command Default**

Totals of LLDP statistics for the system are displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To reset the counters displayed by the `show lldp traffic` command, use the `clear lldp counters` command.

**Task ID**

| ethernet-services | read |

The following example shows sample output for statistics for all LLDP traffic on the system:

```
RP/0/RSP0/CPU0:router# show lldp traffic
LLDP traffic statistics:
  Total frames out: 277
  Total entries aged: 0
  Total frames in: 328
  Total frames received in error: 0
  Total frames discarded: 0
  Total TLVs discarded: 0
  Total TLVs unrecognized: 0
```

**Table 8: show lldp traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total frames out:</td>
<td>Number of LLDP advertisements sent from the device.</td>
</tr>
<tr>
<td>Total entries aged:</td>
<td>Number of LLDP neighbor entries removed due to expiration of the hold time.</td>
</tr>
<tr>
<td>Total frames in:</td>
<td>Number of LLDP advertisements received by the device.</td>
</tr>
<tr>
<td>Total frames received in error:</td>
<td>Number of times the LLDP advertisements contained errors of any type.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total frames discarded:</td>
<td>Number of times the LLDP process discarded an incoming advertisement.</td>
</tr>
<tr>
<td>Total TLVs discarded:</td>
<td>Number of times the LLDP process discarded a Type Length Value (TLV) from an LLDP frame.</td>
</tr>
<tr>
<td>Total TLVs unrecognized:</td>
<td>Number of TLVs that could not be processed because the content of the TLV was not recognized by the device or the contents of the TLV were incorrectly specified.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp, on page 74</td>
<td>Enables LLDP globally for both transmit and receive operation on the system.</td>
</tr>
<tr>
<td>clear lldp, on page 66</td>
<td>Resets LLDP traffic counters or LLDP neighbor information.</td>
</tr>
</tbody>
</table>
show mac-accounting (Ethernet)

To display MAC accounting statistics for an interface, use the `show mac-accounting` command in EXEC mode.

```
show mac-accounting {GigabitEthernet | TenGigE} interface-path-id [location node-id]
```

**Syntax Description**
- `{GigabitEthernet | TenGigE | HundredGigEbundle-ether}`: Indicates the type of Ethernet interface whose MAC accounting statistics you want to display. Enter `GigabitEthernet`, `TenGigE`, or `HundredGigEbundle-ether`.
- `interface-path-id`: Physical interface or virtual interface.
- `location node-id`: (Optional) Displays detailed MAC accounting information for the specified interface on the specified node. The `node-id` argument is entered in the `rack/slot/module/port` notation.

**Note**
- Use the `show interfaces` command to see a list of all interfaces currently configured on the router.
- For more information about the syntax for the router, use the question mark (`?`) online help function.

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**
- **Release**
  - Release 4.1.1: This command was introduced.

**Usage Guidelines**
For the `interface-path-id` argument, use these guidelines:
- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

**Task ID**
- **Task ID**
- **Operations**
- `interface` `read`
These examples show the outputs from the `show mac-accounting` command, which displays MAC accounting statistics on any specified interface:

```
RP/0/RSP0/CPU0:router# show mac-accounting TenGigE 0/2/0/4 location 0/1/CPU0
TenGigE0/2/0/4
    Input (511 free)
    000b.4558.caca: 4 packets, 456 bytes
    Total: 4 packets, 456 bytes
```

### Table 8: show mac-accounting Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface from which the statistics are generated.</td>
</tr>
<tr>
<td>Input</td>
<td>Heading for the ingress MAC accounting statistics. The number of MAC accounting entries still available is shown in parentheses.</td>
</tr>
<tr>
<td>Total</td>
<td>Total statistics for the traffic accounted for by MAC accounting. This excludes any traffic for which there is no MAC address entry, such as non-IP traffic from an unknown MAC source address. This output also excludes any MAC addresses that have 0 packets currently, even if that MAC address was accounted before. Such type of MAC addresses still contribute towards the maximum address limit.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear mac-accounting (Ethernet), on page 68</code></td>
<td>Clears MAC accounting statistics for an interface.</td>
</tr>
<tr>
<td><code>mac-accounting, on page 81</code></td>
<td>Generates accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces.</td>
</tr>
</tbody>
</table>
small-frame-padding

To enable small frame padding on physical interfaces, use the `small-frame-padding` command in the interface configuration mode. To disable small frame padding, use the `no` form of this command.

```
small-frame-padding  interface-path-id
```

**Syntax Description**

- `interface-path-id` Physical interface type.

**Command Default**

None

**Command Modes**

Interface Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.1</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>This command was enabled for Satellite nV access interfaces.</td>
</tr>
<tr>
<td>6.3.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is applicable for all physical interfaces on all types of Cisco ASR 9000 Series Router line cards except Cisco ASR 9000 Ethernet line cards.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the small-frame-padding command:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)# small-frame-padding
```
speed (Fast Ethernet)

To configure the speed for a Fast Ethernet interface, enter the `speed` command in interface configuration mode. To return the system to auto-negotiate speed, use the `no` form of this command.

```plaintext
speed {10 | 100 | 1000}
```

**Syntax Description**
- `10` Configures the interface to transmit at 10 Mbps.
- `100` Configures the interface to transmit at 100 Mbps.
- `1000` Configures the interface to transmit at 1000 Mbps (1 Gbps).

**Command Default**
- If auto-negotiation is enabled on an interface, the default speed is negotiated.
- If auto-negotiation is disabled on an interface, the default speed is the maximum speed allowed on the interface.

**Command Modes**
- Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note** The `speed` command is available on Management Ethernet interfaces and Fast Ethernet interfaces only.
- **Note** Keep in mind that both ends of a link must have the same interface speed. A manually configured interface speed overrides any auto-negotiated speed, which can prevent a link from coming up if the configured interface speed at one end of a link is different from the interface speed on the other end.
- **Note** The `speed` configuration is supported for 1 Gigabit Ethernet copper SFPs and not supported for 1 Gigabit Ethernet optical SFPs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the Fast Ethernet interface to transmit at one gigabit:
speed (Fast Ethernet)

RP/0/RSP0/CPU0:router(config)# interface FastEthernet 0/0/2/0
RP/0/RSP0/CPU0:router(config-if)# speed 1000
transport-mode (UDLR)

To specify the Unidirectional Link Routing (UDLR) mode as receive-only or transmit-only for a 10-Gigabit Ethernet interface, use the transport-mode command in interface configuration mode. To return to the default mode, use the no form of this command.

The signal-degrade option specified is applicable only on 1 GigabitEthernet Cisco ASR 9000 Ethernet and Enhanced Ethernet line cards.

```
transport-mode {rx-only | tx-only | signal-degrade}
```

**Syntax Description**

- rx-only: Configures the 10GE UDLR mode as receive-only.
- tx-only: Configures the 10GE UDLR mode as transmit-only
- signal-degrade: Configures the port as signal-degrade mode. When you configure signal-degrade on 1 GigabitEthernet Cisco ASR 9000 Ethernet and Enhanced Ethernet Line cards, it brings down the interface when low Rx power is detected. Once the signal is recovered, the interface comes up.

**Command Default**

UDLR is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>The signal-degrade keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

UDLR is supported in 10GE LAN mode only on these line cards:

- 24-Port 10-Gigabit Ethernet line card (A9K-24X10GE-SE/TR)
- 36-Port 10-Gigabit Ethernet line card (A9K-36X10GE-SE/TR)

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the 10GE interface for transmit-only mode:

```
RP/0/RSP0/CPU0:router# config
```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# transport-mode tx-only
RP/0/RSP0/CPU0:router(config-if)# commit
Ethernet OAM Commands

This module provides command line interface (CLI) commands for configuring Ethernet Operations, Administration, and Maintenance (EOAM) on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- action capabilities-conflict, on page 117
- action critical-event, on page 119
- action discovery-timeout, on page 121
- action dying-gasp, on page 123
- action high-threshold, on page 125
- action remote-loopback, on page 127
- action session-down, on page 129
- action session-up, on page 131
- action uni-directional link-fault, on page 133
- action wiring-conflict, on page 135
- aggregate, on page 137
- ais transmission, on page 139
- ais transmission up, on page 141
- buckets archive, on page 143
- buckets size, on page 144
- clear error-disable, on page 146
- clear ethernet cfm ccm-learning-database location, on page 147
- clear ethernet cfm interface statistics, on page 148
- clear ethernet cfm local meps, on page 149
- clear ethernet cfm offload, on page 151
- clear ethernet cfm peer meps, on page 152
- clear ethernet cfm traceroute-cache, on page 153
- clear ethernet lmi interfaces, on page 154
- clear ethernet oam statistics, on page 155
- clear ethernet sla statistics all, on page 156
- clear ethernet sla statistics on-demand, on page 157
- clear ethernet sla statistics profile, on page 159
- clear ethernet udlld statistics, on page 161
• connection timeout, on page 162
• continuity-check archive hold-time, on page 164
• continuity-check interval, on page 165
• continuity-check loss auto-traceroute, on page 167
• cos (CFM), on page 168
• debug ethernet cfm packets, on page 169
• debug ethernet cfm protocol-state, on page 172
• domain, on page 174
• efd, on page 176
• error-disable recovery cause, on page 178
• error-disable recovery cause, on page 180
• ethernet cfm (global), on page 182
• ethernet cfm (interface), on page 183
• ethernet lmi, on page 185
• ethernet oam, on page 186
• ethernet oam loopback, on page 187
• ethernet oam profile, on page 189
• ethernet sla, on page 190
• ethernet sla on-demand operation type cfm-delay-measurement probe, on page 191
• ethernet sla on-demand operation type cfm-loopback probe, on page 206
• ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe, on page 213
• ethernet udld reset interface, on page 218
• ethernet uni id, on page 219
• extension remote-uni disable, on page 220
• frame-period threshold, on page 221
• frame-period window, on page 223
• frame-seconds threshold, on page 224
• frame-seconds window, on page 225
• frame threshold, on page 226
• frame window, on page 228
• link-monitor, on page 229
• log ais, on page 230
• log continuity-check errors, on page 231
• log continuity-check mep changes, on page 232
• log crosscheck errors, on page 233
• log disable, on page 235
• log efd, on page 236
• maximum-meps, on page 237
• mep crosscheck, on page 239
• mep-id, on page 240
• mep domain, on page 242
• mib-retrieval, on page 243
• mip auto-create, on page 244
• mode (Ethernet OAM), on page 246
• monitoring, on page 248
• packet size, on page 249
- ping ethernet cfm, on page 251
- polling-verification-timer, on page 254
- priority (SLA), on page 255
- probe, on page 256
- profile (EOAM), on page 257
- profile (SLA), on page 258
- remote-loopback, on page 260
- require-remote, on page 262
- schedule (SLA), on page 264
- send (SLA), on page 267
- service, on page 270
- show error-disable, on page 273
- show efd database, on page 274
- show efd interface, on page 275
- show ethernet cfm ccm-learning-database, on page 276
- show ethernet cfm configuration-errors, on page 278
- show ethernet cfm interfaces ais, on page 280
- show ethernet cfm interfaces statistics, on page 282
- show ethernet cfm local maintenance-points, on page 284
- show ethernet cfm local meps, on page 286
- show ethernet cfm peer meps, on page 292
- show ethernet cfm summary, on page 298
- show ethernet cfm traceroute-cache, on page 300
- show ethernet lmi interfaces, on page 306
- show ethernet loopback active, on page 314
- show ethernet loopback permitted, on page 315
- show ethernet oam configuration, on page 316
- show ethernet oam discovery, on page 319
- show ethernet oam event-log, on page 321
- show ethernet oam interfaces, on page 323
- show ethernet oam statistics, on page 325
- show ethernet sla configuration-errors, on page 327
- show ethernet sla operations, on page 329
- show ethernet sla statistics, on page 332
- show ethernet udld interfaces, on page 340
- show ethernet udld statistics, on page 342
- sla operation, on page 344
- snmp-server traps ethernet cfm, on page 346
- snmp-server traps ethernet oam events, on page 347
- statistics measure, on page 348
- status-counter, on page 350
- symbol-period threshold, on page 351
- symbol-period window, on page 352
- synthetic loss calculation packets, on page 353
- tags, on page 354
- traceroute cache, on page 355
• traceroute ethernet cfm, on page 356
• uni-directional link-fault detection, on page 359
**action capabilities-conflict**

To configure what action is taken on an interface when a capabilities-conflict event occurs, use the `action capabilities-conflict` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action capabilities-conflict {disable | efd | error-disable-interface | log}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td>efd</td>
<td>Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.</td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Puts the interface into the error-disable state when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

**Command Default**

The default action is to create a syslog entry.

**Command Modes**

Ethernet OAM configuration (config-eoam)
Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

- **Release 3.9.0**  This command was introduced.
- **Release 4.0.0**  The `efd` keyword was added.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure that no action is performed on the interface when a capabilities-conflict event occurs.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action capabilities-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a capabilities-conflict event occurs.
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action capabilities-conflict efd

The following example shows how to configure that the interface is put into the error-disable state when a capabilities-conflict event occurs.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action capabilities-conflict error-disable-interface

The following example shows how to configure that a syslog entry is created when a capabilities-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action capabilities-conflict log

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
To configure what action is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer, use the **action critical-event** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

```
action critical-event {disable | error-disable-interface | log}
```

**Syntax Description**
- **disable**: Performs no action on the interface when a critical-event notification is received.
- **error-disable-interface**: Puts the interface into the error-disable state when a critical-event notification is received.
- **log**: (Interface Ethernet OAM configuration only) Creates a syslog entry when a critical-event notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

**Command Default**
The default action is to create a syslog entry.

**Command Modes**
- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- **Task ID**: ethernet-services
- **Operations**: read, write

**Examples**
The following example shows how to configure that no action is performed on the interface when a critical-event notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action critical-event disable
```

The following example shows how to configure that the interface is put into the error-disable state when a critical-event notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
```
RP/0/RSP0/CPU0:router(config-eoam)# **action critical-event error-disable-interface**

The following example shows how to configure that a syslog entry is created when a critical-event notification is received. This configuration overrides the interface Ethernet OAM profile.

RP/0/RSP0/CPU0:router# **configure**
RP/0/RSP0/CPU0:router(config)# **interface gigabitethernet 0/1/0/0**
RP/0/RSP0/CPU0:router(config-if)# **ethernet oam**
RP/0/RSP0/CPU0:router(config-if-eoam)# **action critical-event log**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
**action discovery-timeout**

To configure what action is taken on an interface when a connection timeout occurs, use the `action discovery-timeout` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action discovery-timeout {disable | efd | error-disable-interface | log}
```

**Syntax Description**

- `disable` Performs no action on the interface when a connection timeout occurs.
- `efd` Puts the line protocol into the down state for an interface when a connection timeout occurs. The state is removed when the session is re-established.
- `error-disable-interface` Puts the interface into the error-disable state when a connection timeout occurs.
- `log` (Interface Ethernet OAM configuration only) Creates a syslog entry when a connection timeout occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

**Command Default**
The default action is to create a syslog entry.

**Command Modes**
- Ethernet OAM configuration (config eoam)
- Interface Ethernet OAM configuration (config-if eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The <code>efd</code> keyword was added.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>Removed restriction disallowing default value (log) in Ethernet OAM configuration mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Examples**
The following example shows how to configure that no action is performed on the interface when a connection timeout occurs.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action discovery-timeout disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a connection timeout occurs.
The following example shows how to configure that the interface is put into the error-disable state when a connection timeout occurs.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action discovery-timeout efd
```

The following example shows how to configure that a syslog entry is created when a connection timeout occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action discovery-timeout log
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action dying-gasp

To configure what action is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer, use the `action dying-gasp` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action dying-gasp {disable | error-disable-interface | log}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when a dying-gasp notification is received.</td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Puts the interface into the error-disable state when a dying-gasp notification is received.</td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a dying-gasp notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

**Command Default**
The default action is to create a syslog entry.

**Command Modes**
- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>Removed restriction disallowing default value (log) in Ethernet OAM configuration mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure that no action is performed on the interface when a dying-gasp notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action dying-gasp disable
```

The following example shows how to configure that the interface is put into the error-disable state when a dying-gasp notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
The following example shows how to configure that a syslog entry is created when a dying-gasp notification is received. This configuration overrides the interface Ethernet OAM profile.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action dying-gasp log

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
## action high-threshold

To configure what action is taken on an interface when a high threshold is exceeded, use the `action high-threshold` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action high-threshold {disable | error-disable-interface | log}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>(Interface Ethernet OAM configuration only) Performs no action on the interface when a high threshold is exceeded.</td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Puts the interface into the error-disable state when a high threshold is exceeded.</td>
</tr>
<tr>
<td>log</td>
<td>Creates a syslog entry when a high threshold is exceeded. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

### Command Default

The default is that no action is taken when a high threshold is exceeded.

### Command Modes

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.1.2</td>
<td>Removed restriction disallowing default value (disable) in Ethernet OAM configuration mode.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure that a syslog entry is created on the interface when a high threshold is exceeded.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action high-threshold log
```

The following example shows how to configure that the interface is put into the error-disable state when a high threshold is exceeded.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
```
The following example shows how to configure that no action is taken when a high threshold is exceeded. This configuration overrides the Ethernet OAM profile configuration.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action high-threshold disable

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action remote-loopback

To configure what action is taken on an interface when a remote-loopback event occurs, use the `action remote-loopback` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action remote-loopback {disable | log}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when a remote-loopback event occurs.</td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a remote-loopback event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

### Command Default

The default action is to create a syslog entry.

### Command Modes

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure that no action is performed on the interface when a remote-loopback event occurs.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action remote-loopback disable
```

The following example shows how to configure that a syslog entry is created when a remote-loopback event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action remote-loopback log
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action session-down

To configure what action is taken on an interface when an Ethernet OAM session goes down, use the `action session-down` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action session-down {disable | efd | error-disable-interface | log}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>disable</code></td>
<td>Performs no action on the interface when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td><code>efd</code></td>
<td>Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.</td>
</tr>
<tr>
<td><code>error-disable-interface</code></td>
<td>Puts the interface into the error-disable state when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

**Command Default**
The default action is to create a syslog entry.

**Command Modes**

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The <code>efd</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session goes down.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action session-down disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when an Ethernet OAM session goes down.
The following example shows how to configure that the interface is put into the error-disable state when an Ethernet OAM session goes down.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action session-down error-disable-interface

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session goes down. This configuration overrides the interface Ethernet OAM profile.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action session-down log

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action session-up

To configure what action is taken on an interface when an Ethernet OAM session is established, use the `action session-up` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action session-up [disable | log]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when an Ethernet OAM session is established.</td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when an Ethernet OAM session is established. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

**Command Default**
The default action is to create a syslog entry.

**Command Modes**
- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session is established.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action session-up disable
```

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session is established. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action session-up log
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td></td>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td></td>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action uni-directional link-fault

To configure what action is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer, use the `action uni-directional link-fault` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action uni-directional link-fault {disable | efd | error-disable-interface | log}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td>efd</td>
<td>Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.</td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Puts the interface into the error-disable state when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
</tr>
</tbody>
</table>

**Command Default**
The default action is to create a syslog entry.

**Command Modes**
- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>This command replaces the <code>action link-fault</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command only determines the action taken when a uni-directional link fault notification is received from the peer; it does not affect the action taken when a fault is detected locally.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure that no action is performed on the interface when a link-fault notification is received.

```bash
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action uni-directional link-fault disable
```
The following example shows how to configure putting the interface into the line-protocol-down state when a link-fault notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action uni-directional link-fault efd
```

The following example shows how to configure that the interface is put into the error-disable state when a link-fault notification is received.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action uni-directional link-fault error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a link-fault notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# action uni-directional link-fault log
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
action wiring-conflict

To configure what action is taken on an interface when a wiring-conflict event occurs, use the `action wiring-conflict` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of this command.

```
action wiring-conflict {disable | efd | error-disable-interface | log}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Performs no action on the interface when a capabilities-conflict event occurs.</td>
<td></td>
</tr>
<tr>
<td>efd</td>
<td>Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.</td>
<td></td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Puts the interface into the error-disable state when a capabilities-conflict event occurs.</td>
<td></td>
</tr>
<tr>
<td>log</td>
<td>(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

The default action is to put the interface into error-disable state.

**Command Modes**

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

- Release 3.9.0  This command was introduced.
- Release 4.0.0  The `efd` keyword was added.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure that no action is performed on the interface when a wiring-conflict event occurs.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action wiring-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a wiring-conflict event occurs.
The following example shows how to configure that a syslog entry is created when a wiring-conflict event occurs.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# action wiring-conflict efd

The following example shows how to configure that the interface is put into the error-disable state when a wiring-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
(config-if-eoam)# action wiring-conflict error-disable-interface

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
aggregate

To configure the size and number of bins into which to aggregate the results of statistics collection, use the `aggregate` command in SLA profile statistics configuration mode. To return to the default, use the `no` form of this command.

```
aggregate {bins count width width | none}
```

**Syntax Description**

- **bins count** Number of bins. The range is 2 to 100.
- **width width** For delay and jitter measurements, the size of each bin in milliseconds (range 1-10000). For loss measurements, the size of each bin in percentage points (range 1-100). In addition, the width must be specified if the number of bins is at least 2, regardless of the type of measurement.
- **none** No aggregation is performed. All samples are stored individually.

**Command Default**

- For delay measurements, all collected statistics are aggregated into one bin.
- For loss measurements, the default is aggregation disabled.

**Command Modes**

SLA profile statistics configuration (config-sla-prof-stat-cfg)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The measurement statistics for Y.1731 Synthetic Loss Measurement (SLM) was included.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Changing the aggregation for a given metric clears all stored data for that metric.

When aggregation is enabled, a number of bins are created, each of which represents a range of values. Instead of storing each individual result, all that is stored is a counter of the number of results that fall within the range for each bin. This uses much less memory than storing each individual result.

For delay and jitter measurements, the first bin starts at 0, each bin covers a range of values defined by the specified width, except for the last bin which ends at infinity. For example, an aggregate bin count of 4 and a width of 20 for delay measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with delay ranges 0 to < 20 ms.
- Bin 2—Samples with delay ranges greater than or equal to 20 and < 40 ms.
- Bin 3—Samples with delay ranges greater than or equal to 40 and < 60 ms.
- Bin 4—Samples with delay ranges 60 ms or greater (unbounded).

For synthetic loss measurements, the first bin starts at 0, each bin covers a range of values defined by the specified width, except for the last bin which ends at infinity. For example, an aggregate bin count of 4 and a width of 25 for loss measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with loss ranges 0 to < 25 percentage points.
- Bin 2—Samples with loss ranges greater than or equal to 25 and < 50 percentage points.
• Bin 3—Samples with loss ranges greater than or equal to 50 and < 75 percentage points.
• Bin 4—Samples with loss ranges greater than or equal to 75 and < 100 percentage points.

Note
For delay and jitter measurements (round-trip or one-way), the lower bound of the first bin is zero, and the last bin is effectively of infinite width. If aggregation is disabled, each individual delay value is stored. For loss measurements, the lower bound of the first bin is zero, and the upper bound of the last bin is 100. The last bin may be wider than the other bins. If aggregation is disabled, each calculated FLR value is stored.

Note
The lower bound of each bin is inclusive, while the upper bound is exclusive. Changing the aggregation for a given metric clears all stored data for that metric.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples
This example shows how to configure round-trip-delay statistics measurement in 4 bins each with a range of 20 milliseconds:

```
RE/0/RSP0/CPU0:router# configure
RE/0/RSP0/CPU0:router(config)# ethernet sla
RE/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RE/0/RSP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RE/0/RSP0/CPU0:router(config-sla-prof-stat-cfg)# aggregate bins 4 width 20
```
ais transmission

To configure Alarm Indication Signal (AIS) transmission for a Connectivity Fault Management (CFM) domain service, use the `ais transmission` command in CFM domain service configuration mode. To disable AIS transmission in a CFM domain service, use the `no` form of this command.

```
ais transmission [ { interval 1s | 1m } ] [ cos cos ]
```

### Syntax Description

**interval** *(Optional)* Interval at which AIS packets are transmitted. Valid values are:
- **1s** – Interval of 1 second
- **1m** – Interval of 1 minute

**cos cos** *(Optional)* Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

### Command Default

AIS transmission is disabled by default.

If `interval` is not specified, the default interval is 1 second.

If `cos` is not specified, each MEP uses its own CoS value, inherited from the interface.

### Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

### Command History

**Release** **Modification**

Release 3.9.1  This command was introduced.

### Usage Guidelines

This command enables AIS for all MEPs in the service. AIS messages are triggered by the following events:

- Detection of a CCM defect.
- Detection of a missing peer MEP (when cross-check is configured).
- Receipt of AIS or LCK messages.
- Detection of interface down events (for down MEPs only).

AIS messages are transmitted in the opposite direction of CCMs and other CFM messages that are sent by the MEP. Therefore, up MEPs send AIS messages out of the interface, whereas down MEPs send AIS messages toward the bridging function.

In addition, AIS messages are sent at a higher maintenance level than other CFM messages sent by the MEP:

- If there is a higher-level MEP on the interface in the same direction (up MEP or down MEP), then the AIS messages are passed internally to this higher level MEP. In this case, no AIS messages are actually transmitted (unless the higher-level MEP is also in a service with AIS transmission configured).
- If there is a MIP on the interface, then AIS messages are sent at the level of the MIP.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to configure Alarm Indication Signal (AIS) transmission for a CFM domain service:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service S1 bridge group BG1 bridge-domain BD2
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log ais, on page 230</td>
<td>Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.</td>
</tr>
<tr>
<td>ais transmission up, on page 141</td>
<td>Configures AIS transmission on a CFM interface.</td>
</tr>
<tr>
<td>show ethernet cfm interfaces ais, on page 280</td>
<td>Displays the information about interfaces that are currently transmitting AIS.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
ais transmission up

To configure Alarm Indication Signal (AIS) transmission on a Connectivity Fault Management (CFM) interface, use the **ais transmission up** command in interface CFM configuration mode. To disable AIS transmission on an interface, use the **no** form of this command.

```
ais transmission up [interval 1s | 1m] [cos cos]
```

**Syntax Description**

- **interval** (Optional) Interval at which AIS packets are transmitted. Valid values are:
  - **1s** – Interval of 1 second
  - **1m** – Interval of 1 minute
- **cos cos** (Optional) Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

**Command Default**

AIS transmission is disabled by default.

If **interval** is not specified, the default interval is 1 second.

If **cos** is not specified, each MEP uses its own CoS value, inherited from the interface.

**Command Modes**

- Interface CFM configuration (config-if-cfm)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

AIS transmission packets for CFM can be configured only on interfaces with no down MEPs. AIS packets are transmitted only if a MIP exists on the interface and the line protocol state is down. AIS messages are transmitted up, toward the bridging function (same direction as an up MEP sends CCMs), and they are transmitted at the level of the MIP.

If AIS transmission is configured on an interface with any down MEPs, the configuration is ignored, and an error is displayed in the **show ethernet cfm configuration-errors** command.

**Task ID**

- **Task ID**
  - ethernet-services read, write

**Examples**

The following example shows how to configure AIS transmission on a CFM interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/2
RP/0/RSP0/CPU0:router(config-if)# ethernet cfm
RP/0/RSP0/CPU0:router(config-if-cfm)# ais transmission up interval 1m cos 7
```
## ais transmission up

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ais transmission, on page 139</td>
<td>Configures AIS transmission for a CFM domain service.</td>
</tr>
<tr>
<td></td>
<td>log ais, on page 230</td>
<td>Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.</td>
</tr>
<tr>
<td></td>
<td>show ethernet cfm interfaces ais, on page 280</td>
<td>Displays the information about interfaces that are currently transmitting AIS.</td>
</tr>
<tr>
<td></td>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
buckets archive

To configure the number of buckets to store in memory, use the `buckets archive` command in SLA profile statistics configuration mode. To return to the default value, use the `no` form of this command.

**Syntax Description**

```
buckets archive number
```

- `number` Number of buckets to store. The range is 1 to 100.

**Command Default**

The default number of buckets stored in memory is 100.

**Command Modes**

SLA profile statistics configuration (config-sla-prof-stat-cfg)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The results stored in the oldest bucket are discarded when the limit is reached, to make room for new results. If the number of archived buckets for a given metric decreases, the oldest buckets are deleted and the remaining buckets are untouched. If the number archived buckets for a given metric increases, the newest buckets are filled when the data is collected. See the Usage Guidelines in the `buckets size`, on page 144 command for a description of buckets.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the number of buckets to store in memory:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RSP0/CPU0:router(config-sla-prof-stat-cfg)# buckets archive 50
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>buckets size</code>, on page 144</td>
<td>Configures the size of the buckets in which statistics are collected.</td>
</tr>
</tbody>
</table>
buckets size

To configure the size of the buckets in which statistics are collected, use the `buckets size` command in SLA profile statistics configuration mode. To return the `buckets size` to the default value, use the `no` form of this command.

```
buckets size number {}
```

**Syntax Description**

- **number** Specifies the size of each bucket. The number of probes that each buckets may contain. The range is 1 to 100.
- **per-probe** Probes span multiple buckets.
- **probes** Buckets span multiple probes.

**Command Default**

1 probe per bucket is collected.

**Command Modes**

SLA profile statistics configuration mode (config-sla-prof-stat-cfg)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The <code>per-probe</code> keyword was deprecated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A bucket represents a time period during which statistics are collected. All the results received during that time period are recorded in the corresponding bucket. If aggregation is enabled, each bucket has its own set of bins and counters, and only results received during the time period represented by the bucket are included in those counters.

By default, there is a separate bucket for each probe. The time period is determined by how long the probe lasts (configured by the `probe`, on page 256, `send (SLA)`, on page 267, and `schedule (SLA)`, on page 264 commands). This command allows you to modify the size of buckets so that you can have more buckets per probe, or fewer buckets per probe (fewer buckets allows the results from multiple probes to be included in the same bucket).

**Note**

Changing the size of the buckets for a given metric clears all stored data for that metric. All existing buckets are deleted and new buckets are created.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the size of the buckets in which statistics are collected.
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
RP/0/RSP0/CPU0:router(config-sla-prof-stat-cfg)# buckets size 100 per-probe

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets archive, on page 143</td>
<td>Configures the number of buckets to store in memory.</td>
</tr>
<tr>
<td>probe, on page 256</td>
<td>Enters SLA profile probe configuration mode.</td>
</tr>
<tr>
<td>schedule (SLA), on page 264</td>
<td></td>
</tr>
<tr>
<td>send (SLA), on page 267</td>
<td>Configures the number and timing of packets sent by a probe in an operations profile.</td>
</tr>
</tbody>
</table>
clear error-disable

To clear error-disable reason of an interface, use the **clear error-disable** command in the EXEC mode.

```
clear error-disable {interface <interface> | { all | <location > }}
```

**Syntax Description**

- **interface** The interface for which you want to clear the error-disable reason.
- **location** Clear error-disable for all interfaces on a specific card, or on all cards.

**Command Default**

An interface, location o

**Command Modes**

EXEC mode

**Command History**

```
Release  Modification
3.7.3     This command was introduced.
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID    Operation
interface  exec
```

**Example**

The following example shows how to clear error-disable reason for an interface:

```
RP/0/0/CPU0:ios#sh error-disable
Interface Error-Disable reason Retry (s) Time disabled
------------------- ------------------------------ --------- --------------
Gi0/0/0/0 ethernet-oam-link-fault --- 01:00 01 Jan

RP/0/0/CPU0:ios#
RP/0/0/CPU0:ios#clear error-disable interface G 0/0/0/0
```
**clear ethernet cfm ccm-learning-database location**

To clear the Continuity Check Message (CCM) learning database, use the `clear ethernet cfm ccm-learning-database location` command in EXEC mode.

```
all
node-id
```

**Syntax Description**

- `all` Clears the CCM learning database for all interfaces.
- `node-id` Clears the CCM learning database for the designated node, entered in `rack/slot/module` notation.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- ethernet-services execute

**Examples**

The following example shows how to clear all the CFM CCM learning databases on all interfaces:

```
RP/0/RSP0/CPU0:router# clear ethernet cfm ccm-learning-database location all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet cfm ccm-learning-database</code></td>
<td>Displays the CCM learning database.</td>
</tr>
</tbody>
</table>
# clear ethernet cfm interface statistics

To clear the counters for an Ethernet CFM interface, use the `clear ethernet cfm interface statistics` command in EXEC mode.

```plaintext
clear ethernet cfm interface interface-path-id statistics [location {all | location}]  
clear ethernet cfm interface statistics location {all|node-id}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-path-id</code></td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>(Optional only when used with a specified interface) Clears MAC accounting statistics for a designated interface or for all interfaces.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Clears CFM counters for all interfaces.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>Clears CFM counters for a specified interface, using rack/slot/module notation.</td>
</tr>
</tbody>
</table>

## Command Default
No default behavior or values

## Command Modes
EXEC mode

## Command History
Release 3.7.2 This command was introduced.

## Usage Guidelines
No specific guidelines impact the use of this command.

## Task ID
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

## Examples
The following example shows how to clear all the CFM counters from all interfaces:

```
RP/0/RSP0/CPU0:router# clear ethernet cfm interface statistics location all
```

## Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet cfm interfaces statistics</code>, on page 282</td>
<td>Displays the per-interface counters for CFM.</td>
</tr>
</tbody>
</table>
To clear the counters for all MEPs or a specified MEP, use the **clear ethernet cfm local meps** command in EXEC mode.

```
clear ethernet cfm local meps {all | domain domain-name {all | service service-name {all | mep-id id}} | interface interface-name {all | domain domain-name}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears counters for all local MEPs.</td>
</tr>
<tr>
<td>domain</td>
<td>String of a maximum of 80 characters that identifies the domain in which the maintenance points reside.</td>
</tr>
<tr>
<td>domain-name</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.</td>
</tr>
<tr>
<td>service</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.</td>
</tr>
<tr>
<td>service-name</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.</td>
</tr>
<tr>
<td>mep-id</td>
<td>Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.</td>
</tr>
<tr>
<td>interface</td>
<td>String of a maximum of 80 characters that identifies the Ethernet interface.</td>
</tr>
<tr>
<td>interface-name</td>
<td>String of a maximum of 80 characters that identifies the Ethernet interface.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The following counters are cleared:

- Number of continuity-check messages (CCMs) sent
- Number of CCMs received
- Number of CCMs received out of sequence
- Number of CCMs received, but discarded due to the `maximum-meps` limit
- Number of loopback messages (LBMs), used for CFM ping
- Number of loopback replies (LBRs), used for CFM ping, sent and received
- Number of LBRs received out of sequence
- Number of LBRs received with bad data (such as LBRs containing padding which does not match the padding sent in the corresponding LBM)
- Number of alarm indication signal (AIS) messages sent and received
- Number of lock (LCK) messages received
**clear ethernet cfm local meps**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear counters for all MEPs:

```
RP/0/RSP0/CPU0:router# clear ethernet cfm local meps all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
clear ethernet cfm offload

To trigger the re-application of Maintenance End Points (MEPs) that have been disabled due to exceeding offload resource limits, use the `clear ethernet cfm offload` command in the EXEC mode.

---

**Note**

This command does not clear any counters or stored statistics for the MEPs.

```
clear ethernet cfm offload location node-id
```

**Syntax Description**

- `location node-id` (Optional) Specifies the location for which the re-application of MEPs needs to be triggered.

**Command Default**

The default action is to clear the CFM offload information for all nodes.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to execute the `clear ethernet cfm offload` command:

```
RP/0/RSP0/CPU0:router# clear ethernet cfm offload
```
## clear ethernet cfm peer meps

To clear all peer MEPs or peer MEPs for a specified local MEP, use the `clear ethernet cfm peer meps` command in EXEC mode.

### Syntax
```
clear ethernet cfm peer meps {all | domain domain-name {all | service service-name {all | local mep-id id}} | interface interface-name {all | domain domain-name}}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears counters for all peer MEPs.</td>
</tr>
<tr>
<td>domain</td>
<td>String of a maximum of 80 characters that identifies the domain in which the maintenance points reside.</td>
</tr>
<tr>
<td>service</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.</td>
</tr>
<tr>
<td>local mep-id</td>
<td>Local maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.</td>
</tr>
<tr>
<td>interface</td>
<td>String of a maximum of 80 characters that identifies the Ethernet interface.</td>
</tr>
</tbody>
</table>

### Command Default
No default behavior or values

### Command Modes
EXEC mode

### Command History
```
Release  Modification
3.7.2        This command was introduced.
```

### Usage Guidelines
This command removes all received CCMs and corresponding peer MEPs from the database (other than those configured with cross-check). The peer MEPs will be added again when the next CCM is received.

### Examples
The following example shows how to clear all peer MEPs:
```
RP/0/RSP0/CPU0:router# clear ethernet cfm peer meps all
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
</tbody>
</table>
clear ethernet cfm traceroute-cache

To remove the contents of the traceroute cache, use the `clear ethernet cfm traceroute-cache` command in EXEC mode.

```
clear ethernet cfm traceroute-cache { all | domain domain-name { all | service service-name { all | mep-id id } | interface interface-name { all | domain domain-name } }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>String of a maximum of 80 characters that identifies the domain in which the maintenance points reside.</td>
</tr>
<tr>
<td>Note</td>
<td>For more information about the syntax, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>service</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.</td>
</tr>
<tr>
<td>mep-id</td>
<td>Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.</td>
</tr>
<tr>
<td>interface</td>
<td>String of a maximum of 80 characters that identifies the Ethernet interface.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Examples

The following example shows how to clear all ethernet cfm traceroute-cache:

```
RP/0/RSP0/CPU0:router# clear ethernet cfm traceroute-cache all
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute cache, on page 355</td>
<td>Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.</td>
</tr>
<tr>
<td>show ethernet cfm traceroute-cache, on page 300</td>
<td>Displays the contents of the traceroute cache.</td>
</tr>
</tbody>
</table>
clear ethernet lmi interfaces

To clear Ethernet LMI statistics on one or all interfaces, use the `clear ethernet lmi interfaces` command in EXEC mode.

```
clear ethernet lmi interfaces  {type interface-path-id | all}
```

**Syntax Description**

- **type**
  - Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**
  - Physical interface or virtual interface.

  **Note**
  - Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **all**
  - Specifies clearing of LMI statistics for all Ethernet interfaces running the E-LMI protocol.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

The following example shows how to clear E-LMI statistics for Gigabit Ethernet interface 0/0/0/0:

```
RP/0/RSP0/CPU0:router# clear ethernet lmi interfaces GigabitEthernet 0/0/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet lmi interfaces, on page 306</td>
<td>Displays E-LMI information for an interface, including protocol status and error and event statistics.</td>
</tr>
</tbody>
</table>
clear ethernet oam statistics

To clear the packet counters on Ethernet OAM interfaces, use the `clear ethernet oam statistics` command in EXEC mode.

```
clear ethernet oam statistics [{interface type interface-path-id | location node-id all}]
```

**Syntax Description**

- **interface type interface-path-id** (Optional) Physical interface or virtual interface.
  
  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **location** Clears the statistics for a specific node.
  
  For more information about the syntax for the router, use the question mark (?) online help function.

- **node-id** Path ID of the node.

- **all** Clears the statistics for all nodes on the router.

**Command Default**

No parameters clears the packet counters on all Ethernet OAM interfaces.

**Command Modes**

EXEC mode

**Command History**

- **Release** 3.7.2 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the packet counters on a specific interface:

```
RP/0/RSP0/CPU0:router# clear ethernet oam statistics interface gigabitethernet 0/1/5/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet oam statistics, on page 325</code></td>
<td>Displays the local and remote Ethernet OAM statistics for interfaces.</td>
</tr>
<tr>
<td><code>show ethernet oam interfaces, on page 323</code></td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
clear ethernet sla statistics all

To delete the contents of buckets containing SLA statistics collected by all operations probes, including on-demand operations, use the clear ethernet sla statistics all command in EXEC mode.

```
clear ethernet sla statistics [{current | history}] all
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>current</code></td>
<td>Optional. Clears statistics for buckets currently being filled for all operations.</td>
</tr>
<tr>
<td><code>history</code></td>
<td>Optional. Clears statistics for full buckets for all operations.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Clears statistics for all operations.</td>
</tr>
</tbody>
</table>

**Command Default**

When `current` or `history` are not used, all buckets (current, old, new, half empty, and full) for all operations (including on-demand operations) are cleared. This is equivalent to restarting the operation.

**Command Modes**

EXEC mode

**Command History**

Release 4.0.0  This command was introduced.

**Usage Guidelines**

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 144 command for a description of buckets.

**Examples**

The following example shows how to delete the contents of all buckets containing SLA metrics collected by all probes:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics all
```

The following example shows how to delete the contents of all current buckets containing SLA metrics collected by all probes:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics current all
```

The following example shows how to delete the contents of all full buckets containing SLA metrics collected by all probes:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics history all
```
**clear ethernet sla statistics on-demand**

To delete the contents of buckets containing SLA statistics collected by on-demand probes, use the `clear ethernet sla statistics on-demand` command in EXEC mode.

```
clear ethernet sla statistics [{current | history}] on-demand {all | id} [{interface type interface-path-id domain all | interface type interface-path-id domain domain-name target {all | mac-address H.H.H | mep-id id} | interface all domain domain-name}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current (Optional) Clears statistics for all buckets currently being filled.</td>
</tr>
<tr>
<td>history (Optional) Clears statistics for all full buckets.</td>
</tr>
<tr>
<td>all Clears statistics for all on-demand operations.</td>
</tr>
<tr>
<td>id Clears statistics for the on-demand operation of the specified number.</td>
</tr>
<tr>
<td>interface type (Optional) Clears statistics for the specified interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong> Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td>For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>domain all Clears statistics for on-demand operations for all domains.</td>
</tr>
<tr>
<td>domain domain-name Clears statistics for on-demand operations for the specified domain.</td>
</tr>
<tr>
<td>target all Clears statistics for on-demand operations targeted to all MEPs for the specified interface domain.</td>
</tr>
<tr>
<td>target mac-address H.H.H Clears statistics for on-demand operations targeted to the specified MAC address.</td>
</tr>
<tr>
<td>target mep-id id Clears statistics for on-demand operations targeted to the specified MEP ID.</td>
</tr>
<tr>
<td>interface all (Optional) Clears statistics for on-demand operations on all interfaces.</td>
</tr>
</tbody>
</table>

**Command Default**

When `current` or `history` are not used, all buckets for on-demand operations (current, old, new, half empty, and full) are cleared. This is equivalent to restarting the operation.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 144 command for a description of buckets.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to delete the contents of all buckets currently being filled for the on-demand operation with ID 1:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics current on-demand 1
```

The following example shows how to delete the contents of all buckets for all on-demand operations:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics on-demand all
```

The following example shows how to delete the contents of all buckets for all on-demand operations on a specified interface and domain that is targeted to a specific MEP:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics on-demand all interface TenGigE 0/6/1/0 domain D1 target mep-id 3
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet sla statistics all, on page 156</td>
<td>Deletes the contents of buckets containing SLA statistics collected by all operations probes.</td>
</tr>
<tr>
<td>ethernet sla on-demand operation type cfm-delay-measurement probe, on page 191</td>
<td>Executes an on-demand Ethernet SLA operation probe for CFM delay measurement.</td>
</tr>
<tr>
<td>ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe, on page 213</td>
<td>Executes an on-demand Ethernet SLA operation probe for CFM synthetic loss measurement.</td>
</tr>
<tr>
<td>show ethernet sla operations, on page 329</td>
<td>Displays information about configured Ethernet SLA operations.</td>
</tr>
<tr>
<td>show ethernet sla statistics, on page 332</td>
<td>Displays the contents of buckets containing Ethernet SLA metrics collected by probes.</td>
</tr>
</tbody>
</table>
clear ethernet sla statistics profile

To delete the contents of buckets containing SLA statistics collected by probes for a profile, use the `clear ethernet sla statistics profile` command in EXEC mode.

```
clear ethernet sla statistics [ { current | history }] profile { all | profile-name } [ { interface type interface-path-id domain all | interface type interface-path-id domain domain-name target { all | mac-address H.H.H | mep-id id | interface all domain domain-name } ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>(Optional) Clears statistics for all buckets currently being filled.</td>
</tr>
<tr>
<td>history</td>
<td>(Optional) Clears statistics for all full buckets.</td>
</tr>
<tr>
<td>profile-name</td>
<td>Clears statistics for the specified profile name.</td>
</tr>
<tr>
<td>all</td>
<td>Clears statistics for all profiles.</td>
</tr>
<tr>
<td>interface type</td>
<td>(Optional) Clears statistics for the specified interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>domain all</td>
<td>Clears statistics for on-demand operations for all domains.</td>
</tr>
<tr>
<td>domain domain-name</td>
<td>Clears statistics for on-demand operations for the specified domain.</td>
</tr>
<tr>
<td>target all</td>
<td>Clears statistics for on-demand operations targeted to all MEPs for the specified interface domain.</td>
</tr>
<tr>
<td>target mac-address H.H.H</td>
<td>Clears statistics for on-demand operations targeted to the specified MAC address.</td>
</tr>
<tr>
<td>target mep-id id</td>
<td>Clears statistics for on-demand operations targeted to the specified MEP ID.</td>
</tr>
<tr>
<td>interface all</td>
<td>(Optional) Clears statistics for on-demand operations on all interfaces.</td>
</tr>
</tbody>
</table>

### Command Default

When `current` or `history` are not used, all buckets in the profile (current, old, new, half empty, and full) are cleared. This is equivalent to restarting the operation.

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

See the Usage Guidelines in the buckets size, on page 144 command for a description of buckets.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to delete the contents of all buckets currently being filled for a specified profile:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics current profile P1
```

The following example shows how to delete the contents of all full buckets for a specified profile:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics history profile P2
```

The following example shows how to delete the contents of all buckets for a specified profile:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics profile P3
```

The following example shows how to delete the contents of all buckets for all profiles:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics profile all
```

The following example shows how to delete the contents of all buckets for all profiles on a specified interface and domain that is targeted to a specific MEP:

```
RP/0/RSP0/CPU0:router# clear ethernet sla statistics profile all interface TenGigE 0/6/1/0 domain D1 target mep-id 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets size, on page 144</td>
<td>Configures the size of the buckets in which statistics are collected.</td>
</tr>
</tbody>
</table>
clear ethernet udld statistics

To remove the statistics of state machine transitions and packets exchanged on an interface running UDLD protocol, use the **clear ethernet udld statistics** command in the ethernet interface configuration mode.

```
clear ethernet udld statistics [interface  type  |unaccounted-drops |all]
```

**Syntax Description**

- **interface  type**  
  (Optional) Clears information about the specified interface type. If an interface is specified, only the interface-specific counters are shown and not the node counters.

- **unaccounted-drops**  
  (Optional) Clears information for only the node counters.

- **all**  
  (Optional) Clears all the udld statistics.

**Command Default**

None

**Command Modes**

Ethernet Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to run the **clear ethernet udld statistics** command for an interface:

```
RP/0/RSP0/CPU0:router#clear ethernet udld statistics interface GigabitEthernet 0/1/0/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet udld statistics, on page 342</td>
<td>Displays statistics on state machine transitions and packets sent and received for an UDLD interface.</td>
</tr>
</tbody>
</table>
connection timeout

To configure the timeout value for an Ethernet OAM session, use the `connection timeout` command in Ethernet OAM configuration mode.

```
connection timeout seconds
```

**Syntax Description**

- `seconds` Connection timeout period in number of lost periodic information OAMPDUs. The range is 2 to 30.

**Command Default**

The default value is 5.

**Command Modes**

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

```
Release    Modification
3.9.0       This command was introduced.
```

**Usage Guidelines**

If no packets are received from the OAM peer in the specified connection timeout period which is measured in number of lost periodic Information OAMPDUs, then the OAM session is brought down, and the negotiation phase starts again.

**Task ID**

```
Task ID    Operations
ethernet-services    read, write
```

**Examples**

This example shows how to configure the connection timeout value of an Ethernet OAM session:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# connection timeout 20
```

**Related Commands**

- `action discovery-timeout`, on page 121
- `ethernet oam`, on page 186
- `ethernet oam profile`, on page 189
- `show ethernet oam configuration`, on page 316

Configures what action is taken on an interface when a connection timeout occurs.

Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.

Creates an EOAM profile and enters EOAM configuration mode.

Displays the current active Ethernet OAM configuration on an interface.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam discovery, on page 319</td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
continuity-check archive hold-time

To configure the time limit for how long peer maintenance-end-points (MEPs) are held in the continuity-check database after they have timed out (no more CCMs are received), use the **continuity-check archive hold-time** command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

```
continuity-check archive hold-time minutes
```

**Syntax Description**

| minutes | Time limit (in minutes) that peer MEPs are held in the continuity-check database before they are cleared. Range is 1 to 65535. |

**Command Default**

The default is 100.

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Peer MEPs appear in **show ethernet cfm peer meps** command display output after they timeout (no more continuity check messages (CCMs) are received).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
</tbody>
</table>
continuity-check interval

To enable continuity check and configure the time interval at which continuity-check messages are transmitted or to set the threshold limit for when a MEP is declared down, use the `continuity-check interval` command in CFM domain service configuration mode. To disable continuity check, use the `no` form of this command.

```
continuity-check interval  time  [loss-threshold  threshold]
```

### Syntax Description

- **time**: Interval at which continuity-check messages are transmitted. Valid values are:
  - 10ms: 10 milliseconds
  - 100ms: 100 milliseconds
  - 1s: 1 second
  - 10s: 10 seconds
  - 1m: 1 minute
  - 10m: 10 minutes

- **loss-threshold threshold**: (Optional) Specifies the number of continuity-check messages that are lost before CFM declares that a MEP is down (unreachable). Range is 2 to 255. Used in conjunction with `interval`.

### Command Default

Continuity check is off by default.

If `loss-threshold` is not specified, the default is 3.

### Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td></td>
</tr>
<tr>
<td>Release 4.3.1</td>
<td>The <code>continuity-check interval</code> command was updated to allow CCM time interval of 10ms.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure the time interval at which continuity-check messages are transmitted and set the threshold limit for when a MEP is declared down.

```bash
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
```
continuity-check interval

RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# continuity-check interval 100ms loss-threshold 10
continuity-check loss auto-traceroute

To configure automatic triggering of a traceroute when a MEP is declared down, use the `continuity-check loss auto-traceroute` command in CFM domain service configuration mode. To disable automatic triggering of a traceroute, use the `no` form of this command.

`continuity-check loss auto-traceroute`

This command has no keywords or arguments.

**Command Default**
Auto-trigger is off.

**Command Modes**
CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The results of the traceroute can be seen using the `show ethernet cfm traceroute-cache` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet cfm traceroute-cache</code></td>
<td>Displays the contents of the traceroute cache.</td>
</tr>
</tbody>
</table>
**cos (CFM)**

To configure the class of service (CoS) for all CFM packets generated by the maintenance end point (MEP) on an interface, use the `cos` command in interface CFM MEP configuration mode. To return to the default CoS, use the `no` form of this command.

```
cos  cos
```

**Syntax Description**

```
cos Class of Service for this MEP. The range is 0 to 7.
```

**Command Default**

When not configured, the default CoS value is inherited from the Ethernet interface.

**Command Modes**

Interface CFM MEP configuration (config-if-cfm-mep)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configuring the class of service (CoS) on maintenance end points (MEPs) is supported on all Ethernet interfaces. The specified CoS value is used for all CFM messages transmitted by the MEP, except for the following:

- Loopback and Linktrace replies—These are transmitted using the CoS value received in the corresponding loopback or linktrace message.
- AIS messages—If a different CoS value is specified in the AIS configuration.
- Ethernet SLA probe messages.

**Examples**

The following example shows how to configure the class of service (CoS) for a maintenance end point (MEP) on an interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ethernet cfm mep domain Dm1 service Sv1 mep-id 1
RP/0/RSP0/CPU0:router(config-if-cfm-mep)# cos 7
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
</tbody>
</table>
debug ethernet cfm packets

To log debug messages about CFM packets that are sent or received by the Ethernet connectivity fault management (CFM) process, use the debug ethernet cfm packets command in EXEC mode.

```
ddebug ethernet cfm packets [domain domain-name [service service-name [mep-id mep-id]]]
interface type interface-path-id [domain domain-name] [packet-type {ccm | linktrace | loopback}]
[remote mac-address mac-address] [remote mep-id mep-id] [{sent | received}] [{brief | full | hexdump}]
```

Syntax Description

- **domain domain-name** (Optional) Filters packets for display by the specified CFM maintenance domain, where `domain-name` is a string of up to 80 characters.
- **service service-name** (Optional) Filters packets for display by the specified service name, where `service-name` is a string of up to 80 characters.
- **mep-id mep-id** (Optional) Filters packets for display by the specified maintenance endpoint (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
- **interface type interface-path-id** (Optional) Filters packets for display by the specified physical interface or virtual interface.
  - Note: Use the show interfaces command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **packet-type** (Optional) Filters packets for display by the specified packet type. The following packet types are valid:
  - ais
  - ccm
  - delay-measurement
  - linktrace
  - loopback

- **remote mac-address mac-address** (Optional) Filters packets for display by the specified MAC address.
- **remote mep-id mep-id** (Optional) Filters packets for display by the remote MEP properties.
- **sent** (Optional) Displays only sent packets.
- **received** (Optional) Displays only received packets.
- **brief** (Optional) Displays brief information about each packet.
debug ethernet cfm packets

.full (Optional) Displays a full decode of each packet.

.hexdump (Optional) Displays a full decode and hexadecimal output of each packet.

Command Default
If no parameters are specified, all CFM packets are debugged and logged.

Command Modes
EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Caution

Enabling packet debugging without filters can have an adverse effect on the performance of the router. To avoid this, filters should always be specified to restrict the output to the domain, service, local MEP, interface, direction and packet type of interest.

Packets can be filtered for debugging by specifying any of the optional parameters.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following example shows a sample output of the `debug ethernet cfm packets` command with a full decode and hexadecimal output for sent and received CCM packets:

```
RP/0/RSP0/CPU0:router# debug ethernet cfm packets hexdump

RP/0/RSP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: GigabitEthernet0/1/0/0 ingress: CFM packet rcvd at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0402, dst MAC 0180.c200.0032: Packet processed successfully
RP/0/RSP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: CCM: Level 2, opcode CCM, version 0, RDI bit unset, interval 10s, seq. num 1, remote MEP ID 16, flags 0x05, first TLV offset 70, 0 unknown TLVs
RP/0/RSP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: CCM: MAID: MDID String 'dom4', SMAN String 'ser4'
RP/0/RSP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: CCM: Sender ID: Chassis ID Local 'hpr', Mgmt Addr <none>
RP/0/RSP0/CPU0:May 29 14:15:39.621 : cfmd[150]: PKT-RX: CCM: Port status: Up, interface status Up
RP/0/RSP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX: CCM: Port status: Up, interface status Up
RP/0/RSP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX: CCM: Port status: Up, interface status Up
RP/0/RSP0/CPU0:May 29 14:15:39.622 : cfmd[150]: PKT-RX: Raw Frame:
646f6d34 02047365 72340000 00000000 00000000 00000000 00000000 00000000
01d20400 01d10100 5030768 707200
RP/0/RSP0/CPU0:May 29 14:15:39.625 : cfmd[150]: PKT-TX: GigabitEthernet0/1/0/0 egress: CFM packet sent at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0402, dst MAC 0180.c200.0032
RP/0/RSP0/CPU0:May 29 14:15:39.625 : cfmd[150]: PKT-TX: CCM: Level 2, opcode CCM, version
```
Ethernet OAM Commands

debug ethernet cfm packets

0, RDI bit set, interval 10s, seq. num 16, remote MEP ID 1, flags 0x85, first TLV offset 70, 0 unknown TLVs
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: CCM: MAID: MDID String 'foo', SMAN String 'foo'
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: CCM: Sender ID: Chassis ID Local 'ios', Mgmt Addr <none>
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: CCM: Port status: Up, interface status Up
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: Raw Frame:
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: 0x40018546 00000010 00010403 666F6F02 03666F6F 00000000 00000000 00000000
RP/0/RSP0/CPU0:May 29 14:15:43.625 : cfmd[150]: PKT-TX: 0x00000000 00000000 00000200 01020400 01010100 05030769 6F7300

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ethernet cfm protocol-state, on page 172</td>
<td>Logs debug messages about CFM state machines and protocol events.</td>
</tr>
</tbody>
</table>
debug ethernet cfm protocol-state

To log debug messages about CFM state machines and protocol events, use the `debug ethernet cfm protocol-state` command in EXEC mode.

```
debug ethernet cfm protocol-state [domain domain-name [service service-name [mep-id mep-id]]]
[interface type interface-path-id [domain domain-name]]
```

**Syntax Description**

- **domain domain-name** (Optional) Filters information for display by the specified CFM maintenance domain, where `domain-name` is a string of up to 80 characters.

- **service service-name** (Optional) Filters information for display by the specified service name, where `service-name` is a string of up to 80 characters.

- **mep-id mep-id** (Optional) Filters information for display by the specified maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.

- **interface type interface-path-id** (Optional) Filters information for display by the specified physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

If no parameters are specified, all CFM state machines and protocol events are debugged and logged.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Debug messages can be filtered by specifying any of the optional parameters.

**Task ID**

- `ethernet-services` read

**Examples**

The following example shows a sample output of the `debug ethernet cfm protocol-state` command.

```
RP/0/RSP0/CPU0:router# debug ethernet cfm protocol-state
RP/0/RSP0/CPU0:May 29 14:41:49.966 : cfmd[150]: CFM: Created 1 local MEPs in PM and Engine
RP/0/RSP0/CPU0:May 29 14:41:49.967 : cfmd[150]: CFM: State changes notification for 1 EFPs
RP/0/RSP0/CPU0:May 29 14:42:14.143 : cfmd[150]: CFM: New remote MEP detected in domain foo, service foo for local MEP ID 1 on interface GigabitEthernet0/1/0/0; remote MEP ID 16, MAC 0001.0203.0402, errors: set: mismatched MAID; current: mismatched MAID;
```
RP/0/RSP0/CPU0:May 29 14:42:16.644 : cfmd[150]: CFM: Fault alarm notification for local MEP - domain: foo, service: foo, MEP ID: 1, interface: GigabitEthernet0/1/0/0, defect: cross-connect CCM

RP/0/RSP0/CPU0:May 29 14:43:32.247 : cfmd[150]: CFM: Initiated exploratory linktrace to ffff.ffff.ffff from MEP in domain foo, service foo, MEP ID 1, interface GigabitEthernet0/1/0/0 with ttl 64 and transaction ID 65537, reply-filtering Default and directed MAC None

May 29 14:43:49.155 : cfmd[150]: CFM: Remote MEP timed out in domain foo, service foo for local MEP ID 1 on interface GigabitEthernet0/1/0/0; remote MEP ID 16, MAC 0001.0203.0402, errors: cleared: mismatched MAID; current: none

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug ethernet cfm packets</strong>, on page 169</td>
<td>Logs debug messages about CFM packets that are sent or received by the Ethernet CFM process.</td>
</tr>
</tbody>
</table>
domain

To create and name a container for all domain configurations and enter the CFM domain configuration mode, use the `domain` command in CFM configuration mode. To remove the domain, use the `no` form of this command.

```
domain domain-name level level-value [id null [dns dns-name][mac H.H.H][string string]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain-name</code></td>
<td>Administrative name unique to this container, case sensitive ASCII string, up to 80 characters.</td>
</tr>
<tr>
<td><code>level</code></td>
<td>The CFM protocol level of this domain. Range is 0 to 7.</td>
</tr>
<tr>
<td><code>level-value</code></td>
<td>(Optional) Maintenance domain identifier (MDID) used in conjunction with one of the following keywords to specify the MDID type and value:</td>
</tr>
<tr>
<td><code>id</code></td>
<td>(Optional) null value ID, used with the <code>id</code> keyword.</td>
</tr>
<tr>
<td><code>null</code></td>
<td>(Optional) DNS name, up to 43 characters in length, used with the <code>id</code> keyword.</td>
</tr>
<tr>
<td><code>dns</code></td>
<td>(Optional) Hexadecimal MAC address, used with the <code>id</code> keyword.</td>
</tr>
<tr>
<td><code>mac</code></td>
<td>(Optional) Maintenance domain identifier (MDID) value, up to 43 characters in length, used with the <code>id</code> keyword.</td>
</tr>
<tr>
<td><code>string</code></td>
<td>(Optional) The domain name may be used here as the maintenance domain identifier (MDID) if desired.</td>
</tr>
</tbody>
</table>

### Command Default

If `id` is not specified, the domain name is used as the MDID.

### Command Modes

CFM configuration (config-cfm)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The level must be specified.

The maintenance domain identifier (MDID) is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.

Multiple domains may be specified at the same level. If the MDID is specified as NULL, the MAID is constructed as a short maintenance association name.
### Ethernet OAM Commands

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to create a domain and give it a domain name, level, and maintenance domain identifier (MDID):

```plaintext
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
<tr>
<td>mep domain, on page 242</td>
<td>Creates a MEP on an interface.</td>
</tr>
<tr>
<td>service, on page 270</td>
<td></td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
efd

To enable Ethernet Fault Detection (EFD) on all down Maintenance End Points (MEPs) in a down MEPs service, use the `efd` command in CFM domain service configuration mode. To disable EFD, use the `no` form of this command.

`efd {protection-switching}`

`no efd`

**Syntax Description**

- **protection-switching**: Enables protection switching, which causes high-priority notifications to be sent when peer MEPs specified for cross-check time out, or when CCMs are received with the RDI bit set.

  **Note**: The high-priority notifications only apply to MEPs that are offloaded. In the case of non-offloaded MEPs, enabling protection switching has no effect, and the command only enables EFD.

**Command Default**

EFD is disabled.

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

- **Release 3.9.1**: This command was introduced.
- **Release 4.3.1**: The `protection-switching` keyword was included.

**Usage Guidelines**

EFD can only be enabled for down MEPs within a down MEPs service. If the `efd` command is issued when any MEP in the service has any of the following error conditions, the MEP will shut down the interface:

- The MEP appears cross-connected to another MAID.
- The MEP is receiving invalid CCMs, such as receiving its own MAC or MEP-ID.
- All peer MEPs are reporting a state other than UP via the Port Status TLV.
- A peer MEP is reporting a state other than UP in Interface Status TLV.
- When cross-check is configured, and a session with an expected MEP times out, EFD is triggered on the local MEP.
- No CCMs are received from a peer MEP appearing in the configured cross-check list.
- An RDI is being received from a peer MEP.
- The MEP is receiving an AIS/LCK.

The MEP will bring the interface back up when the error condition is no longer detected.

**Note**

When an interface is shut down by a MEP using EFD, the MEP will continue to send and receive CCMs and other CFM messages.
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enable EFD:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# efd
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show efd interface, on page 275</td>
<td>Displays all interfaces that are shut down because of EFD.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
error-disable recovery cause

To configure error-disable to automatically attempt recovery, use the `error-disable recovery cause` command.

```
error-disable recovery cause {ethernet-oam-critical-event | ethernet-oam-link-fault | ...} [interval<30 - 1,000,000 >]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-oam-critical-event</td>
<td>Used when a critical event is detected by Ethernet Link OAM.</td>
</tr>
<tr>
<td>cause</td>
<td>One of the defined error-disable causes, for example: ethernet-oam-link-fault.</td>
</tr>
<tr>
<td>interval</td>
<td>Specifies the interval, in seconds, at which retries are attempted. The range is 30 to 1,000,000.</td>
</tr>
<tr>
<td>link-oam-link-fault</td>
<td>Used when a unidirectional link is detected by Ethernet Link OAM.</td>
</tr>
</tbody>
</table>

**Command Default**

Default interval period is 300 seconds.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When error disable recovery is enabled, the interface automatically recovers from the error-disabled state, and the device retries bringing the interface up.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows the full list of error-disable recovery causes:

```
RP/0/0/CPU0:ios(config)#error-disable recovery cause ?
cluster-udld    Used when UDLD is enabled on a Cluster port and UDLD is in aggressive mode and UDLD goes unidirectional
link-oam-capabilities-conflict peer Used when Ethernet Link OAM configuration conflicts with the peer
link-oam-critical-event Used when a critical event is detected by Ethernet Link OAM
link-oam-discovery-timeout Used when an Ethernet Link OAM session fails to come up in time
link-oam-dying-gasp Used when a dying gasp is detected by Ethernet Link OAM
link-oam-link-fault Used when a unidirectional link is detected by Ethernet OAM
link-oam-miswired Used when a mis-wiring is detected with Ethernet Link OAM
link-oam-session-down Used when an Ethernet Link OAM session goes down
link-oam-threshold-breached Used when a configured error threshold has been breached
pvrst-pvid-mismatch is different from the VLAN ID on which it was sent.
stp-bpdu-guard Used when an STP BPDU is received on a port on which BPDU
```
Guard is configured
stp-legacy-bpdu and RSTP BPDUs are supported
udld-loopback
  its Tx is directly connected to its Rx
udld-neighbor-mismatch
udld-timeout
udld-unidirectional

Used when a legacy BPDU is received on a port. Only MSTP
Used when UDLD detects that the port is in loopback mode (i.e.
  its Tx is directly connected to its Rx)
Used when mismatched neighbors are detected by UDLD
Used when all UDLD neighbors on the link have timed out
Used when a link is detected to be unidirectional
error-disable recovery cause

To configure error-disable to automatically attempt recovery, use the `error-disable recovery cause` command.

```
error-disable recovery cause {ethernet-oam-critical-event | ethernet-oam-link-fault | ...} [interval=<30 – 1,000,000>]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-oam-critical-event</td>
<td>Used when a critical event is detected by Ethernet Link OAM.</td>
</tr>
<tr>
<td>cause</td>
<td>One of the defined error-disable causes, for example: ethernet-oam-link-fault.</td>
</tr>
<tr>
<td>interval</td>
<td>Specifies the interval, in seconds, at which retries are attempted. The range is 30 to 1,000,000.</td>
</tr>
<tr>
<td>link-oam-link-fault</td>
<td>Used when a unidirectional link is detected by Ethernet Link OAM.</td>
</tr>
</tbody>
</table>

**Command Default**

Default interval period is 300 seconds.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When error disable recovery is enabled, the interface automatically recovers from the error-disabled state, and the device retries bringing the interface up.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows the full list of error-disable recovery causes:

```
RP/0/0/CP001:ios(config)#error-disable recovery cause ?
cluster-udld Used when UDLD is enabled on a Cluster port and UDLD is in aggressive mode and UDLD goes unidirectional
link-oam-capabilities-conflict Used when Ethernet Link OAM configuration conflicts with the peer
link-oam-critical-event Used when a critical event is detected by Ethernet Link OAM
link-oam-discovery-timeout Used when an Ethernet Link OAM session fails to come up in time
link-oam-dying-gasp Used when a dying gasp is detected by Ethernet Link OAM
link-oam-link-fault Used when a unidirectional link is detected by Ethernet Link OAM
link-oam-miswired Used when a mis-wiring is detected with Ethernet Link OAM
link-oam-session-down Used when an Ethernet Link OAM session goes down
link-oam-threshold-breached Used when a configured error threshold has been breached
pvrst-pvid-mismatch is different from the VLAN ID on which it was sent.
stp-bpdu-guard Used when an STP BPDU is received on a port on which BPDU
```
Guard is configured

- **stp-legacy-bpdu**
  - Used when a legacy BPDU is received on a port. Only MSTP and RSTP BPDUs are supported

- **udld-loopback**
  - Used when UDLD detects that the port is in loopback mode (i.e., its Tx is directly connected to its Rx)

- **udld-neighbor-mismatch**
  - Used when mismatched neighbors are detected by UDLD

- **udld-timeout**
  - Used when all UDLD neighbors on the link have timed out

- **udld-unidirectional**
  - Used when a link is detected to be unidirectional
ethernet cfm (global)

To enter Connectivity Fault Management (CFM) configuration mode, use the `ethernet cfm (global)` command in Global Configuration mode.

```
ethernet cfm
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
Global Configuration mode

**Command History**
Release 3.7.2  This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the CFM configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain, on page 174</td>
<td></td>
</tr>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
ethernet cfm (interface)

To enter interface CFM configuration mode, use the `ethernet cfm (interface)` command in interface configuration mode.

**ethernet cfm**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No MEPs are configured on the interface.

**Command Modes**
- Interface configuration (config-if)
- Subinterface configuration (config-subif)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.1.0</td>
<td>Support for subinterface configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enter interface CFM configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ethernet cfm
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cos (CFM), on page 168</td>
<td>Configures the CoS for all CFM packets generated by the MEP on an interface.</td>
</tr>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>mep domain, on page 242</td>
<td>Creates a MEP on an interface.</td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show ethernet cfm local maintenance-points</code>, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td><code>show ethernet cfm local meps</code>, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
ethernet lmi

To enable Ethernet Local Managment Interface (E-LMI) operation on an interface and enter interface Ethernet LMI configuration mode, use the `ethernet lmi` command in interface configuration mode. To disable Ethernet LMI and return to the default, use the `no` form of the command.

**ethernet lmi**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Ethernet LMI is disabled.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Ethernet LMI is supported only on physical Ethernet interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to enable Ethernet LMI on a Gigabit Ethernet interface and enter Ethernet LMI configuration mode:

```
RP/0/RSP0/CPU0:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (Ethernet), on page 72</td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
**ethernet oam**

To enable Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode, use the `ethernet oam` command in interface configuration mode. To disable Ethernet Link OAM, use the `no` form of this command.

```
ethernet oam
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

When enabled on an interface, the Ethernet Link OAM default values apply.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enable Ethernet Link OAM on an interface, the default Ethernet Link OAM values are applied to the interface. For the default Ethernet Link OAM values, see the related Ethernet Link OAM commands.

**Task ID**

| ethernet-services | read, write |

**Examples**

The following example shows how to enable Ethernet Link OAM and enter interface Ethernet OAM configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)#
```
ethernet oam loopback

To start or stop a loopback at the remote end of an Ethernet OAM interface, use the `ethernet oam loopback` command in EXEC mode.

```
ethernet oam loopback {enable | disable} type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Starts a loopback at the remote end.</td>
</tr>
<tr>
<td>disable</td>
<td>Stops the loopback at the remote end.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

- Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

Loopback is not enabled.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command puts the remote peer device into loopback mode. This means that all traffic sent to the peer is looped back, which means that it is sent back from the peer and received by the router. All traffic received from the peer device is discarded.

This command returns when the OAM client receives confirmation from the remote end that the remote loopback has been enabled or disabled. If no response or a failure response is received, an error is returned.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to start a loopback at the far end of an Ethernet OAM interface.

```
RP/0/RSP0/CPU0:router# ethernet oam loopback enable tengigabitethernet 0/6/1/0
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote-loopback, on page 260</td>
<td>Enables a remote loopback on the far end of an Ethernet OAM interface.</td>
</tr>
<tr>
<td>action remote-loopback, on page 127</td>
<td>Configures what action is taken on an interface when a remote-loopback event occurs.</td>
</tr>
<tr>
<td>snmp-server traps ethernet oam events, on page 347</td>
<td></td>
</tr>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
</tbody>
</table>
ethernet oam profile

To create an Ethernet Operations, Administration and Maintenance (EOAM) profile and enter EOAM configuration mode, use the ethernet oam profile command in global configuration mode. To delete an EOAM profile, use the no form of this command.

```
ethernet oam profile  profile-name
```

**Syntax Description**

| profile-name | Text string name of the OAM profile. The maximum length is 32 bytes. |

**Command Default**

No default behavior or values

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can delete an EOAM profile, you must remove the profile from all interfaces to which it is attached.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to create an Ethernet OAM profile and enter Ethernet OAM configuration mode:

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)#
```
**ethernet sla**

To enter the Ethernet Service Level Agreement (SLA) configuration mode, use the `ethernet sla` command in Global Configuration mode.

```
ethernet sla
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the Ethernet SLA configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)#
```
ethernet sla on-demand operation type cfm-delay-measurement probe

To execute an on-demand Ethernet SLA operation probe for CFM delay measurement, use the `ethernet sla on-demand operation type cfm-delay-measurement probe` command in EXEC mode.

```xml
<groupcomp>
<kwd>ethernet</kwd>
<sep></sep>
<kwd>sla</kwd>
<sep></sep>
<kwd>on-demand</kwd>
<sep></sep>
<kwd>operation</kwd>
<sep></sep>
<kwd>type</kwd>
<sep></sep>
<groupchoice>
<kwd>cfm-delay-measurement</kwd>
<kwd>cfm-delay-measurement-v0</kwd>
</groupchoice>
<sep></sep>
<kwd>probe</kwd>
<sep></sep>
<groupcompimportance='optional'>
<kwd>priority</kwd>
<sep></sep>
<kwd>number</kwd>
</groupcomp>
<sep></sep>
<groupcompimportance='optional'>
<kwd>send</kwd>
<sep></sep>
</groupcomp>
```
ethernet sla on-demand operation type cfm-delay-measurement probe

packet

once every number milliseconds seconds minutes hours burst once every number seconds minutes hours

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
ethernet sla on-demand operation type cfm-delay-measurement probe
<kwd>hex</kwd>
<kwd>0x</kwd>
<kwd>HHHHHHHHH</kwd>
<kwd>pseudo-random</kwd>
<kwd>domain</kwd>
<kwd>domain_name</kwd>
<kwd>source</kwd>
<kwd>interface</kwd>
<kwd>type</kwd>
<kwd>interface-path-id</kwd>
<kwd>target</kwd>
<kwd>mac-address</kwd>
<kwd>H</kwd>
<kwd>H</kwd>
ethernet sla on-demand operation type cfm-delay-measurement probe

</groupcomp>
<sep> </sep>
<groupcomp >
<delim>.</delim>
<kwd>H</kwd>
</groupcomp>
<sep> </sep>
<groupcomp >
<delim>.</delim>
<kwd>H</kwd>
</groupcomp>
</groupcomp>

<kwd>mep-id</kwd>
<sep> </sep>
<kwd>id_number</kwd>
</groupcomp>
</groupchoice>
<sep> </sep>
<groupcomp importance='optional' >
<kwd>statistics</kwd>
<sep> </sep>
<kwd>measure</kwd>
<sep> </sep>
</groupcomp>
</groupchoice>
<sep> </sep>
<groupchoice >
<kwd>one-way-delay-ds</kwd>
<kwd>one-way-delay-sd</kwd>
<kwd>one-way-jitter-ds</kwd>
<kwd>one-way-jitter-sd</kwd>
<kwd>round-trip-delay</kwd>
<kwd>round-trip-jitter</kwd>
</groupchoice>
<sep> </sep>
<groupcomp importance='optional' >
aggregate

<groupchoice>
  none
<groupcomp>
  bins
<sep>
  number
<sep>
  width
<sep>
  milliseconds
</groupcomp>
</groupchoice>

<groupchoice>
  archive
  number
</groupchoice>
<groupchoice>
  size
  number
</groupchoice>
<groupchoice>
  per-probe
  probes
</groupchoice>

ethernet sla on-demand operation type clm-delay-measurement probe
ethernet sla on-demand operation type cfm-delay-measurement probe
ethernet sla on-demand operation type cfm-delay-measurement probe

</groupcomp>
<groupcomp>
<kwd>in</kwd>
<sep></sep>
<kwd>number</kwd>
<sep></sep>
<groupchoice>
<kwd>seconds</kwd>
<kwd>minutes</kwd>
<kwd>hours</kwd>
</groupchoice>
</groupcomp>
</groupchoice>
<sep></sep>
<groupcompimportance='optional'>
<kwd>for</kwd>
<sep></sep>
<kwd>duration</kwd>
<sep></sep>
<groupchoice>
<kwd>seconds</kwd>
<kwd>minutes</kwd>
<kwd>hours</kwd>
</groupchoice>
</groupcomp>
<sep></sep>
<groupcompimportance='optional'>
<kwd>repeat</kwd>
<sep></sep>
<kwd>every</kwd>
<sep></sep>
<kwd>number</kwd>
<sep></sep>
<groupchoice>
<kwd>seconds</kwd>  
<kwd>minutes</kwd>  
<kwd>hours</kwd>  
</groupchoice>  
</sep>  
<kwd>count</kwd>  
</sep>  
<kwd>probes</kwd>  
</groupcomp>  
</groupcomp>  
<kwd.importance='optional'>asynchronous</kwd>  
</groupcomp>  

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>priority number</strong></td>
<td>(Optional) Configures the priority of outgoing SLA probe packets. The range is 0 to 7. The default is to use the COS bits for the egress interface.</td>
</tr>
<tr>
<td><strong>send packet once</strong></td>
<td>(Optional) Sends one packet one time.</td>
</tr>
<tr>
<td>**send packet every number {milliseconds</td>
<td>seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 3600 <code>seconds</code></td>
</tr>
<tr>
<td></td>
<td>• 1 to 1440 <code>minutes</code></td>
</tr>
<tr>
<td></td>
<td>• 1 to 168 <code>hours</code></td>
</tr>
<tr>
<td></td>
<td>• 100 to 10000 <code>milliseconds</code></td>
</tr>
<tr>
<td></td>
<td>(specified in increments of 100)</td>
</tr>
<tr>
<td><strong>send burst once</strong></td>
<td>(Optional) Specifies that a burst of packets is sent one time. This is the default.</td>
</tr>
</tbody>
</table>
send burst every *number* {seconds | minutes | hours}  
(Optional) Sends a burst of packets every specified number of seconds, minutes, or hours, where *number* is in the following range:

- 1–3600 **seconds**
- 1–1440 **minutes**
- 1–168 **hours**

The default is to send a burst every 10 seconds.

**packet count number**  
Specifies the number of packets to be sent in a burst, in the range 2 to 600. The default is 10.

**interval number {milliseconds | seconds}**  
Specifies the time between sending packets in a burst, where *number* is in the following range:

- 100 to 30000 **milliseconds**
- 1 to 30 **seconds**

**Note**  
The total length of a burst (the packet count multiplied by the interval) must not exceed 1 minute.

**packet size bytes**  
Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.

**test pattern hex 0x HHHHHHHHH**  
(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.

**domain domain-name**  
Specifies the name of the domain for the locally defined CFM MEP.

**source interface type**  
Specifies the source interface type of the locally defined CFM MEP. For more information, use the question mark (?) online help function.
**interface-path-id**

Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**target mac-address H.H.H**

Specifies the MAC address (in dotted hexadecimal format) of the target MEP that is known to the local MEP for the probe.

**target mep-id id-number**

Specifies the ID (from 1 to 8191) of the target MEP that is known to the local MEP for the probe.

**statistics measure**

(Optional) Specifies the type of statistics to collect:

- **one-way-delay-ds**—One-way delay statistics from destination to source.
- **one-way-delay-sd**—One-way delay statistics from source to destination.
- **one-way-jitter-ds**—One-way delay jitter from destination to source.
- **one-way-jitter-sd**—One-way delay jitter from source to destination.
- **round-trip-delay**—Round-trip delay statistics.
- **round-trip-jitter**—Round-trip jitter statistics.

All statistics are collected by default.

**aggregate none**

(Optional) Specifies that statistics are not aggregated into bins, and each statistic is stored individually.

**Caution**

This option can be memory-intensive and should be used with care.
### Aggregate Bins

**aggregate bins number**

(Optional) Specifies the number of bins (from 2 to 100) within each bucket to store sample packets from the probe. The default is to aggregate into one bin.

### Width

**width milliseconds**

Specifies the range of the samples to be collected within each bin in milliseconds, from 1 to 10000. Based on the specified width, bins are established in the following way:

- **Delay measurements** (round-trip or one-way)—The lower bound of the bins is zero and the first bin’s upper limit is 0 plus the specified width, and the last bin is unbounded.
- **Jitter measurements** (round-trip or one-way)—The bins are evenly distributed around zero, with both the lowest and highest numbered bins being unbounded.

See the Usage Guidelines for more information.

### Buckets Archive

**buckets archive number**

(Optional) Specifies the number of buckets to store in memory from 1 to 100. The default is 100.

### Buckets Size

**buckets size number**

(Optional) Specifies the number of buckets to be used for probes from 1 to 100. The default is 1.

### Per-Probe

**per-probe**

Specifies that probes span multiple buckets.

### Probes

**probes**

Specifies that buckets span multiple probes.

### Schedule Now

**schedule now**

(Optional) Specifies that the probe begins as soon as you enter the command. This is the default.

### Schedule At

**schedule at hh:mm**

(Optional) Specifies a specific time at which to start the probe in 24-hour notation.

### SS

**ss**

(Optional) Number of seconds into the next minute at which to start the probe.
**day**  
(Optional) Number in the range 1 to 31 of the day of the month on which to start the probe.

**month**  
(Optional) Name of the month (full word in English) in which to start the probe.

**year**  
(Optional) Year (fully specified as 4 digits) in which to start the probe.

**schedule in number {seconds | minutes | hours}**  
(Optional) Specifies a relative time, as a number of seconds, minutes or hours from the current time, at which to start the probe, where `number` is in the following ranges:
- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours

**for duration {seconds | minutes | hours}**  
(Optional) Specifies the length of the probe as a number of seconds, minutes, or hours, where `number` is in the following ranges:
- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours

**Note**  
The duration should not exceed the interval specified by the `repeat every` option.

**repeat every number {seconds | minutes | hours}**  
(Optional) Specifies the interval at which to restart the probe as a number of seconds, minutes, or hours, where `number` is in the following ranges:
- 1 to 90 seconds
- 1 to 90 minutes
- 1 to 24 hours

The default is that probes are not repeated, and there is no default interval.

**count probes**  
Specifies the number of probes to run in the range 1–100. There is no default.
asynchronous

(Optional) Specifies that the command displays the on-demand operation ID and exits immediately, with the operation continuing in the background.

The default is synchronous and the operation displays the on-demand operation ID and all results on the console when it completes.

Command Default

No on-demand operations are configured or executed.

Command Modes

EXEC mode

Command History

Release    Modification
Release 4.0.0  This command was introduced.
Release 4.3.0  The cfm-delay-measurement-v0 option was included.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows how to enter the most basic SLA on-demand operation to measure CFM delay statistics. This example implements these defaults:

- Send a burst once for a packet count of 10 and interval of 1 second (10-second probe).
- Use default class of service (CoS) for the egress interface.
- Measure all statistics, including both one-way and round-trip delay and jitter statistics.
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

RP/0/RSP0/CPU0:router# ethernet sla on-demand operation type cfm-delay-measurement probe domain D1 source interface TenGigE 0/6/1/0 target mep-id 100

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet sla statistics all, on page 156</td>
<td>Deletes the contents of buckets containing SLA statistics collected by all operations probes.</td>
</tr>
<tr>
<td>clear ethernet sla statistics on-demand, on page 157</td>
<td>Deletes the contents of buckets containing SLA statistics collected by on-demand probes.</td>
</tr>
<tr>
<td>show ethernet sla operations, on page 329</td>
<td>Displays information about configured Ethernet SLA operations.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet sla statistics, on page 332</code></td>
<td>Displays the contents of buckets containing Ethernet SLA metrics collected by probes.</td>
</tr>
</tbody>
</table>
To execute an on-demand Ethernet SLA operation probe for CFM loopback measurement, use the `ethernet sla on-demand operation type cfm-loopback probe` command in EXEC mode.

```
ethernet sla on-demand operation type cfm-delay-measurement cfm-delay-measurement-v0probe
[priority number]
send {packet {once | every number {milliseconds | seconds | minutes | hours}}} | burst {once | every number {seconds | minutes | hours}} packet count number interval number {milliseconds | seconds}
[packet size bytes [test pattern {hex 0x HHHHHH | pseudo-random}]}
domain domain_name source interface type interface-path-id target {mac-address H.H.H.H | mep-id id_number}
[ statistics measure {one-way-delay-ds | one-way-delay-sd | one-way-jitter-ds | one-way-jitter-sd | round-trip-delay | round-trip-jitter}
aggregate {none | bins number width milliseconds}
buckets {archive number | size number {per-probe | probes}}
schedule {now | at hh:mm:ss [day month year] | in number {seconds | minutes | hours}}
for duration {seconds | minutes | hours}
repeat every number {seconds | minutes | hours} count probes
[asynchronous]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>priority number</code></td>
<td>(Optional) Configures the priority of outgoing SLA probe packets. The range is 0 to 7. The default is to use the COS bits for the egress interface.</td>
</tr>
<tr>
<td><code>send packet once</code></td>
<td>(Optional) Sends one packet one time.</td>
</tr>
<tr>
<td>`send packet every number {milliseconds</td>
<td>seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 1440 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1 to 168 hours</td>
</tr>
<tr>
<td></td>
<td>• 100 to 10000 milliseconds (specified in increments of 100)</td>
</tr>
<tr>
<td><code>send burst once</code></td>
<td>(Optional) Specifies that a burst of packets is sent one time. This is the default.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>send burst every</td>
<td>Sends a burst of packets every specified number of seconds, minutes, or hours, where number is in the following range:</td>
</tr>
<tr>
<td>number {seconds</td>
<td>- 1–3600 seconds</td>
</tr>
<tr>
<td>minutes</td>
<td>hours}</td>
</tr>
<tr>
<td></td>
<td>- 1–168 hours</td>
</tr>
<tr>
<td>The default is to send a burst every 10 seconds.</td>
<td></td>
</tr>
<tr>
<td>packet count</td>
<td>Specifies the number of packets to be sent in a burst, in the range 2 to 600. The default is 10.</td>
</tr>
<tr>
<td>number</td>
<td></td>
</tr>
<tr>
<td>interval</td>
<td>Specifies the time between sending packets in a burst, where number is in the following range:</td>
</tr>
<tr>
<td>number {milliseconds</td>
<td>seconds}</td>
</tr>
<tr>
<td></td>
<td>- 1 to 30 seconds</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The total length of a burst (the packet count multiplied by the interval) must not exceed 1 minute.</td>
</tr>
<tr>
<td>packet size</td>
<td>Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.</td>
</tr>
<tr>
<td>bytes</td>
<td></td>
</tr>
<tr>
<td>test pattern hex</td>
<td>Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.</td>
</tr>
<tr>
<td>0x HHHHHHHHH</td>
<td></td>
</tr>
<tr>
<td>test pattern</td>
<td>Specifies a pseudo-random bit sequence determined by the protocol to fill the outgoing probe packet to the specified minimum packet size.</td>
</tr>
<tr>
<td>pseudo-random</td>
<td></td>
</tr>
<tr>
<td>domain</td>
<td>Specifies the name of the domain for the locally defined CFM MEP.</td>
</tr>
<tr>
<td>domain-name</td>
<td></td>
</tr>
</tbody>
</table>
### ethernet sla on-demand operation type cfm-loopback probe

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source interface <strong>type</strong></td>
<td>Specifies the source interface type of the locally defined CFM MEP. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>target mac-address <strong>H.H.H.H</strong></td>
<td>Specifies the MAC address (in dotted hexadecimal format) of the target MEP that is known to the local MEP for the probe.</td>
</tr>
<tr>
<td>target mep-id <strong>id-number</strong></td>
<td>Specifies the ID (from 1 to 8191) of the target MEP that is known to the local MEP for the probe.</td>
</tr>
<tr>
<td>statistics measure</td>
<td>(Optional) Specifies the type of statistics to collect:</td>
</tr>
<tr>
<td></td>
<td>• <strong>one-way-delay-ds</strong>—One-way delay statistics from destination to source.</td>
</tr>
<tr>
<td></td>
<td>• <strong>one-way-delay-sd</strong>—One-way delay statistics from source to destination.</td>
</tr>
<tr>
<td></td>
<td>• <strong>one-way-jitter-ds</strong>—One-way jitter statistics from destination to source.</td>
</tr>
<tr>
<td></td>
<td>• <strong>one-way-jitter-sd</strong>—One-way jitter statistics from source to destination.</td>
</tr>
<tr>
<td></td>
<td>• <strong>round-trip-delay</strong>—Round-trip delay statistics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>round-trip-jitter</strong>—Round-trip jitter statistics.</td>
</tr>
</tbody>
</table>

All statistics are collected by default.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate none</td>
<td>(Optional) Specifies that statistics are not aggregated into bins, and each statistic is stored individually.</td>
</tr>
<tr>
<td>aggregate bins number</td>
<td>(Optional) Specifies the number of bins (from 2 to 100) within each bucket to store sample packets from the probe. The default is to aggregate into one bin.</td>
</tr>
<tr>
<td>width milliseconds</td>
<td>Specifies the range of the samples to be collected within each bin in milliseconds, from 1 to 10000. Based on the specified width, bins are established in the following way:</td>
</tr>
<tr>
<td></td>
<td>• Delay measurements (round-trip or one-way)—The lower bound of the bins is zero and the first bin’s upper limit is 0 plus the specified width, and the last bin is unbounded.</td>
</tr>
<tr>
<td></td>
<td>• Jitter measurements (round-trip or one-way)—The bins are evenly distributed around zero, with both the lowest and highest numbered bins being unbounded.</td>
</tr>
<tr>
<td></td>
<td>See the Usage Guidelines for more information.</td>
</tr>
<tr>
<td>buckets archive number</td>
<td>(Optional) Specifies the number of buckets to store in memory from 1 to 100. The default is 100.</td>
</tr>
<tr>
<td>buckets size number</td>
<td>(Optional) Specifies the number of buckets to be used for probes from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td>per-probe</td>
<td>Specifies that probes span multiple buckets.</td>
</tr>
<tr>
<td>probes</td>
<td>Specifies that buckets span multiple probes.</td>
</tr>
</tbody>
</table>
### schedule now
(Optional) Specifies that the probe begins as soon as you enter the command. This is the default.

### schedule at *hh:mm:ss*
(Optional) Specifies a specific time at which to start the probe in 24-hour notation.

### day
(Optional) Number in the range 1 to 31 of the day of the month on which to start the probe.

### month
(Optional) Name of the month (full word in English) in which to start the probe.

### year
(Optional) Year (fully specified as 4 digits) in which to start the probe.

### schedule in *number* {seconds | minutes | hours}
(Optional) Specifies a relative time, as a number of seconds, minutes or hours from the current time, at which to start the probe, where *number* is in the following ranges:
- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours

### for duration {seconds | minutes | hours}
(Optional) Specifies the length of the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges:
- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours

**Note** The duration should not exceed the interval specified by the `repeat every` option.
**repeat every number {seconds | minutes | hours}**

(Optional) Specifies the interval at which to restart the probe as a number of seconds, minutes, or hours, where *number* is in the following ranges:

- 1 to 90 *seconds*
- 1 to 90 *minutes*
- 1 to 24 *hours*

The default is that probes are not repeated, and there is no default interval.

**count probes**

Specifies the number of probes to run in the range 1–100. There is no default.

**asynchronous**

(Optional) Specifies that the command displays the on-demand operation ID and exits immediately, with the operation continuing in the background.

The default is synchronous and the operation displays the on-demand operation ID and all results on the console when it completes.

---

**Command Default**

No on-demand operations are configured or executed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The <code>cfm-delay-measurement-v0</code> keyword was included.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the most basic SLA on-demand operation to measure CFM loopback statistics. This example implements the following defaults:

- Send a burst once for a packet count of 10 and interval of 1 second (10-second probe).
- Use default test pattern of 0’s for padding.
- Use default class of service (CoS) for the egress interface.
- Measure all statistics.
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

RP/0/RSP0/CPU0:router# ethernet sla on-demand operation type cfm-loopback
   probe packet size 1500 domain D1 source interface TenGigE 0/6/1/0 target mep-id 100

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet sla statistics all, on page 156</td>
<td>Deletes the contents of buckets containing SLA statistics collected by all operations probes.</td>
</tr>
<tr>
<td>clear ethernet sla statistics on-demand, on page 157</td>
<td>Deletes the contents of buckets containing SLA statistics collected by on-demand probes.</td>
</tr>
<tr>
<td>show ethernet sla operations, on page 329</td>
<td>Displays information about configured Ethernet SLA operations.</td>
</tr>
<tr>
<td>show ethernet sla statistics, on page 332</td>
<td>Displays the contents of buckets containing Ethernet SLA metrics collected by probes.</td>
</tr>
</tbody>
</table>
To execute an on-demand Ethernet SLA operation probe for CFM synthetic loss measurement, use the `ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe` command in EXEC mode.

```
ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe [priority number] [send {packet {once | every number {milliseconds | seconds | minutes | hours}} | burst {once | every number {seconds | minutes | hours}}] packet count number interval number {milliseconds | seconds} | burst calculation packets number | packet size bytes [test pattern hex 0x HHHHHHHH] | domain domain_name source interface type interface-path-id target {mac-address H.H.H.H | mep-id id_number} | statistics measure {one-way-loss-sd | one-way-loss-ds} | aggregate {none | bins number width count}] | buckets {archive number | size number | per-probe | probes}] | [schedule {now | at hh:mm [ss] | day [month [year]]} | in number {seconds | minutes | hours}] | for duration {seconds | minutes | hours}] | [repeat every number {seconds | minutes | hours} | count probes]] [asynchronous]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>priority number</strong></td>
<td>(Optional) Configures the priority of outgoing SLA probe packets. The range is 0 to 7. The default is to use the COS bits for the egress interface.</td>
</tr>
<tr>
<td><strong>send packet once</strong></td>
<td>(Optional) Sends one packet one time.</td>
</tr>
<tr>
<td>**send packet every number {milliseconds</td>
<td>seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 1440 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1 to 168 hours</td>
</tr>
<tr>
<td></td>
<td>• 100 to 10000 milliseconds (specified in increments of 100)</td>
</tr>
<tr>
<td><strong>send burst once</strong></td>
<td>(Optional) Specifies that a burst of packets is sent one time. This is the default.</td>
</tr>
<tr>
<td>**send burst every number {</td>
<td>seconds</td>
</tr>
<tr>
<td></td>
<td>• 1–3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• 1–1440 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1–168 hours</td>
</tr>
<tr>
<td></td>
<td>The default is to send a burst every 10 seconds.</td>
</tr>
<tr>
<td><strong>packet count number</strong></td>
<td>Specifies the number of packets to be sent in a burst, in the range 2 to 600. The default is 10.</td>
</tr>
</tbody>
</table>
The document provides detailed information about configuring Ethernet Operations, Administration, and Management (OAM) commands for Cisco ASR 9000 Series Routers. The specific commands and their functionalities are as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval number {milliseconds</td>
<td>seconds}</td>
</tr>
<tr>
<td></td>
<td>• 100 to 3000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>• 1 to 30 seconds</td>
</tr>
<tr>
<td>Note</td>
<td>The total length of a burst (the packet count multiplied by the interval) must not exceed 1 minute.</td>
</tr>
<tr>
<td>packet size bytes</td>
<td>Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value is the total frame size including the Layer 2 or Layer 3 packet header.</td>
</tr>
<tr>
<td>test pattern hex 0x HHHHHHHHH</td>
<td>(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.</td>
</tr>
<tr>
<td>synthetic loss calculation packets number</td>
<td>Defines the number of packets that must be used to make each FLR calculation for synthetic loss measurements. It ranges from 10 to 12096000.</td>
</tr>
<tr>
<td>domain domain-name</td>
<td>Specifies the name of the domain for the locally defined CFM MEP.</td>
</tr>
<tr>
<td>source interface type</td>
<td>Specifies the source interface type of the locally defined CFM MEP. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>target mac-address H.H.H</td>
<td>Specifies the MAC address (in dotted hexadecimal format) of the target MEP that is known to the local MEP for the probe.</td>
</tr>
<tr>
<td>target mep-id id-number</td>
<td>Specifies the ID (from 1 to 8191) of the target MEP that is known to the local MEP for the probe.</td>
</tr>
<tr>
<td>statistics measure</td>
<td>(Optional) Specifies the type of statistics to collect:</td>
</tr>
<tr>
<td></td>
<td>• one-way-loss-ds—One-way loss statistics from destination to source.</td>
</tr>
<tr>
<td></td>
<td>• one-way-loss-sd—One-way loss statistics from source to destination.</td>
</tr>
</tbody>
</table>
aggregate none
(Optional) Specifies that statistics are not aggregated into bins, and each statistic is stored individually.

Caution This option can be memory-intensive and should be used with care.

aggregate bins number
(Optional) Specifies the number of bins (from 2 to 100) within each bucket to store sample packets from the probe. The default is to aggregate into one bin.

width count
Specifies the range of the samples to be collected within each bin in percentage points, from 1 to 100.

buckets archive number
(Optional) Specifies the number of buckets to store in memory from 1 to 100. The default is 100.

buckets size number
(Optional) Specifies the number of buckets to be used for probes from 1 to 100. The default is 1.

per-probe
Specifies that probes span multiple buckets.

probes
Specifies that buckets span multiple probes.

schedule now
(Optional) Specifies that the probe begins as soon as you enter the command. This is the default.

schedule at hh:mm
(Optional) Specifies a specific time at which to start the probe in 24-hour notation.

ss
(Optional) Number of seconds into the next minute at which to start the probe.

day
(Optional) Number in the range 1 to 31 of the day of the month on which to start the probe.

month
(Optional) Name of the month (full word in English) in which to start the probe.

year
(Optional) Year (fully specified as 4 digits) in which to start the probe.

schedule in number {seconds | minutes | hours}
(Optional) Specifies a relative time, as a number of seconds, minutes or hours from the current time, at which to start the probe, where number is in these ranges:

- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours
**for duration {seconds | minutes | hours}**

(Optional) Specifies the length of the probe as a number of seconds, minutes, or hours, where *number* is in these ranges:

- 1 to 3600 *seconds*
- 1 to 1440 *minutes*
- 1 to 24 *hours*

**Note** The duration should not exceed the interval specified by the repeat every option.

**repeat every number {seconds | minutes | hours}**

(Optional) Specifies the interval at which to restart the probe as a number of seconds, minutes, or hours, where *number* is in these ranges:

- 1 to 90 *seconds*
- 1 to 90 *minutes*
- 1 to 24 *hours*

The default is that probes are not repeated, and there is no default interval.

**count probes**

Specifies the number of probes to run in the range 1–100. There is no default.

**asynchronous**

(Optional) Specifies that the command displays the on-demand operation ID and exits immediately, with the operation continuing in the background.

The default is synchronous and the operation displays the on-demand operation ID and all results on the console when it completes.

---

**Command Default**

No on-demand operations are configured or executed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>
Example

This example shows a minimum configuration, that specifies the local domain and source interface and target MEP, using these defaults:

- Send a burst once for a packet count of 100 and interval of 100 milliseconds.
- The number of packets to be used for FLR calculation is 100.
- Measure the one way loss statistics in both the directions.
- Aggregate statistics into one bin.
- Schedule now.
- Display results on the console.

RP/0/RSP0/CPU0:router#ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe
    domain D1 source interface TenGigE 0/6/1/0 target mac-address 2.3.4

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet sla statistics all, on page 156</td>
<td>Deletes the contents of buckets containing SLA statistics collected by all operations probes.</td>
</tr>
<tr>
<td>clear ethernet sla statistics on-demand, on page 157</td>
<td>Deletes the contents of buckets containing SLA statistics collected by on-demand probes.</td>
</tr>
<tr>
<td>show ethernet sla operations, on page 329</td>
<td>Displays information about configured Ethernet SLA operations.</td>
</tr>
<tr>
<td>show ethernet sla statistics, on page 332</td>
<td>Displays the contents of buckets containing Ethernet SLA metrics collected by probes.</td>
</tr>
</tbody>
</table>
ethernet udld reset interface

To reset the UDLD protocol state for a specified interface or for all interfaces, use the `ethernet udld reset interface` command in the Ethernet Interface Configuration mode.

```
ethernet udld reset interface [interface type | all]
```

**Syntax Description**

- `interface type` (Optional) Specifies the interface type for which the UDLD protocol state needs to be reset.
- `all` (Optional) Resets the UDLD state for all interfaces.

**Command Default**

No default behavior or values

**Command Modes**

Ethernet Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to run the `ethernet udld reset interface` command:

```
RP/0/RSP0/CPU0:router# ethernet udld reset interface GigabitEthernet 0/10/0/11
```
ethernet uni id

To specify a name for the Ethernet User-Network Interface (UNI) link, use the `ethernet uni id` command in interface configuration mode.

```
ethernet uni id  name
```

**Syntax Description**

- **name**  Maximum of 64 characters to identify the Ethernet UNI link.

**Command Default**

No name is specified for the Ethernet UNI link.

**Command Modes**

Interface (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The UNI name should be unique among all UNIs that are part of a given Ethernet Virtual Connection (EVC). When the Ethernet Local Management Interface (E-LMI) protocol is running on the UNI, the name specified in the `ethernet uni id` command is advertised by E-LMI to the Customer Edge (CE) device. It is also carried in Ethernet Connectivity Fault Management (CFM) Continuity Check Messages (CCMs) if there is an Up MEP on the UNI, and passed to E-LMI on the peer MEP so that it can be advertised to the remote CE device.

**Task ID**

```
Task ID  Operation
interface  read, write
```

The following example shows how to configure the UNI name called "PE1-CustA-Slot0-Port0" on Gigabit Ethernet interface 0/0/0/0:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet uni id PE1-CustA-Slot0-Port0
```

**Related Commands**

```
Command                      Description
interface (Ethernet), on page 72  Specifies or creates an Ethernet interface and enters interface configuration mode.
```
extension remote-uni disable

To disable transmission of the Cisco-proprietary Remote UNI Details information element in Ethernet LMI (E-LMI) STATUS messages, use the `extension remote-uni disable` command in interface Ethernet LMI configuration mode. To return to the default, use the `no` form of the command.

**extension remote-uni disable**

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco-proprietary Remote UNI Details information element is sent in E-LMI STATUS messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Ethernet LMI configuration (config-if-elmi)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the <code>extension remote-uni disable</code> command to have stricter conformance to the MEF 16 E-LMI specification for information elements in STATUS messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to disable transmission of the Cisco-proprietary Remote UNI Details information element:

```
RP/0/RSP0/CPU0:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)# extension remote-uni disable
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface (Ethernet), on page 72</code></td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><code>ethernet lmi, on page 185</code></td>
<td>Enables E-LMI operation on an interface and enters interface Ethernet LMI configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
**frame-period threshold**

To configure the thresholds that trigger an Ethernet OAM frame-period error event, use the `frame-period threshold` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the `no` form of this command.

```
frame-period threshold {frames [low threshold [thousand | million | billion ]]|high threshold [thousand | million | billion ]}|ppm [low threshold ][high threshold ]
```

### Syntax Description

- **low threshold** (Optional) Low threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000.
- **high threshold** (Optional) High threshold, in frames, that triggers a frame-period error event. The range is 0 to 1000000. The high threshold value can be configured only in conjunction with the low threshold value.

### Command Default

The default low threshold is 1 ppm.

### Command Modes

- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

### Usage Guidelines

The frame period window is defined in the IEEE specification as a number of received frames, in our implementation it is x milliseconds.

To obtain the number of frames, the configured time interval is converted to a window size in frames using the interface speed. For example, for a 1Gbps interface, the IEEE defines minimum frame size as 512 bits. So, we get a maximum of approximately 1.5 million frames per second. If the window size is configured to be 8 seconds (8000ms) then this would give us a Window of 12 million frames in the specification's definition of Errored Frame Window.

The thresholds for frame-period are measured in errors per million frames. Hence, if you configure a window of 8000ms (that is a window of 12 million frames) and a high threshold of 100, then the threshold would be crossed if there are 1200 errored frames in that period (that is, 100 per million for 12 million).

When the low threshold is passed, a frame-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to configure the low and high thresholds that trigger a frame-period error event.

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# frame-period threshold ppm low 100 high 600000
```
frame-period window

To configure the window size for an Ethernet OAM frame-period error event, use the `frame-period window` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the `no` form of this command.

```
frame-period window {milliseconds window | frames window [thousand | million | billion]}
```

### Syntax Description

| window | Size of the window for a frame-period error in milliseconds. The range is 100 to 60000. |

### Command Default

The default value is 1000 milliseconds.

### Command Modes

- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.1.32</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The IEEE 802.3 standard defines the window size as number of frames rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed. Note that the conversion assumes that all frames are of the minimum size.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure the window size for a frame-period error.

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# frame-period window milliseconds 60000
```
frame-seconds threshold

To configure the thresholds that trigger a frame-seconds error event, use the `frame-seconds threshold` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the `no` form of this command.

```
frame-seconds threshold low threshold [high threshold]
```

**Syntax Description**

- `low threshold` (Optional) Low threshold, in seconds, that triggers a frame-seconds error event. The range is 0 to 900.
- `high threshold` (Optional) High threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900. The high threshold value can be configured only in conjunction with the low threshold value.

**Command Default**
The default value is 1.

**Command Modes**
- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the low threshold is passed, a frame-seconds error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

**Task ID**

- **Task ID**: ethernet-services
- **Operations**: read, write

**Examples**

The following example shows how to configure the low and high thresholds that trigger a frame-seconds error event:

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor {config-eoam}# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# frame-seconds threshold low 10 high 900
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>link-monitor, on page 229</td>
<td>Enters Ethernet OAM link monitor configuration mode.</td>
</tr>
</tbody>
</table>
**frame-seconds window**

To configure the window size for the OAM frame-seconds error event, use the `frame-seconds window` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the `no` form of this command.

```
frame-seconds window window
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>window</td>
<td>Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 90000.</td>
</tr>
</tbody>
</table>

**Note**
The only accepted values are multiples of the line-card-specific polling interval, that is, 1000 milliseconds for most line cards.

**Command Default**

The default value is 60000.

**Command Modes**

- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the window size for a frame-seconds error.

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>link-monitor, on page 229</td>
<td>Enters Ethernet OAM link monitor configuration mode.</td>
</tr>
</tbody>
</table>
To configure the thresholds that triggers an Ethernet OAM frame error event, use the `frame threshold` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the `no` form of this command.

```
frame threshold low threshold [high threshold]
```

### Syntax Description

- **Low threshold**, in symbols, that triggers a frame error event. The range is 0 to 12000000.
- **High threshold**, in symbols, that triggers a frame error event. The range is 0 range is 0 to 12000000. The high threshold value can be configured only in conjunction with the low threshold value.
- **In optional, at least one of high and low must be specified** High threshold, in symbols, that causes a frame error event to trigger an action. The range is 1 to 12000000.

### Command Default

The default low threshold is 1.

### Command Modes

- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When the low threshold is passed, a frame error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

### Task ID

- `ethernet-services` read, write

### Examples

The following example shows how to configure the low and high thresholds that trigger a frame error event:

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# frame threshold low 100 high 60000
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td></td>
<td>link-monitor, on page 229</td>
<td>Enters Ethernet OAM link monitor configuration mode.</td>
</tr>
</tbody>
</table>
frame window

To configure the frame window size of an OAM frame error event, use the `frame window` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the `no` form of this command.

```
frame window window
```

**Syntax Description**

`window` Size of the window for a frame error in milliseconds. The range is 1000 to 60000.

**Command Default**

The default value is 1000.

**Command Modes**

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows how to configure the window size for a frame error.

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# frame window 60
```

**Related Commands**

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>link-monitor, on page 229</td>
<td>Enters Ethernet OAM link monitor configuration mode.</td>
</tr>
</tbody>
</table>
```
**link-monitor**

To enter Ethernet OAM link monitor configuration mode, use the `link-monitor` command in Ethernet OAM configuration mode. To enter interface Ethernet OAM link monitor configuration mode, use the `link-monitor` command in interface Ethernet OAM configuration mode.

### Syntax Description

This command has no keywords or arguments.

### Command Default

No default behavior or values

### Command Modes

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enter the Ethernet OAM link monitor configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)#
```

The following example shows how to enter the link monitor configuration mode from interface Ethernet OAM configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# link-monitor
```
log ais

To configure AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received, use the log ais command in CFM domain service configuration mode. To disable AIS logging, use the no form of this command.

**log ais**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Logging is disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>CFM domain service configuration (config-cfm-dmn-svc)</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 3.9.1  This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ais transmission, on page 139</td>
<td>Configures AIS transmission for a CFM domain service.</td>
</tr>
<tr>
<td>ais transmission up, on page 141</td>
<td>Configures AIS transmission on a CFM interface.</td>
</tr>
<tr>
<td>show ethernet cfm interfaces ais, on page 280</td>
<td>Displays the information about interfaces that are currently transmitting AIS.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>
log continuity-check errors

To enable logging of continuity-check errors, use the **log continuity-check errors** command in CFM domain service configuration mode. To disable logging of continuity-check errors, use the no form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Logging is disabled.

**Command Modes**
CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The following types of continuity-check errors are logged:

- Incorrect level (cross-connect)
- Incorrect interval
- Incorrect MA-ID (cross-connect)
- Local MAC address received (loop)
- Local MEP-ID received (mis-config)
- Invalid source MAC received
- RDI received

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable logging of continuity check errors:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log continuity-check errors
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log continuity-check errors
```
**log continuity-check mep changes**

To enable logging of peer maintenance-end-point (MEP) state changes, use the `log continuity-check mep changes` command in CFM domain service configuration mode. To disable logging of peer MEP state changes, use the no form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Logging is disabled

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables logging of state changes that occur in MEPs for a particular service, such as:

- New peer MEP detected.
- Peer MEP time out (loss of continuity) detected.

**Note**

If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable logging of continuity-check mep changes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log continuity-check mep changes
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log continuity-check mep changes
```
log crosscheck errors

To enable logging of crosscheck error events, use the `log crosscheck errors` command in CFM domain service configuration mode. To disable logging of crosscheck error events, use the `no` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Logging is disabled.

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables logging of crosscheck errors, such as:

- MEPs missing
- Additional peer MEPs detected

---

**Note**

Crosscheck errors are only detected and logged when crosscheck is configured using the `mep crosscheck` and `mep-id` commands.

---

**Examples**

The following example shows how to enable logging of crosscheck errors:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log crosscheck errors
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log crosscheck errors
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mep crosscheck</code>, on page 239</td>
<td>Enters CFM MEP crosscheck configuration mode.</td>
</tr>
<tr>
<td><code>mep-id</code>, on page 240</td>
<td>Enables crosscheck on a MEP.</td>
</tr>
</tbody>
</table>
log disable

To turn off syslog messages for Ethernet LMI (E-LMI) errors or events, use the log disable command in interface Ethernet LMI configuration mode. To return to the default, use the no form of the command.

```
log {errors | events} disable
```

**Syntax Description**
- errors: Disables logging of E-LMI protocol and reliability errors.
- events: Disables logging of significant E-LMI protocol events.

**Command Default**
E-LMI syslog messages are enabled for errors and events.

**Command Modes**
Interface Ethernet LMI configuration (config-if-elmi)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To see statistics on E-LMI protocol and reliability errors and protocol events, use the show ethernet lmi interfaces command.

**Task ID**
- ethernet-services: read, write

The following example shows how to disable logging of E-LMI protocol and reliability errors:

```
RP/0/RSP0/CPU0:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)# log errors disable
```

The following example shows how to disable logging of E-LMI events:

```
RP/0/RSP0/CPU0:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)# log events disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (Ethernet), on page 72</td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>ethernet lmi, on page 185</td>
<td>Enables E-LMI operation on an interface and enters interface Ethernet LMI configuration mode.</td>
</tr>
<tr>
<td>show ethernet lmi interfaces, on page 306</td>
<td>Displays E-LMI information for an interface, including protocol status and error and event statistics.</td>
</tr>
</tbody>
</table>
To enable logging of Ethernet Fault Detection (EFD) state changes to an interface (such as when an interface is shut down or brought up via EFD), use the `log efd` command in CFM domain service configuration mode. To disable EFD logging, use the `no log efd` command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
EFD logging is disabled.

**Command Modes**
CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
When EFD logging is enabled, a syslog is generated whenever the EFD state of an interface changes.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable EFD logging:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service S1 down-meps
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# log efd
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>efd, on page 176</td>
<td>Enables EFD on all down MEPs in a down MEPs service.</td>
</tr>
<tr>
<td>show efd interface, on page 275</td>
<td>Displays all interfaces that are shut down because of EFD.</td>
</tr>
</tbody>
</table>
maximum-meps

To configure the maximum number of maintenance end points (MEPs) for a service, use the `maximum-meps` command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

`maximum-meps number`

**Syntax Description**

- **number**: Maximum number of MEPS allowed for this service. The range is 2 to 8190.

**Command Default**

The default is 100.

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command configures the maximum number of peer maintenance end points (MEPs). It does not limit the number of local MEPs. The configured `maximum-meps number` must be at least as great as the number of configured crosscheck MEPs.

The `maximum-meps number` limits the number of peer MEPs, for which local MEPs store continuity-check messages (CCMs). When the limit is reached, CCMs from any new peer MEPs are ignored, but CCMs from existing peer MEPs continue to be processed normally.

The `maximum-meps number` also limits the size of the CCM learning database.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the maximum number of maintenance end points (MEPs) for a service:

```
RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# ethernet cfm
RP/0/RSP0/CP00:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CP00:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CP00:router(config-cfm-dmn-svc)# maximum-meps 4000
```

```
RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# ethernet cfm
RP/0/RSP0/CP00:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CP00:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RSP0/CP00:router(config-cfm-dmn-svc)# maximum-meps 4000
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain, on page 174</td>
<td></td>
</tr>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
<tr>
<td>service, on page 270</td>
<td></td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
</tbody>
</table>
mep crosscheck

To enter CFM MEP crosscheck configuration mode, use the mep crosscheck command in CFM domain service configuration mode.

mep crosscheck

Syntax Description
This command has no keywords or arguments.

Command Default
Not configured, in which case no crosscheck is performed on the MEP.

Command Modes
CFM domain service configuration (config-cfm-dmn-svc)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enter CFM MEP crosscheck configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/RSP0/CPU0:router(config-cfm-xcheck)#
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# mep crosscheck
RP/0/RSP0/CPU0:router(config-cfm-xcheck)#
```
**mep-id**

To enable crosscheck on a maintenance end point (MEP), use the **mep-id** command in CFM MEP crosscheck configuration mode. To disable crosscheck on a MEP, use the **no** form of this command.

```
mep-id  mep-id-number  [mac-address  mac-address]
```

**Syntax Description**
- **mac** (Optional) MAC address of the interface upon which the MEP resides, in standard hexadecimal format, hh:hh:hh:hh:hh:hh.
- **mac-address**

**Command Default**
Not configured, in which case no crosscheck is performed on the MEP.

**Command Modes**
CFM MEP crosscheck configuration (config-cfm-xcheck)

**Command History**
- Release 3.9.0  This command was introduced.

**Usage Guidelines**
This command enables Crosscheck on the maintenance end point (MEP) specified by the MEP ID number (**mep-id-number**). The range for MEP ID numbers is 1 to 8191. Crosscheck is enabled when the first crosscheck MEP is entered.

Repeat this command for every MEP that you want to include in the expected set of MEPs for crosscheck.

Crosscheck detects the following two additional defects for continuity-check messages (CCMs) on peer MEPS:

- **Peer MEP missing**—A crosscheck MEP is configured, but has no corresponding peer MEP from which to receive CCMs.
- **Peer MEP unexpected**—A peer MEP is sending CCMs, but no crosscheck MEP is configured for it.

**Note**
If more than one local MEP is configured for a service, all the local MEPS must be included in the list of configured crosscheck MEPS.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to statically define a maintenance end point (MEP) under a service, so that it can be crosschecked.

```
RP/0/RSP0/CPU0:router#  configure
RP/0/RSP0/CPU0:router(config)#  ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)#  domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)#  service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#  mep crosscheck
```
mep domain

To create a maintenance end point (MEP) on an interface, use the **mep domain** command in interface CFM configuration mode. To remove the MEP from the interface, use the no form of this command.

```
mep domain  domain-name  service  service-name  mep-id  id-number
```

**Syntax Description**

- **domain domain-name**: Domain in which to create the maintenance end point (MEP).
- **service service-name**: Operation service in which to create the maintenance end point (MEP).
- **mep-id id-number**: Maintenance end points (MEP) identifier to assign to this MEP. The range is 1 to 8191.

**Command Default**

No MEPS are configured on the interface.

**Command Modes**

Interface CFM configuration (config-if-cfm)

**Command History**

Release 3.9.1 This command was introduced. This command replaces the **ethernet cfm mep** command.

**Usage Guidelines**

CFM Maintenance end points (MEPs) are supported on all Ethernet interfaces and VLAN subinterfaces. This command creates MEPS in the UP MEP state, unless the specified **service** is configured with MEPs in the DOWN MEP state. See the **service**, on page 270 command.

**Task ID**

**Task ID**

- ethernet-services
  - read,
  - write

**Examples**

The following example shows how to create a MEP using an ID of 1 on the CFM domain named DM1 and service named Sv1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ethernet cfm
RP/0/RSP0/CPU0:router(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
</tbody>
</table>
mib-retrieval

Syntax Description

mib-retrieval [disable]

disable  Disables MIB retrieval on the Ethernet OAM interface.

Command Default

MIB retrieval is disabled by default.

Command Modes

Ethernet OAM configuration (config-eoam)
Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release 3.9.0  This command was introduced.

Usage Guidelines

When MIB retrieval is enabled on an Ethernet OAM interface, the OAM client advertises support for MIB retrieval to the peer.

When MIB retrieval is disabled (the default), only the enable form of the mib-retrieval command is available in interface Ethernet OAM configuration mode. The disable keyword is provided to override the profile when needed.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enable MIB retrieval on a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# mib-retrieval
```
mip auto-create

To enable the automatic creation of Maintenance Intermediate Points (MIPs) in a bridge domain or cross-connect, use the `mip auto-create` command in CFM domain service configuration mode. To disable automatic creation of MIPs, use the `no` form of this command.

```
mip auto-create {all | lower-mep-only} {ccm-learning}
```

**Syntax Description**

- `all` [Optional] Enables automatic creation of MIPs on all interfaces.
- `lower-mep-only` [Optional] Enables automatic creation of MIPs only on interfaces with a MEP at a lower level.
- `ccm-learning` [Optional] Enables CCM learning for MIPs created in this service. This must be used only in services with a relatively long CCM interval of at least 100 ms. CCM learning at MIPs is disabled by default.

**Command Default**

None

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc) mode

**Command History**

- Release 3.9.0   This command was introduced.
- Release 4.3.1   The `ccm-learning` keyword was introduced.

**Usage Guidelines**

The MIP auto-creation feature is configured only for services associated with bridge domains or cross-connects. Unlike MEPs, MIPs are not explicitly configured on each interface. MIPs are created automatically according to the algorithm specified in the CFM 802.1ag standard. For each interface, the algorithm, in brief, operates in this manner:

- The bridge-domain or cross-connect for the interface is found, and all services associated with that bridge-domain or cross-connect are considered for MIP auto-creation.
- The level of the highest-level MEP on the interface is found. From among the services considered above, the service in the domain with the lowest level that is higher than the highest MEP level is selected. If there are no MEPs on the interface, the service in the domain with the lowest level is selected.
- The MIP auto-creation configuration for the selected service is examined to determine whether a MIP should be created.

**Note**

Configuring a MIP auto-creation policy for a service does not guarantee that a MIP will automatically be created for that service. The policy is only considered if that service is first selected by the algorithm.
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enable the automatic creation of MIPs for all interfaces in a bridge domain:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# mip auto-create all
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain, on page 174</td>
<td></td>
</tr>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>service, on page 270</td>
<td></td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
</tbody>
</table>
mode (Ethernet OAM)

To configure the Ethernet OAM mode on an interface, use the `mode` command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the `no` form of the command.

```
mode {active | passive}
```

**Syntax Description**
- `passive` Specifies that the interface operates in passive mode, where it cannot initiate the discovery process, generate a retrieval PDU, or request loopback.
- `active` (Interface Ethernet OAM configuration only) Specifies that the interface operates in active mode to initiate processes and make requests.

**Command Default**
The default is active.

**Command Modes**
- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**
- Release 3.9.0  This command was introduced.

**Usage Guidelines**
If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

**Task ID**
- `ethernet-services` read, write

**Examples**
The following example shows how to enable Ethernet OAM passive mode on a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/RSP0/CPU0:router(config-if-eoam)# mode passive
```

**Related Commands**
- `ethernet oam profile`, on page 189: Creates an EOAM profile and enters EOAM configuration mode.
- `ethernet oam`, on page 186: Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
- `profile (EOAM)`, on page 257: Attaches an Ethernet OAM profile to an interface.
### Ethernet OAM Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
monitoring

To enable Ethernet OAM link monitoring, use the `monitoring` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return link monitoring to its default state of enabled, use the `no` form of this command.

```
monitoring [disable]
```

**Syntax Description**

- **disable** (Optional) Disables Ethernet OAM link monitoring.

  **Note** When configuring on a profile, only the `monitoring disable` form of the command is supported.

**Command Default**

Link monitoring is enabled by default.

**Command Modes**

- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.1.32</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Monitoring is enabled by default. To disable it either on a profile or an interface, use the `monitoring disable` form of the command.

If monitoring is disabled on a profile, but you want to override the configuration and enable it for an interface, use the `monitoring` command in interface Ethernet OAM link monitor configuration mode.

You cannot configure the `monitoring` command without the `disable` keyword on a profile.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to disable link-monitoring on an Ethernet OAM interface:

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# monitoring disable
```
# packet size

To configure the minimum size (in bytes) for outgoing probe packets, including padding when necessary, use the `packet size` command in SLA profile probe configuration mode. To remove this configuration, use the `no form` of this command.

```
packet size bytes [test pattern {hex 0x HHHHHHHHH | pseudo-random}]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bytes</code></td>
<td>(Optional) Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value refers to the total frame size including the Layer 2 or Layer 3 packet header. Optional TLVs, such as the End TLV, are only included when the requested packet size allows.</td>
</tr>
<tr>
<td><code>test pattern</code></td>
<td>(Optional) Specifies a 4-byte string (8 hexadecimal characters) to repeat as many times as required to fill the outgoing probe packet to the specified minimum packet size. The default is all 0s.</td>
</tr>
<tr>
<td><code>hex 0x HHHHHHHHH</code></td>
<td>(Optional) Specifies a pseudo-random bit sequence determined by the protocol to fill the outgoing probe packet to the specified minimum packet size.</td>
</tr>
</tbody>
</table>

## Command Default

The minimum packet size is not configured. When a minimum packet size is configured and padding is required, the default padding is all 0s.

## Command Modes

SLA profile probe configuration (config-sla-prof-pb)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The <code>test pattern hex</code> and <code>pseudo-random</code> keywords were added.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

For supported packet types, this configuration determines the minimum size of all outgoing SLA probe packets, including the size to which they are padded. The amount of padding that is added to a packet depends on the type of frame that is sent and the amount of data in the frame.

When the packet size is not configured, packets are sent at the minimum size required to fit all the required information. Even when the packet size is configured, the packets may be larger than the configured size if the required information exceeds the configured value.

If a probe packet is too large, it may get dropped somewhere in the network.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to configure the minimum size of outgoing probe packets using default padding of all 0s as needed:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# packet size 9000
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# commit
```

The following example shows how to configure a hexadecimal test pattern to pad packets with to reach the minimum packet size:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# packet size 9000 test pattern hex 0xabcdabcd
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# commit
```
ping ethernet cfm

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance end point (MEP) or MAC address destination from the specified source MEP, and display a summary of the responses, use the ping ethernet cfm command in EXEC mode.

```
ping ethernet cfm domain domain-name service service-name {mac-address mac | mep-id id} source [mep-id source-id] interface interface-path-id [cos cos-val] [count n] [frame-size size] [data-pattern hex] [interval seconds] [timeout time]
```

### Syntax Description

- **domain domain-name**
  - String of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
  - **Note**: For more information about the syntax, use the question mark (?) online help function.

- **service service-name**
  - String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.

- **mac-address mac**
  - 6-byte ID number of the MAC address of the destination MEP.

- **mep-id id**
  - Maintenance end point (MEP) ID number of the destination MEP. The range for MEP ID numbers is 1 to 8191.

- **source**
  - Source information.

- **mep-id source-id**
  - (Optional) Maintenance end point (MEP) ID number of the source MEP. The range for MEP ID numbers is 1 to 8191.

- **interface interface-path-id**
  - Physical interface or virtual interface.
  - **Note**: Use the `show interfaces` command to see a list of all interfaces currently configured on the router.
  - For more information about the syntax for the router, use the question mark (?) online help function.

- **cos cos-val**
  - (Optional) Class of Service (CoS) value that identifies the class of traffic of the source MEP. The valid values are from 0 to 7.

- **count n**
  - (Optional) Number of pings as an integer value. The default is 5.

- **frame-size size**
  - (Optional) Size, as an integer, of the ping frames. Frames are padded to read the specified size. The default is 0 (no padding).

- **data-pattern hex**
  - (Optional) Hexadecimal value to be used as the data pattern for padding within a ping frame, when padding is required due to the `frame-size` configuration. The default is 0.

- **interval seconds**
  - (Optional) Specifies, in seconds, the time between pings. The `n` argument is entered in seconds. The default is 1 second.
timeout time  (Optional) Timeout, in seconds, for the ping packet. The default is 2.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can use this command, a local MEP must be configured for the domain and the interface.

The command displays the following information:

- Number of loopback message being sent
- Timeout period
- Domain name
- Domain level
- Service name
- Source MEP ID
- Interface
- Target MAC address
- MEP ID – If no MEP ID is specified, “No MEP ID specified” is displayed.
- Running time for the current ping operation to complete

*Note*  
The remaining information is not displayed until the current ping operation is complete. If the user interrupts the operation during this time (by pressing control-C), the prompt is returned and no further information is displayed. However, all loopback messages continue to be sent.

- Success rate of responses received – displayed as a percentage followed by the actual number of responses
- The round trip time minimum/maximum/average in milliseconds
- Out-of-sequence responses – displayed as a percentage followed by the actual number of out-of-sequence responses when at least one response is received. An out-of-sequence response occurs if the first response does not correspond with the first message sent, or a subsequent response is not the expected next response after a previously received response.
- Bad data responses – displayed as a percentage followed by the actual number of bad data responses when at least one response is received. A bad data response occurs if the padding data in the response does not match the padding data that is in the sent message. This can only happen if the sent message is padded using the `frame-size` option.
- Received packet rate – displayed in packets per second when at least two responses are received. This approximate rate of response is the time between the first response received and the last response received, divided by the total number of responses received.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>
Example

The following example shows how to send an Ethernet CFM loopback message:

```shell
RP/0/RSP0/CPU0:router# ping ethernet cfm domain D1 service S1 mep-id 16 source interface GigabitEthernet 0/0/0/0

Type escape sequence to abort.
Sending 5 CFM Loopbacks, timeout is 2 seconds -
Domain foo (level 2), Service foo
Source: MEP ID 1, interface GigabitEthernet0/0/0/0
Target: 0001.0002.0003 (MEP ID 16):
   Running (5s) ...
Success rate is 60.0 percent (3/5), round-trip min/avg/max = 1251/1349/1402 ms
Out-of-sequence: 0.0 percent (0/3)
Bad data: 0.0 percent (0/3)
Received packet rate: 1.4 pps
```
polling-verification-timer

To set or disable the Metro Ethernet Forum (MEF) T392 Polling Verification Timer (PVT) for Ethernet Local Management Interface (E-LMI) operation, use the **polling-verification-timer** command in interface Ethernet LMI configuration mode. To return to the default, use the **no** form of the command.

```
polling-verification-timer {interval | disable}
```

**Syntax Description**
- **interval**
  - Number of seconds in the range 5 to 30. The default is 15.
- **disable**
  - Turns off the timer.

**Command Default**
The T392 Polling Verification Timer is set to 15 seconds.

**Command Modes**
Interface Ethernet LMI configuration (config-if-elmi)

**Command History**
- **Release 4.1.0**
  - This command was introduced.

**Usage Guidelines**
The PVT specifies the allowable time between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the Customer Edge (CE) device before recording an error. If the PVT expiration time is reached on consecutive packets for the number of times specified by the **status-counter** command without a STATUS ENQUIRY being received, the E-LMI protocol status is changed to Down.

**Task ID**
- **Task ID**
  - ethernet-services
  - Operation
    - read,
    - write

The following example shows how to set the MEF Polling Verification Timer for E-LMI to 30 seconds:

```
RP/0/RSP0/CP0:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CP0:router(config-if))# ethernet lmi
RP/0/RSP0/CP0:router(config-if-elmi)# polling-verification-timer 30
```

**Related Commands**
- **interface (Ethernet), on page 72**
  - Specifies or creates an Ethernet interface and enters interface configuration mode.
- **ethernet lmi, on page 185**
  - Enables E-LMI operation on an interface and enters interface Ethernet LMI configuration mode.
- **show ethernet lmi interfaces, on page 306**
  - Displays E-LMI information for an interface, including protocol status and error and event statistics.
priority (SLA)

To configure the priority of outgoing SLA probe packets, use the **priority** command in SLA profile probe configuration mode. To return the priority to the default value, use the `no` form of this command.

```
priority  priority
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority  priority</td>
<td>Priority level. The range is 0 to 7.</td>
</tr>
</tbody>
</table>

**Command Default**

When the priority is not configured by SLA, the default is the Class of Service (CoS) priority for the egress interface.

**Command Modes**

SLA profile probe configuration (config-sla-prof-pb)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default priority for all CFM operation types is the Class of Service (CoS) priority for the egress interface. SLA operations that are configured on Maintenance End Points (MEPs) do not use the Class of Service (CoS) settings that are configured independently on Maintenance End Points (MEPs). Use this command to change the priority level of SLA probe packets.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the priority of outgoing SLA probe packets.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# priority 7
```
probe

To enter SLA profile probe configuration mode, use the **probe** command in SLA profile configuration mode. To exit to the previous mode, use the no form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

If no items are configured in the probe mode, all items in the probe mode use their default values.

**Command Modes**

SLA profile configuration (config-sla-prof)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Each profile may optionally have 1 probe submode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the SLA profile probe configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)#
```
profile (EOAM)

To attach an Ethernet OAM profile to an interface, use the `profile` command in interface Ethernet OAM configuration mode. To remove the profile from the interface, use the no form of this command.

```
profile name
```

**Syntax Description**

- `name`: Text name of the Ethernet OAM profile to attach to the interface.

**Command Default**

No profile is attached.

**Command Modes**

Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When an Ethernet OAM profile is attached to an interface using this command, all of the parameters configured for the profile are applied to the interface.

Individual parameters that are set by the profile configuration can be overridden by configuring them directly on the interface.

**Examples**

The following example shows how to attach an Ethernet OAM profile to a Gigabit Ethernet interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# profile Profile_1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
profile (SLA)

To create an SLA operation profile and enter the SLA profile configuration mode, use the `profile` command in SLA configuration mode. To remove the profile, use the `no` form of this command.

```
profile profile-name type  {{ cfm-delay-measurement | cfm-delay-measurement-v0 | cfm-loopback | cfm-synthetic-loss-measurement }}
```

**Syntax Description**

- **profile-name**: Profile name, case-sensitive string up to 31 characters in length. The name “all” cannot be used.
- **type**: Specifies the type of packets sent by operations in this profile. Valid types are:
  - `cfm-delay-measurement`: CFM delay measurement packets
  - `cfm-delay-measurement-v0`: CFM delay measurement version 0 packets
  - `cfm-loopback`: CFM loopback packets
  - `cfm-synthetic-loss-measurement`: CFM synthetic loss measurement packets

**Command Default**

No default behavior or values

**Command Modes**

Ethernet SLA configuration (config-sla)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The <code>cfm-delay-measurement-v0</code> and <code>cfm-synthetic-loss-measurement</code> keyword was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note**
  - Each profile is uniquely identified by its name. Changing the packet `type` for the profile removes all stored data from the profile and is equivalent to deleting the profile and creating a new profile.

- **Note**
  - You can configure the Ethernet SLA profile to use Y.1731 DMM frames. The restriction of 150 configured Ethernet SLA operations for each CFM MEP is removed not only for profiles using DMM frames, but also for profiles using the other supported Y.1731 frame types, such as loopback measurement and synthetic loss measurement. For interoperability purposes, it is still possible to configure profiles to use DMM v0 frames. This is done by specifying a type of `cfm-delay-measurement-v0` on the `profile(SLA)` command. The limit of 150 configured operations for each CFM MEP still applies in this case.
### Examples

This example shows how to configure an SLA operation profile and enter the SLA profile configuration mode:

```bash
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)#
```
remote-loopback

To enable a remote loopback on the far end of an Ethernet OAM interface, use the `remote-loopback` command in Ethernet OAM configuration or interface Ethernet OAM configuration mode. To return the interface to the default (disabled), use the `disable` keyword.

```
remote-loopback  [disable]
```

### Syntax Description

- **disable** Disables the remote loopback at the far end of the Ethernet OAM interface.

### Command Default

Remote loopback is disabled by default.

### Command Modes

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

### Command History

- **Release 3.9.0** This command was introduced.
- **Release 6.1.2** Removed restriction disallowing `remote-loopback disable` version of the command in Ethernet OAM configuration mode.

### Usage Guidelines

When remote loopback is enabled on an Ethernet OAM interface, the OAM client advertises support for remote loopback to the peer.

When remote loopback is disabled (the default), only the enable form of the `remote-loopback` command is available in interface Ethernet OAM configuration mode. The `disable` keyword is provided to override the profile when needed.

### Task ID

- **Task ID**
  - ethernet-services  read, write

### Examples

The following example shows how to enable remote loopback on a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/5/6
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/RSP0/CPU0:router(config-if-eoam)# remote-loopback
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
</tbody>
</table>
## Ethernet OAM Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet oam</code>, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td><code>ethernet oam loopback</code>, on page 187</td>
<td>Starts or stops a loopback at the remote end of an Ethernet OAM interface.</td>
</tr>
<tr>
<td><code>profile (EOAM)</code>, on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
<tr>
<td><code>show ethernet oam configuration</code>, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td><code>show ethernet oam interfaces</code>, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
require-remote

To require that certain features are enabled before an OAM session can become active, or to disable a requirement that is part of an active OAM profile, use the `require-remote` command in Ethernet OAM configuration or interface Ethernet OAM configuration mode. To remove the configuration and return to the default, use the `no` form of this command.

```
require-remote {mode {active | passive} | mib-retrieval | remote-loopback | link-monitoring [disabled]}
```

**Syntax Description**

| mode (active | passive) | Requires that active or passive mode is configured on the peer device before the OAM profile can become active. |
| mib-retrieval | Requires that MIB-retrieval is configured on the peer device before the OAM profile can become active. |
| remote-loopback | Requires that remote-loopback is configured on the peer device before the OAM profile can become active. |
| link-monitoring | Requires that link-monitoring feature is configured on the peer device before the OAM profile can become active. |
| disabled (Optional—Interface Ethernet OAM configuration only) Overrides the Ethernet OAM profile configuration for this option and disables the feature at the specified interface. |

**Command Default**

No default behaviour or values

**Command Modes**

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `disabled` keyword is available only when you are configuring Ethernet OAM on an interface, and is used to override the configuration that is part of an active OAM profile.

The `disabled` keyword does not remove the configuration of the command. Use the `no` form of this command to do that.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to require that specific features are enabled before an OAM session can become active
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# require-remote mode active
RP/0/RSP0/CPU0:router(config-eoam)# require-remote mib-retrieval
RP/0/RSP0/CPU0:router(config-eoam)# require-remote link-monitoring

The following example shows how to disable requirements on a particular interface that is part of an active OAM profile:

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/6/5/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# require-remote mode active disabled
RP/0/RSP0/CPU0:router(config-if-eoam)# require-remote mib-retrieval disabled
RP/0/RSP0/CPU0:router(config-if-eoam)# require-remote link-monitoring disabled

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
<tr>
<td>action capabilities-conflict, on page 117</td>
<td>Configures what action is taken on an interface when a capabilities-conflict event occurs.</td>
</tr>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td>show ethernet oam discovery, on page 319</td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
**schedule (SLA)**

To schedule an operation probe in a profile, use the `schedule` command in SLA profile configuration mode. To disable a schedule, use the `no` form of this command.

**Hourly Scheduling**
```
schedule every number {hours | minutes} [first at hh:mm:ss] [for duration {seconds | minutes | hours}]
```

**Daily Scheduling**
```
schedule every day [at hh:mm] [for duration {seconds | minutes | hours | days}]
```

**Weekly Scheduling**
```
schedule every week on day [at hh:mm] [for duration {seconds | minutes | hours | days | week}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>every week on day [at hh:mm][f]</code></td>
<td>Schedules a probe one day per week, on the specified <code>day</code>, at the specified time <code>(hh:mm)</code>, for the specified <code>duration</code>.</td>
</tr>
<tr>
<td>`duration {seconds</td>
<td>minutes</td>
</tr>
<tr>
<td><code>every day [at hh:mm][f]</code></td>
<td>Schedules a probe every day, at the specified time <code>(hh:mm)</code>, for the specified <code>duration</code>.</td>
</tr>
<tr>
<td>`duration {seconds</td>
<td>minutes</td>
</tr>
<tr>
<td>`every number {hours</td>
<td>minutes} first at hh:mm[.ss]`</td>
</tr>
<tr>
<td>`every number {hours</td>
<td>minutes} [f]`</td>
</tr>
<tr>
<td>`duration {seconds</td>
<td>minutes</td>
</tr>
</tbody>
</table>

**Day of the week. Valid values are:**
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
**hh:mm hh:mm[ss]** Time of day in 24 hour time:
- \( hh:mm \) = hour:minutes example: 22:30
- \( hh:mm:ss \) = hour:minutes:seconds example: 12:30:10 (seconds are optional)

**duration** Duration of probe. The ranges are:
- 1 to 3600 seconds
- 1 to 1440 minutes
- 1 to 24 hours
- 1 day
- 1 week

**number** Number of hours or minutes.
- Valid values for hours are the factors of 24: 1, 2, 3, 4, 6, 8, 12
- Valid values for minutes are the factors of 1440 (up to 90): 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 32, 36, 40, 45, 48, 60, 80, 90

---

**Command Default**
The default is every hour. If the **at** keyword is not specified, the start time of each operation is distributed uniformly within the duration of the probe. If the **for** keyword is not specified, only one single burst is sent.

**Command Modes**
SLA profile configuration (config-sla-prof)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Schedules are optional, but a profile may contain only one schedule.

Any change to a schedule causes all stored data for that operation to be deleted.

Changing a schedule is equivalent to deleting an operation and creating a new operation.

The **for duration** option must be specified if (and only if) the probe is configured to send multiple packets (or bursts of packets), using the **send packet every** or **send burst every** configuration of the **send (SLA)** command. If the **send (SLA)** command is not configured for the probe, or if **send burst once** is configured, the **for duration** option must not be used. If it is used in those cases, an error is returned.

The **for duration** option must not exceed the **schedule every {week | day | number}** option.

When the “**first at hh:mm:ss**” option is used, the configured time is used to calculate an offset after midnight when the first probe should be sent each day. The offset is calculated by taking the configured time plus the interval. Thus, probes may be sent before the configured time.
For example, if you configure “schedule every 6 hours first at 11:15,” then the offset after midnight will be 5:15 (11:15 plus 6:00) and probes will be sent each day at 05:15, 11:15, 17:15 and 23:15.

The following examples show how to schedule operation probes in a profile:

**Example 1: Weekly Scheduling on a Specified Day at a Specified Time and Duration**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# schedule every week on Monday at 23:30 for 1 hour
```

**Example 2: Daily Scheduling at a Specified Time and Duration**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# schedule every day at 11:30 for 5 minutes
```

**Example 3: Hourly Scheduling Beginning at a Specified Time**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# schedule every 2 hours first at 13:45:01
```

**Example 4: Hourly Scheduling for a Specified Duration**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# schedule every 6 hours for 2 hours
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send (SLA), on page 267</td>
<td>Configures the number and timing of packets sent by a probe in an operations profile.</td>
</tr>
</tbody>
</table>
send (SLA)

To configure the number and timing of packets sent by a probe in an operations profile, use the send command in SLA profile probe configuration mode. To return to the default, use the no form of the command.

```
send burst {every number {seconds | minutes | hours} | once} packet count packets interval number {seconds | milliseconds}
send packet {every number {milliseconds | seconds | minutes | hours} | once}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>burst every</td>
<td>Sends a burst of packets every specified number of seconds, minutes, or hours, where number is in the following range:</td>
</tr>
<tr>
<td>number {</td>
<td>• 1–3600 seconds</td>
</tr>
<tr>
<td>seconds</td>
<td>• 1–1440 minutes</td>
</tr>
<tr>
<td>minutes</td>
<td>• 1–168 hours</td>
</tr>
<tr>
<td>hours}</td>
<td>burst once</td>
</tr>
<tr>
<td>burst once</td>
<td>Sends a single burst one time.</td>
</tr>
<tr>
<td>packet count</td>
<td>Specifies the number of packets in each burst. The range is 2 to 600.</td>
</tr>
<tr>
<td>packets</td>
<td>interval number {seconds</td>
</tr>
<tr>
<td>packet every</td>
<td>Specifies the time interval (in seconds or milliseconds) between each packet in a burst, where number is in the following range:</td>
</tr>
<tr>
<td>number {</td>
<td>• 1–30 seconds</td>
</tr>
<tr>
<td>milliseconds</td>
<td>• 50–30000 milliseconds</td>
</tr>
<tr>
<td>seconds</td>
<td>packet every number {milliseconds</td>
</tr>
<tr>
<td>packets</td>
<td>Sends one packet every specified number of milliseconds, seconds, minutes, or hours, where number is in the following range:</td>
</tr>
<tr>
<td>interval</td>
<td>• 1–3600 seconds</td>
</tr>
<tr>
<td>number {</td>
<td>• 1–1440 minutes</td>
</tr>
<tr>
<td>seconds</td>
<td>• 1–168 hours</td>
</tr>
<tr>
<td>minutes</td>
<td>• 50–10000 milliseconds</td>
</tr>
<tr>
<td>hours}</td>
<td>packet once</td>
</tr>
<tr>
<td>packet once</td>
<td>Sends a single packet one time.</td>
</tr>
</tbody>
</table>

**Command Default**

If the operation is configured to measure jitter or data packet loss, the default is to send a single burst of 2 packets with a second interval between the packets.

If the operation is configured to measure synthetic packet loss, the default is to send a single burst of 10 packets with a 100 millisecond interval between the packets.

If the operation does not calculate jitter, data, or synthetic packet loss, the default is to send a single packet one time.

**Command Modes**

SLA profile probe configuration (config-sla-prof-pb)
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3.0</td>
<td>The statistics measurement for Y.1731 Synthetic Loss Measurement was included.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The total length of a burst is the packet count multiplied by the interval and must not exceed 1 minute.

The minimum interval supported is platform and packet-type dependent, so certain a configuration may cause an error even if it falls within the specified limits. In the case of Ethernet SLA, the shortest interval for packet types not used for synthetic loss measurement is 100ms.

When burst once is sent, a single burst is sent at the start of the probe. If the schedule defines a duration for the probe, a configuration warning is flagged. The same is true if the default is in effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

These examples show how to configure the types of packets sent by a probe in an operations profile:

**Example 1: Sending a Burst of a Number of Packets With a Specified Interval Every Specified Number of Seconds**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# send burst every 60 seconds packet count 30 interval 1 second
RP/0/RSP0/CPU0:router(config-sla-prof-pb)#
```

**Example 2: Sending a Burst of a Number of Packets With a Specified Interval One Time**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# send burst once packet count 2 interval 1 second
RP/0/RSP0/CPU0:router(config-sla-prof-pb)#
```

**Example 3: Sending a Single Packet Every Specified Number of Seconds**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# probe
```
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# send packet every 1 second
To associate a service with a domain and enter CFM domain service configuration mode, use the `service` command in CFM domain configuration mode. To remove a service from a domain, use the `no` form of this command.

```
service service-name {bridge group bridge-domain-group bridge-domain bridge-domain-name | down-meps | xconnect group xconnect-group-name {p2p xconnect-name | mp2mp xconnect-name ce-id ce-id-value remote-ce-id remote-ce-id-value} | [icc-based icc-string umc-string] | [string text] | [number number] | [vlan-id id-number] | [vpn-id oui-vpnid]}]
```

**Syntax Description**

- **service-name**: Administrative name for the service. Case sensitive ASCII string up to 80 characters.
  
  Used in conjunction with one of the following services:
  
  - **bridge**
  - **down-meps**
  - **xconnect**

- **bridge**: Specifies the use of a bridge domain. Used in conjunction with **group** and **bridge-domain**.
  
  **Note**: When `bridge` is specified, all MEPs are up and MIPs are permitted.

- **group bridge-domain-group**: Specifies the name of the bridge domain group.

- **bridge-domain bridge-domain-name**: Specifies the name of the bridge domain and enters the Ethernet CFM domain service mode.

- **down-meps**: Specifies that all MEPs are down and no MIPs are permitted.

- **xconnect**: Specifies the use of a cross connect. Used in conjunction with **group** and **p2p** or **mp2mp**.
  
  **Note**: When `xconnect` is specified, all MEPs are up and MIPs are permitted.

- **group xconnect-group-name**: Specifies the name of the cross connect group.

- **p2p xconnect-name**: Specifies the name of the point-to-point cross connect and enters the Ethernet CFM domain service mode.

- **mp2mp xconnect-name**: Specifies the name of the multipoint-to-multipoint cross connect and enters the Ethernet CFM domain service mode.

- **ce-id ce-id-value**: Specifies the local Customer Edge (CE) identifier.

- **remote-ce-id remote-ce-id-value**: Specifies the remote Customer Edge (CE) identifier.
id (Optional) Service identifier. Valid service identifiers are:

- **icc-based** *icc-string  unc-string* — ITU-based Carrier Code format, with the total ICC and Unique MEG ID Code (UMC) string length no greater than 13 characters.
- **number** *number* — Number from 0 to 65535.
- **string** *text* — String length no longer than 46 minus MDID length.
- **vlan-id** *id-number* — Number from 1 to 4094.
- **vpn-id** *oui-vpnid* — VPN ID in RFC 2685 format (HHH:HHHH)

**Command Default**

If id is not specified, the service name is used as the Short MA name.

**Command Modes**

CFM domain configuration (config-cfm-dmn)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.1.0</td>
<td>This command was modified. The <strong>icc-based</strong> keyword was added.</td>
</tr>
<tr>
<td>5.3.1</td>
<td>This command was modified to enable CFM on multipoint-to-multipoint cross connects.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Short MA Name is the second part of the Maintenance Association Identifier (MAID) in CFM frames. If the Short MA Name (service id) is not specified, the service administrative name is used by default.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to associate a bridge domain service to a domain and enter CFM domain service configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Bridge_Service bridge group BD1 bridge-domain B1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#
```

The following example shows how to specify that all MEPs are down and no MIPs are permitted, and enter CFM domain service configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Serv_1 down-meps
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#
```
The following example shows how to associate a p2p cross connect service to a domain and enter CFM domain service configuration mode.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
```

The following example shows how to enable CFM on a multipoint-to-multipoint cross connect.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service Cross_Connect_2 xconnect group XG2 mp2mp X2
   ce-id 201 remote-ce-id 202
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge group (VPLS)</td>
<td>bridge group</td>
<td>Creates a bridge group to contain bridge domains.</td>
</tr>
<tr>
<td>bridge-domain (VPLS)</td>
<td>bridge-domain</td>
<td>Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.</td>
</tr>
<tr>
<td>domain, on page 174</td>
<td>domain</td>
<td>Creates and names a container for all domain configurations and enter the CFM domain configuration mode.</td>
</tr>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>ethernet cfm</td>
<td>Enters Ethernet CFM configuration mode.</td>
</tr>
<tr>
<td>p2p</td>
<td>p2p</td>
<td>Enters p2p configuration mode to configure point-to-point cross-connects.</td>
</tr>
<tr>
<td>show ethernet cfm configuration-errors, on page 278</td>
<td>show ethernet cfm configuration</td>
<td>Displays information about errors that are preventing configured cfm operations from becoming active, as well as any warnings that have occurred.</td>
</tr>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>show ethernet cfm local maintenance-points</td>
<td>Displays all the maintenance points that have been created.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>show ethernet cfm local meps</td>
<td>Displays information about local MEPs.</td>
</tr>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>show ethernet cfm peer meps</td>
<td>Displays other MEPs detected by a local MEP.</td>
</tr>
<tr>
<td>xconnect group</td>
<td>xconnect group</td>
<td>Configures a cross-connect group.</td>
</tr>
</tbody>
</table>
show error-disable

To display the error-disabled state of interfaces, use the `show error-disable` command in the EXEC mode.

```
show error-disable [recovery] [interface <interface>]
```

**Syntax Description**
- `recovery`: Enables error disabled recovery on an interface.
- `interface`: Displays error-disable state for a single interface.

**Command Default**
This command includes all the error-disabled interfaces.

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Example**
The following example shows how to display the error disable information.

```
show error-disable
[recovery]
[interface <interface>]
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Error-Disable reason</th>
<th>Retry (s)</th>
<th>Time disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1/0/3</td>
<td>ethernet-oam-link-fault</td>
<td>1020000</td>
<td>17:12:23 04/31</td>
</tr>
<tr>
<td>Gi0/2/0/1</td>
<td>ethernet-oam-critical-event</td>
<td>---</td>
<td>20:04 04/31/06</td>
</tr>
<tr>
<td>Gi10/11/0/12.1234</td>
<td>ethernet-oam-high-threshold</td>
<td>245</td>
<td>20:02:42</td>
</tr>
</tbody>
</table>

show error-disable trace
[essential | non-essential]

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error-disable recovery cause</td>
<td>Enables error disabled recovery on an interface.</td>
</tr>
<tr>
<td>clear error-disable, on page 146</td>
<td>Clears all error disabled conditions on an interface.</td>
</tr>
</tbody>
</table>
show efd database

To display complete information about all interfaces brought down due to EFD, use the show efd database command in EXEC mode.

```
show  efd database  [server | client] [interface ]
```

### Syntax Description

- **client**
  - Displays all interfaces brought down by EFD filtered by a specific client protocol.

- **server**
  - Displays all interfaces brought down by EFD filtered by interface owner.

- **interface**
  - Displays a specific EFD state for the EFD state, if applicable.

### Command Default

This command display all interfaces brought down by EFD.

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

### Example

The following example shows how to display the error disable information.

```
# show efd database
Client CFM
---------
Interface  Since  Success  Mag  Req  Del
-------------------
GigE0/0/0/0.0  07/08/09 14:53  Yes  No  No

Server VLAN MA
--------
Interface  Clients
-----------
GigE0/0/0/0.0  CFM
```
show efd interface

To display all interfaces that are shut down because of Ethernet Fault Detection (EFD), or to display whether a specific interface is shut down because of EFD, use the `show efd interface` command in EXEC mode:

```
show efd interface [type interface-path-id]
```

**Syntax Description**

- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

If no parameters are specified, all interfaces that are shut down because of EFD are displayed.

**Command Modes**

EXEC mode

**Command History**

Release 3.9.1  This command was introduced.

**Usage Guidelines**

If this command is issued when no EFD errors are detected, the system displays the following message:

```
< date time >
No matching interfaces with EFD-shutdown triggered
```

**Task ID**

- `ethernet-services` read, write

**Examples**

The following example shows how to display all interfaces that are shut down because of Ethernet Fault Detection (EFD):

```
RP/0/RSP0/CPU0:router# show efd interfaces

Server VLAN MA
-------------------------
Interface Clients
-------------------------
GigE0/0/0/0.0 CFM
```
show ethernet cfm ccm-learning-database

To display the Continuity Check Message (CCM) learning database, use the `show ethernet cfm ccm-learning-database` command in EXEC mode.

`show ethernet cfm ccm-learning-database [location node-id]`

**Syntax Description**

| Location | node-id | (Optional) Displays the CFM CCM learning database for the designated node. The `node-id` argument is entered in the `rack/slot/module` notation. |

**Command Default**

All CFM ccm-learning-databases on all interfaces are displayed.

**Command Modes**

EXEC mode

**Command History**

Release 3.7.2 This command was introduced.

**Usage Guidelines**

The CCM Learning Database is populated by MEPs and MIPs that have received continuity-check messages (CCMs). The information in the CCM Learning Database is used to reply to traceroutes when no applicable entries are found in the main MAC learning table.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display all the CFM CCM learning databases on all interfaces:

```
RP/0/RSP0/CPU0# show ethernet cfm ccm-learning-database
Location 0/0/CPU0:
Domain/Level Service Source MAC Interface
---------------------- -------------------- -------------- ------------------
foo/2 foo 0001.0203.0401 Gi0/0/0/0
foo/2 foo 0001.0203.0402 PW
```

**Table 10: show ethernet cfm ccm-learning-database Field Descriptions**

<p>| Domain/Level | The domain name and the level of the domain for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain. |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>The name of the service for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source MAC</td>
<td>Source MAC address in the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages targeted at this MAC address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface through which the CCM entered the router. This will be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• An interface or sub-interface name</td>
</tr>
<tr>
<td></td>
<td>• A pseudowire identification (neighbor address and PW ID)</td>
</tr>
<tr>
<td></td>
<td>• PW – Indicates the CCM was received through the PW in a cross-connect</td>
</tr>
<tr>
<td></td>
<td>• XC ID – the internal cross-connect ID value, indicating that the CCM was received through an interface that no longer exists, or is no longer in L2 mode.</td>
</tr>
</tbody>
</table>
show ethernet cfm configuration-errors

To display information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred, use the `show ethernet cfm configuration-errors` command in EXEC mode.

```
show ethernet cfm configuration-errors [domain domain-name] [interface type interface-path-id]
```

**Syntax Description**

- **domain domain-name** (Optional) Displays information about the specified CFM domain name.
- **interface type** (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

All CFM configuration errors on all domains are displayed.

**Command Modes**

EXEC mode

**Command History**

- **Release**
- **Modification**
  - Release 3.7.2 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display all the CFM configuration errors on all domains:

```
RP/0/RSP0/CPU0:router# show ethernet cfm configuration-errors
Domain fig (level 5), Service bay
  * MIP creation configured using bridge-domain blort, but bridge-domain blort does not exist.
  * An Up MEP is configured for this domain on interface GigabitEthernet0/1/2/3.234 and an Up MEP is also configured for domain blort, which is at the same level (5).
  * A MEP is configured on interface GigabitEthernet0/3/2/1.1 for this domain/service, which has CC interval 100ms, but the lowest interval supported on that interface is 1s.
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>ethernet cfm (interface), on page 183</td>
<td>Enters interface CFM configuration mode.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
show ethernet cfm interfaces ais

To display the information about interfaces that are currently transmitting Alarm Indication Signal (AIS), use the `show ethernet cfm interfaces ais` command in EXEC mode.

```
show ethernet cfm interfaces [type interface-path-id] ais [location node-id]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id** (Optional) Displays information about the node location specified as rack / slot / module.

  Location cannot be specified if you configure an interface type.

**Command Default**

If no parameters are specified, information for all AIS interfaces is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `location` keyword cannot be specified if an interface has been specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the information published in the Interface AIS table:

```
RP/0/RSP0/CP00:router# show ethernet cfm interfaces ais

Defects (from at least one peer MEP):
  A - AIS received  I - Wrong interval
  R - Remote Defect received  V - Wrong Level
  L - Loop (our MAC received)  T - Timed out (archived)
  C - Config (our ID received)  M - Missing (cross-check)
  X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
  P - Peer port down  D - Local port down

  Trigger Transmission
  AIS --------- Via ---------------------------
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
### Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ais transmission, on page 139</td>
<td>Configures AIS transmission for a CFM domain service.</td>
</tr>
<tr>
<td>log ais, on page 230</td>
<td>Configures AIS logging for a CFM domain service to indicate when AIS or LCK packets are received.</td>
</tr>
<tr>
<td>ais transmission up, on page 141</td>
<td>Configures AIS transmission on a CFM interface.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
</tbody>
</table>

## show ethernet cfm interfaces ais

### Table 11: show ethernet cfm interfaces ais Field Descriptions

<table>
<thead>
<tr>
<th>Interface (State)</th>
<th>Dir</th>
<th>L Defects</th>
<th>Levels</th>
<th>L Int</th>
<th>Last started</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1/0/0.234 (Up)</td>
<td>Dn</td>
<td>5 RPC</td>
<td>6</td>
<td>7</td>
<td>01:32:56 ago</td>
<td>5576</td>
</tr>
<tr>
<td>Gi0/1/0/0.567 (Up)</td>
<td>Up</td>
<td>0 M</td>
<td>2,3</td>
<td>5</td>
<td>00:16:23 ago</td>
<td>983</td>
</tr>
<tr>
<td>Gi0/1/0/1.1 (Dn)</td>
<td>Up</td>
<td>D</td>
<td></td>
<td></td>
<td>01:02:44 ago</td>
<td>3764</td>
</tr>
<tr>
<td>Gi0/1/0/2 (Up)</td>
<td>Dn</td>
<td>0 RX</td>
<td>1!</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Interface (State)**: The name and state of the interface.
- **AIS dir**: The direction that the AIS packets are transmitted, up or down.
- **Trigger L**: The level of the lowest MEP that is transmitting AIS. The field is blank if there are no down MEPs on the interface, and AIS is being transmitted due to configuration on the interface itself.
- **Trigger Defects**: Defects detected by the lowest MEP transmitting AIS.
- **Via Levels**: The level at which AIS is being transmitted outside of the interface via a MIP. The field is blank if this is not occurring.
- **Transmission L**: The level at which AIS is being transmitted outside of the interface, via a MIP. The field is blank if this is not occurring.
- **Transmission Int**: The interval at which AIS is being transmitted outside of the interface via a MIP. The field is blank if this is not occurring.
- **Transmission last started**: If AIS is being transmitted outside of the interface, the time that the signal started. The field is blank if this is not occurring.
- **Transmission packets**: If AIS is being transmitted outside of the interface, the number of packets sent by the transmitting MEP since it was created or since its counters were last cleared. The field is blank if this is not occurring.
show ethernet cfm interfaces statistics

To display the per-interface counters for Ethernet Connectivity Fault Management (CFM), use the `show ethernet cfm interfaces statistics` command in EXEC mode.

```
show ethernet cfm interfaces [type interface-path-id] statistics [location node-id]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id** (Optional) Displays information about the node location specified as rack / slot / module. Location cannot be specified if you configure an interface type.

**Command Default**

All CFM counters from all interfaces are displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.1</td>
<td>The command is enhanced to retrieve PM statistics from satellite.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The location cannot be specified if a particular interface is specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows all the CFM counters on all interfaces:

```
RP/0/RSP0/CPU0:router# show ethernet cfm interfaces statistics
Location 0/1/CPU0:

Interface Malformed Dropped Last Malformed Reason
----------------- --------- --------- ---------------------
Gi0/1/0/3.185 0 0
Gi0/1/0/7.185 0 0
Gi0/1/0/7.187 0 0
```
RP/0/RSP0/CPU0: router# show ethernet cfm interfaces statistics
Location 0/0/CPU0:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Malformed</th>
<th>Dropped</th>
<th>Last Malformed Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi100/0/0/0</td>
<td>10</td>
<td>2</td>
<td>Packet malformed - SLM is too short or too long</td>
</tr>
<tr>
<td>Gi100/0/0/3</td>
<td>4</td>
<td>1</td>
<td>Host: Packet malformed - invalid source MAC address Satellite: Packet malformed - the format of one or more timestamps is invalid</td>
</tr>
</tbody>
</table>

Table 12: show ethernet cfm statistics Field Descriptions

<table>
<thead>
<tr>
<th>Interface</th>
<th>Name of the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malformed</td>
<td>Number of packets that have been received at this interface that have been found to be non-compliant with the packet formats specified in IEEE 802.1ag and ITU-T Y.1731.</td>
</tr>
<tr>
<td>Dropped</td>
<td>Number of valid (well-formed) packets that have been received at this interface, that have been dropped in software. Packets may be dropped for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• Packet has an unknown operation code, and reached a MEP.</td>
</tr>
<tr>
<td></td>
<td>• Packet dropped at a MEP because it has a lower CFM level than the MEP.</td>
</tr>
<tr>
<td></td>
<td>• Packet could not be forwarded because the interface is STP blocked.</td>
</tr>
<tr>
<td></td>
<td>• Packet could not be forwarded because it is destined for this interface.</td>
</tr>
<tr>
<td>Last Malformed Reason</td>
<td>Operation code for the last malformed packet received, and the reason that it was found to be malformed. If no malformed packets have been received, this field is blank.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet cfm interface statistics, on page 148</td>
<td>Clears the counters for an Ethernet CFM interface.</td>
</tr>
</tbody>
</table>
**show ethernet cfm local maintenance-points**

To display a list of local maintenance points, use the `show ethernet cfm local maintenance-points` command in EXEC mode.

```
show ethernet cfm local maintenance-points [{domain domain-name [service service-name] | interface type interface-path-id}] [{mep | mip}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain domain-name</code></td>
<td>(Optional) Displays information about the specified domain, where <code>domain-name</code> is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.</td>
</tr>
<tr>
<td><code>service service-name</code></td>
<td>(Optional) Displays information about the specified service, where <code>service-name</code> is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.</td>
</tr>
<tr>
<td><code>interface type</code></td>
<td>(Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>mep</code></td>
<td>(Optional) Displays information about maintenance end points (MEPs).</td>
</tr>
<tr>
<td><code>mip</code></td>
<td>(Optional) Displays information about maintenance intermediate points (MIPs).</td>
</tr>
</tbody>
</table>

**Command Default**

All maintenance points from all interfaces are displayed.

**Command Modes**

EXEC mode

**Command History**

Release 3.7.2  This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display maintenance points:

```
RP/0/RSP0/CPU0:router# show ethernet cfm local maintenance-points
```
### Table 13: show ethernet cfm local maintenance-points Field Descriptions

<table>
<thead>
<tr>
<th>Domain/Level</th>
<th>Service</th>
<th>Interface</th>
<th>Type</th>
<th>ID</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>bar/0</td>
<td>bar</td>
<td>Gi0/0/0/0</td>
<td>Dn MEP</td>
<td>1</td>
<td>03:04:00</td>
</tr>
<tr>
<td>baz/4</td>
<td>baz</td>
<td>Gi0/0/0/1.1</td>
<td>MIP</td>
<td>03:04:01</td>
<td></td>
</tr>
<tr>
<td>baz/4</td>
<td>baz</td>
<td>Gi0/0/0/2</td>
<td>MIP</td>
<td>03:04:02</td>
<td></td>
</tr>
<tr>
<td>foo/?</td>
<td>foo</td>
<td>Gi0/0/0/3</td>
<td>MEP</td>
<td>1</td>
<td>03:04:03?</td>
</tr>
<tr>
<td>qux/2</td>
<td>qux</td>
<td>Gi0/0/0/1.1</td>
<td>Up MEP</td>
<td>10</td>
<td>03:04:01</td>
</tr>
<tr>
<td>qux/2</td>
<td>qux</td>
<td>Gi0/0/0/2</td>
<td>Up MEP</td>
<td>11</td>
<td>03:04:02</td>
</tr>
</tbody>
</table>

**Domain/Level**
- The domain name and the level of the domain. If the domain is not configured globally, a question mark (?) is displayed for the Level.

**Service**
- The name of the service.

**Interface**
- The interface containing the maintenance point.

**Type**
- The type of maintenance point:
  - MIP
  - Up MEP
  - Down MEP
  - MEP—If the MEP belongs to a service that is not configured globally, the type cannot be determined and just MEP is displayed.

**ID**
- The configured MEP ID.
- **Note**: Since MIPs do not have an ID, this column is blank for MIPs.

**MAC**
- The last 3 octets of the interface MAC address.
- **Note**: The first three octets are typically the Cisco OUI.

**Note**
- If the MEP has a configuration error, an exclamation point (!) is displayed at the end of the line in the display output.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
<tr>
<td>traceroute cache, on page 355</td>
<td>Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
show ethernet cfm local meps

To display information about local maintenance end points (MEPs), use the `show ethernet cfm local meps` command in EXEC mode.

```
show ethernet cfm local meps [(domain domain-name [service service-name [mep-id id]]) | interface type interface-path-id [domain domain-name]] [(errors [detail | verbose] | detail | verbose]]
```

**Syntax Description**

- `domain domain-name` (Optional) Displays information about the specified CFM domain, where `domain-name` is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.

- `service service-name` (Optional) Displays information about the specified service, where `service-name` is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.

- `interface type` (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.

- `interface-path-id` Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- `mep-id id` (Optional) Displays information about the specified MEP, where `id` is a number of a local maintenance end point (MEP). The range is 1 to 8191.

- `errors` (Optional) Displays information about peer MEPs with errors.

- `detail` (Optional) Displays detailed information.

- `verbose` (Optional) Displays detailed information, plus counters for each type of CFM packet.

**Command Default**

Brief information is displayed for all local MEPs.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.9.1</td>
<td>New output fields were added for AIS.</td>
</tr>
<tr>
<td>4.3.1</td>
<td>The <code>show ethernet cfm local meps detail</code> and <code>show ethernet cfm local meps verbose</code> command outputs were modified to include CCM interval information.</td>
</tr>
<tr>
<td>5.3.1</td>
<td>The <code>show ethernet cfm local meps verbose</code> command output is modified to include counts for more packet types (DMM, DMR, SLM, SLR, LMM, LMR), and exclude rows in which the sent and received packet count is zero.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

All MEPs are displayed in the `show ethernet cfm local meps` command output, unless they have configuration errors.

### Examples

#### Example 1: show ethernet cfm local meps Command

This example shows sample output of the default statistics for local MEPs without any filtering:

```
RP/0/RSP0/CPU0:router# show ethernet cfm local meps
A - AIS received    I - Wrong interval
R - Remote Defect received  V - Wrong Level
L - Loop (our MAC received)  T - Timed out (archived)
C - Config (our ID received)  M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
P - Peer port down

Domain foo (level 6), Service bar
ID Interface (State) Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
100 Gi1/1/0/1.234 (Up) Up 0/0 N A L7

Domain fred (level 5), Service barney
ID Interface (State) Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
2 Gi0/1/0/0.234 (Up) Up 3/2 Y RPC L6

RP/0/0/CPU0:router# show ethernet cfm local meps
A - AIS received    I - Wrong interval
R - Remote Defect received  V - Wrong Level
L - Loop (our MAC received)  T - Timed out (archived)
C - Config (our ID received)  M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
P - Peer port down

Domain foo (level 6), Service bar
ID Interface (State) Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
100 Gi1/1/0/1.234 (Up) Up 0/0 N A

Domain fred (level 5), Service barney
ID Interface (State) Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
2 Gi0/1/0/0.234 (Up) Up 3/2 Y RPC
```

#### Table 14: show ethernet cfm local meps Field Descriptions

<table>
<thead>
<tr>
<th>ID</th>
<th>Configured MEP ID of the MEP.</th>
</tr>
</thead>
</table>
Interface that the MEP is configured under, and the state of the interface. The states are derived from the interface state, the Ethernet Link OAM interworking state, and the Spanning Tree Protocol (STP) state.

The following states are reported:

- **Up** – Interface Up, Ethernet Link OAM Up, STP Up
- **Down** – Interface Down or Admin Down
- **Test** – Interface Up, Ethernet Link OAM loopback mode
- **Blkd** – Interface Up, Ethernet Link OAM Up, STP Blocked
- Otherwise, the interface state.

<table>
<thead>
<tr>
<th>Dir</th>
<th>Direction of the MEP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD</td>
<td>Remote Defect. Y (yes) indicates that a remote defect is detected on at least one peer MEP. In which case, the RDI bit is set in outgoing CCM messages. Otherwise, N (no).</td>
</tr>
<tr>
<td>MEPs</td>
<td>Total number of peer MEPS sending CCMs to the local MEP.</td>
</tr>
<tr>
<td>Err</td>
<td>Number of peer MEPS for which at least one error has been detected.</td>
</tr>
<tr>
<td>Defects</td>
<td>Types of errors detected. Each error is listed as a single character. Multiple errors are listed if they are from the same MEP. Possible errors are listed at the top of the display output of the command.</td>
</tr>
<tr>
<td>AIS</td>
<td>Alarm Indication Signal. If AIS is configured for the service, the configured level is displayed when an alarm is signaled. If AIS is not configured for the service, or if no alarm is currently signaled, this field is blank.</td>
</tr>
</tbody>
</table>

**Example 2: show ethernet cfm local meps Command Filtered by Domain and Service**

```
RP/0/RSP0/CPU0:router# show ethernet cfm local meps domain foo service bar
A - AIS received  I - Wrong interval
R - Remote Defect received  V - Wrong Level
L - Loop (our MAC received)  T - Timed out (archived)
C - Config (our ID received)  M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
P - Peer port down

Domain foo (level 6), Service bar
ID Interface (State) Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
100 Gi1/1/0/1.234 (Up) Up 0/0 N A L7
```

```
RP/0/0/CPU0:router# show ethernet cfm local meps domain foo service bar
A - AIS received  I - Wrong interval
R - Remote Defect received  V - Wrong Level
L - Loop (our MAC received)  T - Timed out (archived)
C - Config (our ID received)  M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
P - Peer port down

Domain foo (level 6), Service bar
```
Example 3: show ethernet cfm local meps detail Command

This example shows sample output of detailed statistics for local MEPs:

<table>
<thead>
<tr>
<th>ID</th>
<th>Interface (State)</th>
<th>Dir MEPs/Err RD Defects</th>
<th>AIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Gi1/1/0/1.234 (Up)</td>
<td>Up</td>
<td>0/0</td>
</tr>
</tbody>
</table>

The Discarded CCMs field is not displayed when the number is zero (0). It is unusual for the count of discarded CCMs to be anything other than zero, since CCMs are only discarded when the limit on the number of peer MEPs is reached. The Peer MEPs field is always displayed, but the counts are always zero when continuity check is not enabled.

Note

RP/0/RSP0/CPU0:router# show ethernet cfm local meps detail

Domain foo (level 6), Service bar
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 100

Interface state: Up MAC address: 1122.3344.5566
Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

CCM generation enabled: No
AIS generation enabled: Yes (level: 7, interval: 1s)
Sending AIS: Yes (started 01:32:56 ago)
Receiving AIS: Yes (from lower MEP, started 01:32:56 ago)

Domain fred (level 5), Service barney
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 2

Interface state: Up MAC address: 1122.3344.5566
Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
Cross-check defects: 0 missing, 0 unexpected

CCM generation enabled: Yes (Remote Defect detected: Yes)
CCM defects detected: R - Remote Defect received
P - Peer port down
C - Config (our ID received)
AIS generation enabled: Yes (level: 6, interval: 1s)
Sending AIS: Yes (to higher MEP, started 01:32:56 ago)
Receiving AIS: No

Example 4: show ethernet cfm local meps verbose Command

RP/0/0/CPU0:router# show ethernet cfm local meps detail

Domain foo (level 5), Service bar
Down MEP on GigabitEthernet0/1/0/0.123, MEP-ID 20

Interface state: Up MAC address: 1122.3344.5566
Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)
Cross-check errors: 0 missing, 0 unexpected

CCM generation enabled: Yes, 10ms
CCM processing offloaded to high-priority software
AIS generation enabled: No
Sending AIS: No
Receiving AIS: No
This example shows sample output of detailed statistics for local MEPs:

```
RP/0/RSP0/CPU0:router# show ethernet cfm local meps verbose
```

Domain foo (level 6), Service bar
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 100

```
Interface state: Up          MAC address: 1122.3344.5566
Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)
CCM generation enabled: No  AIS generation enabled: Yes (level: 7, interval: 1s)
Sending AIS: Yes (started 01:32:56 ago)  Receiving AIS: Yes (from lower MEP, started 01:32:56 ago)
EFD triggered: No
```

<table>
<thead>
<tr>
<th>Packet</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>5576</td>
<td>0</td>
</tr>
<tr>
<td>SLM</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>SLR</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>DMM</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>DMR</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Domain fred (level 5), Service barney
Up MEP on GigabitEthernet0/1/0/0.234, MEP-ID 2

```
Interface state: Up          MAC address: 1122.3344.5566
Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
Cross-check errors: 0 missing (0 auto), 0 unexpected
CCM generation enabled: Yes, 1s (Remote Defect detected: Yes)
CCM processing offloaded to software
CCM defects detected: R - Remote Defect received
                      P - Peer port down
                      C - Config (our ID received)
AIS generation enabled: Yes (level: 6, interval: 1s)
Sending AIS: Yes (to higher MEP, started 01:32:56 ago)
Receiving AIS: No
```

<table>
<thead>
<tr>
<th>Packet</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCM</td>
<td>12345</td>
<td>67890 (out of seq: 6, discarded: 10)</td>
</tr>
<tr>
<td>LBM</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>LBR</td>
<td>0</td>
<td>5 (out of seq: 0, with bad data: 0)</td>
</tr>
<tr>
<td>AIS</td>
<td>0</td>
<td>46910</td>
</tr>
<tr>
<td>LMM</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>LMR</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

Domain gaz (level 4), Service baz
Up MEP on Standby Bundle-Ether 1, MEP-ID 3

```
Interface state: Up          MAC address: 6655.4433.2211
Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)
CCM generation enabled: Yes, 1s (Remote Defect detected: No)
CCM processing offloaded to software
Sending disabled on local standby MEP
CCM defects detected: Defects below ignored on local standby MEP
                      I - Wrong interval
                      V - Wrong level
```
AIS generation enabled: No
Sending AIS: No
Receiving AIS: No

<table>
<thead>
<tr>
<th>Packet</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCM</td>
<td>0</td>
<td>67890</td>
</tr>
<tr>
<td>LBM</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>LBR</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>AIS</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>LCK</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

Domain bar (level 3), Service boz
Down MEP on GigabitEthernet102/1/0/0.345, MEP-ID 200

---

Interface state: Up
MAC address: 1122.3344.5566
Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

AIS generation enabled: No
Sending AIS: No
Receiving AIS: No

No packets sent/received

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
### show ethernet cfm peer meps

To display information about maintenance end points (MEPs) for peer MEPs, use the `show ethernet cfm peer meps` command in EXEC mode.

```
show ethernet cfm peer meps
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain domain-name</code></td>
<td>(Optional) Displays information about a CFM domain, where <code>domain-name</code> is a</td>
</tr>
<tr>
<td></td>
<td>string of a maximum of 80 characters that identifies the domain in which</td>
</tr>
<tr>
<td></td>
<td>the maintenance points reside.</td>
</tr>
<tr>
<td><code>interface type</code></td>
<td>(Optional) Displays information about the specified interface type. For</td>
</tr>
<tr>
<td></td>
<td>more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>local mep-id id</code></td>
<td>(Optional) Displays information about a local MEP, where <code>id</code> is the number</td>
</tr>
<tr>
<td></td>
<td>of the MEP.</td>
</tr>
<tr>
<td><code>missing</code></td>
<td>(Optional) Displays information about peer MEPs that are missing.</td>
</tr>
<tr>
<td><code>peer mep-id id</code></td>
<td>(Optional) Displays information about a peer MEP, where <code>id</code> is the number</td>
</tr>
<tr>
<td></td>
<td>of the MEP.</td>
</tr>
<tr>
<td><code>peer mac-address H.H.H</code></td>
<td>(Optional) Displays information about a peer MEP, where <code>H.H.H</code> is the</td>
</tr>
<tr>
<td></td>
<td>hexadecimal address of the MEP.</td>
</tr>
<tr>
<td><code>service service-name</code></td>
<td>(Optional) Displays information about a CFM service, where <code>service-name</code></td>
</tr>
<tr>
<td></td>
<td>is a string of a maximum of 154 characters that identifies the maintenance</td>
</tr>
<tr>
<td></td>
<td>association to which the maintenance points belong.</td>
</tr>
<tr>
<td><code>unexpected</code></td>
<td>(Optional) Displays information about unexpected peer MEPs.</td>
</tr>
<tr>
<td><code>cross-check</code></td>
<td>(Optional) Displays information about peer MEPs with cross-check errors.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed information.</td>
</tr>
</tbody>
</table>

#### Command Default

Peer MEPs for all domains are displayed.

#### Command Modes

EXEC mode
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If a Local MEP is receiving Wrong Level CCMs, and if the Remote MEP has its CCM processing offloaded, then the last CCM cannot be displayed.

Task ID

<table>
<thead>
<tr>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
</tr>
</tbody>
</table>

Examples

The following example shows sample output of MEPs detected by a local MEP:

```
RP/0/RSP0/CPU0:router# show ethernet cfm peer meps

Flags:
> - Ok   I - Wrong interval
R - Remote Defect received  V - Wrong level
L - Loop (our MAC received)  T - Timed out
C - Config (our ID received)  M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
* - Multiple errors received

Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St ID MAC Address Port Up/Downtime CcmRcvd SeqErr RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- ----- 
V 10 0001.0203.0403 Up 00:01:35 2 0 0 2
================================================================================
Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
================================================================================
St ID MAC Address Port Up/Downtime CcmRcvd SeqErr RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- ----- 
> 20 0001.0203.0402 Up 00:00:03 4 1 0 0
> 21 0001.0203.0403 Up 00:00:04 3 0 0 0
Domain dom5 (level 2), Service dom5

Table 15: show ethernet cfm peer meps Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>St</td>
<td>Status: one or two characters, representing the states listed at the top of the output.</td>
</tr>
<tr>
<td>ID</td>
<td>Peer MEP ID</td>
</tr>
<tr>
<td>MAC address</td>
<td>Peer MAC Address. If this entry is a configured cross-check MEP, with no MAC address specified, and no CCMs are currently being received from a peer MEP with a matching MEP ID, then this field is blank.</td>
</tr>
<tr>
<td>Port</td>
<td>Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.</td>
</tr>
</tbody>
</table>
If CCMs are currently being received, it is the time since the peer MEP last came up, which is the time since the first CCM was received.

If CCMs are not currently being received, it is the time since the peer MEP last went down, which is the time since the loss threshold was exceeded and a loss of continuity was detected.

<table>
<thead>
<tr>
<th>Time since the peer MEP last came up or went down.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If CCMs are currently being received, it is the time since the peer MEP last came up, which is the time since the first CCM was received.</td>
</tr>
<tr>
<td>If CCMs are not currently being received, it is the time since the peer MEP last went down, which is the time since the loss threshold was exceeded and a loss of continuity was detected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total number of CCMs received from this peer MEP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CmRcvd</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of CCMs received out-of-sequence.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeqErr</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of CCMs received with the RDI bit set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of CCMs received with CCM defects, such as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
</tr>
</tbody>
</table>

- Invalid level error
- Maintenance Association Identifier (MAID) error
- Interval error
- Received with out MEP ID error
- Invalid source MAC error

This example shows sample detailed output of MEPs detected by a local MEP:

RP/0/RSP0/CPU0:router# show ethernet cfm peer meps detail
Domain dom3 (level 5), Service ser3
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
----------------------------------------------------------------------------------------------------------------------------------
Peer MEP-ID 10, MAC 0001.0203.0403
  CFM state: Wrong level, for 00:01:34
  Port state: Up
  CCM defects detected: V - Wrong Level
  CCMs received: 5
    Out-of-sequence: 0
    Remote Defect received: 5
    Wrong Level: 0
    Cross-connect (wrong MAID): 0
    Wrong Interval: 5
    Loop (our MAC received): 0
    Config (our ID received): 0
  Last CCM received
    Level: 4, Version: 0, Interval: 1min
    Sequence number: 5, MEP-ID: 10
    MAID: String: dom3, String: ser3
    Port status: Up, Interface status: Up

Domain dom4 (level 2), Service ser4
Down MEP on GigabitEthernet0/0/0/0 MEP-ID 1
----------------------------------------------------------------------------------------------------------------------------------
Peer MEP-ID 20, MAC 0001.0203.0402
  CFM state: Ok, for 00:00:04
  Received CCM handling offloaded to software
  Port state: Up
  CCMs received: 7
    Out-of-sequence: 1

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
Remote Defect received: 0
Wrong Level: 0
Cross-connect (wrong MAID): 0
Wrong Interval: 0
Loop (our MAC received): 0
Config (our ID received): 0

Last CCM received
Level: 2, Version: 0, Interval: 10s
Sequence number: 1, MEP-ID: 20
MAID: String: dom4, String: ser4
Chassis ID: Local: ios; Management address: 'Not specified'
Port status: Up, Interface status: Up

Peer MEP-ID 21, MAC 0001.0203.0403
CFM state: Ok, for 00:00:05
Port state: Up
CCMs received: 6
Out-of-sequence: 0
Remote Defect received: 0
Wrong Level: 0
Cross-connect (wrong MAID): 0
Wrong Interval: 0
Loop (our MAC received): 0
Config (our ID received): 0

Last CCM received 00:00:05 ago:
Level: 2, Version: 0, Interval: 10s
Sequence number: 1, MEP-ID: 21
MAID: String: dom4, String: ser4
Port status: Up, Interface status: Up

Domain dom5 (level 2), Service ser5
Up MEP on Standby Bundle-Ether 1 MEP-ID 1

Peer MEP-ID 600, MAC 0001.0203.0401
CFM state: Ok (Standby), for 00:00:08, RDI received
Port state: Down
CCM defects detected: Defects below ignored on local standby MEP
I - Wrong Interval
R - Remote Defect received

CCMs received: 5
Out-of-sequence: 0
Remote Defect received: 5
Wrong Level: 0
Cross-connect W(wrong MAID): 0
Wrong Interval: 5
Loop (our MAC received): 0
Config (our ID received): 0

Last CCM received 00:00:08 ago:
Level: 2, Version: 0, Interval: 10s
Sequence number: 1, MEP-ID: 600
MAID: DNS-like: dom5, String: ser5
Chassis ID: Local: ios; Management address: 'Not specified'
Port status: Up, Interface status: Down

Peer MEP-ID 601, MAC 0001.0203.0402
CFM state: Timed Out (Standby), for 00:15:14, RDI received
Port state: Down
CCM defects detected: Defects below ignored on local standby MEP
I - Wrong Interval
R - Remote Defect received
T - Timed Out
P - Peer port down

CCMs received: 2
Out-of-sequence: 0
Remote Defect received: 2
Wrong Level: 0
Cross-connect (wrong MAID): 0
Wrong Interval: 2
Loop (our MAC received): 0
Config (our ID received): 0

Last CCM received 00:15:49 ago:
Level: 2, Version: 0, Interval: 10s
Sequence number: 1, MEP-ID: 600
MAID: DNS-like: dom5, String: ser5
Chassis ID: Local: ios; Management address: 'Not specified'
Port status: Up, Interface status: Down

Table 16: show ethernet cfm peer meps detail Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFM state</td>
<td>State of the peer MEP, how long it has been up or down, and whether the RDI bit was set in the last received CCM. The following possible states are shown if CCMs are currently being received:</td>
</tr>
<tr>
<td></td>
<td>• Missing</td>
</tr>
<tr>
<td></td>
<td>• Timed out—No CCMs have been received for the loss time</td>
</tr>
<tr>
<td></td>
<td>• Ok</td>
</tr>
<tr>
<td></td>
<td>• Indication of a defect</td>
</tr>
<tr>
<td>Port state</td>
<td>Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.</td>
</tr>
</tbody>
</table>
Types of CCM defects that have been detected.

The possible defects are:

- Remote Defect received—The last CCM received from the peer had the RDI bit set.
- Loop (our MAC received)—CCMs were received from a peer with the same MAC address as the local MEP.
- Config (our ID received)—CCMs were received from a peer with the same MEP ID as the local MEP.
- Cross-connect (wrong MAID)—The last CCM received from the peer contained a domain/service identifier that did not match the locally configured domain/service identifier.
- Peer port down—The last CCM received from the peer contained an Interface Status indicating that the interface on the peer was not up.
- Wrong interval—The last CCM received contained a CCM interval that did not match the locally configured CCM interval.
- Wrong level—The last CCM received was for a lower level than the level of the local MEP.
- Timed out—No CCMs have been received within the loss time.
- Missing (cross-check)—Cross-check is configured and lists this peer MEP, but no CCMs have been received within the loss time.
- Unexpected (cross-check)—Cross check is configured for this service and does not list this peer MEP, but CCMs have been received from it within the loss time.

<table>
<thead>
<tr>
<th>CCM defects detected</th>
<th>Types of CCM defects that have been detected.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The possible defects are:</td>
</tr>
<tr>
<td></td>
<td>• Remote Defect received—The last CCM received from the peer had the RDI bit set.</td>
</tr>
<tr>
<td></td>
<td>• Loop (our MAC received)—CCMs were received from a peer with the same MAC address as the local MEP.</td>
</tr>
<tr>
<td></td>
<td>• Config (our ID received)—CCMs were received from a peer with the same MEP ID as the local MEP.</td>
</tr>
<tr>
<td></td>
<td>• Cross-connect (wrong MAID)—The last CCM received from the peer contained a domain/service identified that did not match the locally configured domain/service identifier.</td>
</tr>
<tr>
<td></td>
<td>• Peer port down—The last CCM received from the peer contained an Interface Status indicating that the interface on the peer was not up.</td>
</tr>
<tr>
<td></td>
<td>• Wrong interval—The last CCM received contained a CCM interval that did not match the locally configured CCM interval.</td>
</tr>
<tr>
<td></td>
<td>• Wrong level—The last CCM received was for a lower level than the level of the local MEP.</td>
</tr>
<tr>
<td></td>
<td>• Timed out—No CCMs have been received within the loss time.</td>
</tr>
<tr>
<td></td>
<td>• Missing (cross-check)—Cross-check is configured and lists this peer MEP, but no CCMs have been received within the loss time.</td>
</tr>
<tr>
<td></td>
<td>• Unexpected (cross-check)—Cross check is configured for this service and does not list this peer MEP, but CCMs have been received from it within the loss time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CCMs received</th>
<th>Number of CCMs received in total, by defect type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last CCM received</td>
<td>How long ago the last CCM was received, and a full decode of its contents. Any unknown TLVs are displayed in hexadecimal.</td>
</tr>
<tr>
<td>Offload status</td>
<td>Offload status of received CCM handling.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm local maintenance-points, on page 284</td>
<td>Displays a list of local maintenance points.</td>
</tr>
<tr>
<td>show ethernet cfm local meps, on page 286</td>
<td>Displays information about local MEPs.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
show ethernet cfm summary

To display summary information about CFM, use the `show ethernet cfm summary` command in the EXEC mode.

```
show ethernet cfm summary  location node-id
```

**Syntax Description**

- `location node-id`  (Optional) Specifies the location for which CFM summary is required. If the location is not specified, an overall summary for all nodes is displayed, followed by information for each node. If the location is specified, only information from that node is displayed.

**Command Default**

An overall summary for all nodes is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to display ethernet CFM summary:

```
RP/0/RSP0/CPU0:router# show ethernet cfm summary

CFM System Summary
-------------------
Domains 4
Services 10000
Local MEPS 10000
Operational 9997
  Down MEPS 9997
  Up MEPS 0
  Offloaded 200
  3.3ms 100
  10ms 100
  Disabled (misconfiguration) 2
  Disabled (resource limit) 1
  Disabled (operational error) 0
Peer MEPS 9997
Operational 9990
  Defect detected 5
  No defect detected 9985
Timed out 7
MIPs 0
```
## Ethernet OAM Commands

**show ethernet cfm summary**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>10000</td>
</tr>
<tr>
<td>Bridge domains/Xconnects</td>
<td>10000</td>
</tr>
<tr>
<td>Traceroute Cache entries</td>
<td>3</td>
</tr>
<tr>
<td>Traceroute Cache replies</td>
<td>11</td>
</tr>
<tr>
<td>CCM Learning Database entries</td>
<td>10000</td>
</tr>
</tbody>
</table>

**CFM Summary for 0/0/CPU0**

------------------------

Initial resynchronization: complete

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>4</td>
</tr>
<tr>
<td>Services</td>
<td>10000</td>
</tr>
<tr>
<td>Local MEPs</td>
<td>1000</td>
</tr>
<tr>
<td>Operational</td>
<td>999</td>
</tr>
<tr>
<td>Down MEPs</td>
<td>999</td>
</tr>
<tr>
<td>Up MEPs</td>
<td>0</td>
</tr>
<tr>
<td>Offloaded</td>
<td>100</td>
</tr>
<tr>
<td>3.3ms</td>
<td>100</td>
</tr>
<tr>
<td>10ms</td>
<td>0</td>
</tr>
<tr>
<td>Disabled (misconfiguration)</td>
<td>1</td>
</tr>
<tr>
<td>Disabled (offload resource limit)</td>
<td>0</td>
</tr>
<tr>
<td>Disabled (operational error)</td>
<td>0</td>
</tr>
<tr>
<td>Peer MEPs</td>
<td>999</td>
</tr>
<tr>
<td>Operational</td>
<td>998</td>
</tr>
<tr>
<td>Defect detected</td>
<td>2</td>
</tr>
<tr>
<td>No defect detected</td>
<td>996</td>
</tr>
<tr>
<td>Timed out</td>
<td>1</td>
</tr>
<tr>
<td>MIPs</td>
<td>0</td>
</tr>
<tr>
<td>Interfaces</td>
<td>1000</td>
</tr>
<tr>
<td>Bridge domains/Xconnects</td>
<td>10000</td>
</tr>
<tr>
<td>Traceroute Cache entries</td>
<td>1</td>
</tr>
<tr>
<td>Traceroute Cache replies</td>
<td>3</td>
</tr>
<tr>
<td>CCM Learning Database entries</td>
<td>1000</td>
</tr>
</tbody>
</table>
show ethernet cfm traceroute-cache

To display the contents of the traceroute cache, use the `show ethernet cfm traceroute-cache` command in EXEC mode.

```
show ethernet cfm traceroute-cache [[domain domain-name] [service service-name] [local mep-id id] [transaction-id id]] [interface type interface-path-id] [domain domain-name] [transaction-id id]] [exploratory | targeted] [status {complete | incomplete}] [detail]
```

**Syntax Description**

- **domain domain-name** (Optional) Displays information about a CFM domain, where `domain-name` is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.

- **service service-name** (Optional) Displays information about a CFM service, where `service-name` is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.

- **local mep-id id** (Optional) Displays information for the specified local maintenance endpoint (MEP). The range for MEP ID numbers is 1 to 8191.

- **transaction-id id** (Optional) Displays information for the specified transaction.

- **interface type** (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** (Optional) Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **exploratory** (Optional) Displays information for exploratory traceroutes.

- **targeted** (Optional) Displays information for traceroutes that are not exploratory, but explicitly mapped.

- **status** (Optional) Displays status information.

- **complete** (Optional) Displays status information for traceroutes that have received all replies.

- **incomplete** (Optional) Displays status information for traceroutes that are still receiving replies.

- **detail** (Optional) Displays detailed information.

**Command Default**

Shows output for the default traceroute.

**Command Modes**

EXEC mode
**Usage Guidelines**

Use the `show ethernet cfm traceroute-cache` command to display the contents of the traceroute cache; for example, to see the maintenance intermediate points (MIPs) and maintenance end points (MEPs) of a domain as they were discovered. The data is historic. The traceroute cache stores entries from previous traceroute operations.

In the output, the traceroutes sourced from each local MEP are listed. The heading for the local MEP contains the domain name and level, service name, MEP ID and interface name.

**Examples**

The following example shows sample output for the `show ethernet cfm traceroute-cache` command:

```
RP/0/RSP0/CPU0:router# show ethernet cfm traceroute-cache
Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
---------------------------------------------------------------
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402, TTL 64, Trans ID 2:
Hop Hostname/Last Ingress MAC/name Egress MAC/Name Relay
--- ------------------------ ---------------------- ---------------
 1 ios 0000-0001.0203.0400 0001.0203.0400 [Down] FDB
 2 abc ios 0001.0203.0401 [Ok] FDB
 3 bcd 0001.0203.0402 [Ok] GigE0/0 Hit
Replies dropped: 0
```

```
Traceroutes in domain foo (level 2), service foo
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0
---------------------------------------------------------------
Traceroute at 2009-05-18 12:03:31 to 0001.0203.0403, TTL 64, Trans ID 1:
Hop Hostname/Last Ingress MAC/name Egress MAC/Name Relay
--- ------------------------ ---------------------- ---------------
 1 abc 0000-0001.0203.0400 0001.0203.0401 [Ok] FDB
 2 bob abc 0001.0203.0402 [Ok] MPDB
 3 cba bob 0001.0203.0403 [Ok] G10/2/0/3.45 Hit
Replies dropped: 0
```

```
Traceroute at 2009-05-18 12:15:47 to 0001.0203.0409, TTL 64, Trans ID 3, automatic:
00:00:05 remaining
```
Traceroute at 2009-05-18 12:20:10 explore to ffff.ffff.ffff, TTL 64, Trans ID 4, Timeout auto, Reply Filter Default:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Hostname/Last Ingr/Egr MAC/name</th>
<th>Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>abc Ingress 0015.0000.323f [Ok] FDB</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>abc Egress 0015.0000.323e [Ok] FDB</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0002-0016.eeee.1234 abc Ingress 0016.eeee.1234 [Ok] FDB</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0000-0016.eeee.4321 Egress 0016.eeee.4321 [Ok] FDB</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>rtr Ingress 0015.0000.f123 [Ok] FDB</td>
<td></td>
</tr>
</tbody>
</table>

Replies dropped: 0

Table 17: show ethernet cfm traceroute-cache Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceroute at</td>
<td>Date and time the traceroute was started.</td>
</tr>
<tr>
<td>to</td>
<td>Destination MAC address.</td>
</tr>
<tr>
<td>explore to</td>
<td>(Exploratory traceroutes) MAC address of the target for the exploratory traceroute.</td>
</tr>
<tr>
<td>TTL</td>
<td>Initial Time To Live used for the traceroute operation.</td>
</tr>
<tr>
<td>Trans ID</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>Timeout</td>
<td>(Exploratory traceroutes) If no timeout was configured, “Timeout auto” is shown.</td>
</tr>
<tr>
<td>Reply Filter</td>
<td>(Exploratory traceroutes) Type of filter.</td>
</tr>
<tr>
<td>automatic</td>
<td>Indicates that the traceroute was triggered automatically (for example, as a result of a peer MEP exceeding the loss threshold, or if Continuity-Check Auto-traceroute is configured).</td>
</tr>
<tr>
<td>00:00:00 remaining</td>
<td>If the traceroute is in progress, the time remaining until it completes.</td>
</tr>
<tr>
<td>No replies received</td>
<td>Traceroute has completed but no replies were received.</td>
</tr>
<tr>
<td>Replies dropped</td>
<td>Number of replies dropped.</td>
</tr>
<tr>
<td>FDB only</td>
<td>Indicates FDB-only was configured for a standard traceroute.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hop</td>
<td>Number of hops between the source MEP and the Maintenance Point that sent the reply. (Exploratory traceroutes) The display is indented by an extra character as the hop increases, so that the tree of responses can be seen.</td>
</tr>
<tr>
<td>Hostname/Last</td>
<td>On the first line, the hostname of the Maintenance Point that sent the reply. On the second line, the hostname of the previous Maintenance Point in the path. If either of the hostnames is unknown, the corresponding Egress ID is displayed instead.</td>
</tr>
<tr>
<td>Ingr/Egr</td>
<td>(Exploratory traceroutes) Indicates whether the reply is for an ingress or egress interface, but never both.</td>
</tr>
<tr>
<td>Ingress MAC/Name</td>
<td>If the reply includes information about the ingress interface, then the first line displays the ingress interface MAC address and the ingress action. The ingress interface name, if known, is displayed on the second line.</td>
</tr>
<tr>
<td>Egress MAC/Name</td>
<td>If the reply includes information about the egress interface, then the first line displays the egress interface MAC address and the egress action. The egress interface name, if known, is displayed on the second line.</td>
</tr>
<tr>
<td>MAC/Name</td>
<td>(Exploratory traceroutes) The MAC address of the interface from which the reply was sent, and the ingress/egress action, are displayed on the first line. If the interface name was present in the reply, it is displayed on the second line.</td>
</tr>
<tr>
<td>Relay</td>
<td>Type of relay action performed.</td>
</tr>
<tr>
<td></td>
<td>For standard traceroutes, the possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Hit—The target MAC address was reached.</td>
</tr>
<tr>
<td></td>
<td>• FDB—The target MAC address was found in the Filtering Database (the MAC learning table on the switch) and will be forwarded by the interface.</td>
</tr>
<tr>
<td></td>
<td>• MPDB—The target MAC address was found in the MP Database (the CCM Learning database on the switch).</td>
</tr>
<tr>
<td></td>
<td>In addition, “MEP” is displayed on the second line if a terminal MEP was reached.</td>
</tr>
<tr>
<td></td>
<td>For exploratory traceroutes, the possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Hit—The target MAC address was reached.</td>
</tr>
<tr>
<td></td>
<td>• FDB—The target MAC address was found in the Filtering Database and will be forwarded at this interface.</td>
</tr>
<tr>
<td></td>
<td>• Flood—The target MAC address was not found in the Filtering database, and will be flooded at this interface.</td>
</tr>
<tr>
<td></td>
<td>• Drop—The target MAC address will not be forwarded at this interface.</td>
</tr>
</tbody>
</table>

The following example shows sample output for the `show ethernet cfm traceroute-cache detail` command:
show ethernet cfm traceroute-cache

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface GigabitEthernet0/0/0/0

Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Hostname</th>
<th>Ingress MAC</th>
<th>Egress MAC</th>
<th>Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ios</td>
<td>0001.0203.0400 [Down]</td>
<td></td>
<td>FDB</td>
</tr>
</tbody>
</table>
  
  Level: 4, version: 0, Transaction ID: 2
  TTL: 63, Relay Action: RlyFDB
  Forwarded, Terminal MEP not reached
  Last egress ID: 0000-0001.0203.0400
  Next egress ID: 0000-0001.0203.0400
  Ingress interface:
  Action: IngDown, MAC: 0001.0203.0400
  ID: Local: Gi0/0/0/0
  Hostname: Local: ios, address Not specified

| 2   | abc      | 0001.0203.0401 [Ok] |            | FDB   |
  
  Level: 4, version: 0, Transaction ID: 2
  TTL: 62, Relay Action: RlyFDB
  Forwarded, Terminal MEP not reached
  Last egress ID: 0000-0001.0203.0400
  Next egress ID: 0000-0001.0203.0401
  Egress interface:
  Action: EgOk, MAC: 0001.0203.0401
  ID: Not present
  Hostname: Local: abc, address Not specified

| 3   | bcd      | 0001.0203.0402 [Ok] |            | Hit   |
  
  Level: 4, version: 0, Transaction ID: 2
  TTL: 61, Relay Action: RlyHit
  Not Forwarded, Terminal MEP not reached
  Last egress ID: 0000-0001.0203.0401
  Next egress ID: Not Forwarded
  Ingress interface:
  Action: IngOk, MAC: 0001.0203.0402
  ID: Local: GigE0/0
  Hostname: Local: bcd, address Not specified

Replies dropped: 0

Traceroute at 2009-05-18 12:30:10 explore to ffff.ffff.ffff from 0204.0608.0a0c,
TTL 255, Trans ID 5, Timeout auto, Reply Filter Spanning Tree:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Hostname</th>
<th>Ingr/Egr MAC</th>
<th>Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000-0015.0000.ffe</td>
<td>0015.0000.ffe [Ok]</td>
<td>FDB</td>
</tr>
</tbody>
</table>
  
  Level: 2, version: 0, Transaction ID: 5
  TTL: 254, Relay Action: RlyFDB
  Forwarded, Terminal MEP not reached
  Next-Hop Timeout: 5 seconds
  Delay Model: Logarithmic
  Last egress ID: 0000-0002.0002.0002
  Next egress ID: 0000-0015.0000.ffe
  Ingress interface:
  Action: ELRIngOk, MAC: 0015.0000.ffe
  ID: Local: Gi0/0/0/0.1
2 0001-0030.0000.fffd Egress 0030.0000.fffd [Ok] Drop
Level: 2, version: 0, Transaction ID: 5
TTL: 253, Relay Action: RlyDrop
Not Forwarded, Terminal MEP not reached
Next-Hop Timeout: 5 seconds
Delay Model: Logarithmic
Last egress ID: 0000-0015.0000.fffe
Next egress ID: 0030-0000.0000.fffd
Egress interface:
  Action: ELREgrOk, MAC: 0030.0000.fffd
  ID: Local: G10/1/0/1.2

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute cache, on page 355</td>
<td>Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.</td>
</tr>
<tr>
<td>clear ethernet cfm traceroute-cache, on page 153</td>
<td>Removes the contents of the traceroute cache.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
show ethernet lmi interfaces

To display Ethernet Local Management Interface (E-LMI) information for an interface, including protocol status and error and event statistics, use the `show ethernet lmi interfaces` command in EXEC mode.

```
show ethernet lmi interfaces [type interface-path-id][brief | detail][location location]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>brief</th>
<th>(Optional) Displays summary information about the E-LMI protocol status, number of EVCs and errors, and CE-VLAN/EVC map type.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>detail</td>
<td>(Optional) Displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred, including details about subinterfaces and EVC status.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td></td>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**
- Use the `show interfaces` command to see a list of all interfaces currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

| location location | (Optional) Displays E-LMI information for the designated node. The location argument is entered in the `rack/slot/module` notation. |

**Note**
- The location cannot be specified when you specify an interface type.

**Command Default**
The output displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred since the protocol was enabled on the interface or counters were cleared.

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If Protocol Errors are seen in the output, then the CE device is sending packets to the PE device, but the PE does not understand those packets. This suggests an incorrect implementation of the E-LMI protocol on the CE side, or corruption of the packets on the path between the CE and PE. E-LMI packets have a strictly defined
structure in the MEF 16 standard, and any deviation from that results in a protocol error. The PE will not respond to any packets that are malformed and result in a protocol error.

The Reliability Error counters can indicate that messages are being lost between the PE and CE devices. The timers in the last block of the output should indicate that messages are being sent and received by the PE device. Consider the following actions when these Reliability Errors occur:

- **Status Enq Timeouts**—If this counter is continuously incrementing, it indicates that the Polling Timer on the CE is configured to a greater value than the PVT configuration on the PE. Status Enquiry messages will be sent less frequently than the PVT expects them and PVT timeouts occur. Be sure that the value of the PVT (specified by the `polling-verification-timer` command on the PE) is greater than the Polling Timer value on the CE device.

- **Invalid Sequence Number**—Indicates that messages from the PE are not being received by the CE. Be sure that the correct interface on the CE device is connected to the corresponding E-LMI interface on the PE device, so that communication can take place. Verify that both interfaces are Up.

- **Invalid Report Type**—This error can occur under the following conditions:
  - If the protocol is in the process of a status update and an "E-LMI Check" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.
  - If the protocol is not in the process of a status update and a "Full Status Continued" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.

If the protocol is in the process of a status update and a "Full Status" type of STATUS ENQUIRY is received by the PE, then the PE restarts the status update but does not record any error.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows sample output for the default form of the command:

```
RP/0/RSP0/CPU0:router# show ethernet lmi interfaces
Interface: GigabitEthernet0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

Reliability Errors:
  Status Enq Timeouts 19 Invalid Sequence Number 0
  Invalid Report Type 0

Protocol Errors:
  Malformed PDUs 0 Invalid Protocol Version 0
  Invalid Message Type 0 Out of Sequence IE 0
  Duplicated IE 0 Mandatory IE Missing 0
  Invalid Mandatory IE 0 Invalid non-Mandatory IE 0
  Unrecognized IE 0 Unexpected IE 0
```
Table 18: show ethernet lmi interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface:</td>
<td>Name of the interface running the E-LMI protocol.</td>
</tr>
<tr>
<td>Ether LMI Link Status:</td>
<td>Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).</td>
</tr>
<tr>
<td>UNI Id:</td>
<td>Name of the UNI as configured by the <code>ethernet uni id</code> command. This output field does not appear if the UNI ID is not configured.</td>
</tr>
<tr>
<td>Line Protocol State:</td>
<td>Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.</td>
</tr>
<tr>
<td>MTU (x PDUs reqd for full report)</td>
<td>Maximum Transmission Unit of the interface and the number (x) of E-LMI PDUs of that size required to send one full status report.</td>
</tr>
<tr>
<td>CE-VLAN/EVC Map Type: <code>type (x EVCs)</code></td>
<td>Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values for <code>type</code> are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number <code>x</code> of EVCs in the map are displayed in parentheses.</td>
</tr>
<tr>
<td>Configuration: Status counter</td>
<td>Value of the MEF N393 Status Counter as configured by the <code>status-counter</code> command.</td>
</tr>
<tr>
<td>Polling Verification Timer</td>
<td>Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the <code>polling-verification-timer</code> command. Displays &quot;disabled&quot; if the PVT is turned off.</td>
</tr>
<tr>
<td>Last Data Instance Sent:</td>
<td>Current value of the Data Instance.</td>
</tr>
<tr>
<td>Last Sequence Numbers: Sent x, Received y</td>
<td>Values of the last sent (x) and received (y) sequence numbers as reported in sent PDUs.</td>
</tr>
</tbody>
</table>
Reliability Errors:

Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared:

- **Status Enq Timeouts**—Increments every time the Polling Verification Timer (PVT) expires.
- **Invalid Report Type**—Increments if the Report Type is not appropriate to the protocol's current state. There are four Report Types defined by the E-LMI Standard, and only three of them can appear in Status Enquiry messages that the PE receives. These are: E-LMI Check, Full Status and Full Status Continued.
- **Invalid Sequence Number**—Increments whenever the received sequence number in a Status Enquiry from the CE does not match the last sent sequence number in the PE response. Indicates that messages from the PE are not being received by the CE. The PE continues to respond with the requested Report Type.

For more information about possible actions, see the "Usage Guidelines" section.

Protocol Errors:

(Malformed PDUs, Invalid Message Type, Duplicated IE, and others)

Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.

Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.

Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.

The following example shows sample output for the `show ethernet lmi interfaces brief` form of the command:

```
RP/0/RSP0/CPU0:router# show ethernet lmi interfaces brief
Interface       ELMI  LineP  #     CE-VLAN/
ELMI LineP state state EVCs Errors EVC Map
-------------------------------------------------------------------
G10/0/0/0       Up    Up     3  19 Multiplexing, no bundling
G10/0/0/1       Down Admin-down 1  0 All to One Bundling
```

**Table 19: show ethernet lmi interfaces brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface running the E-LMI protocol.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELMI State</td>
<td>Status of the E-LMI protocol. Possible values are Up, Down, or N/A if the Polling Verification Timer is disabled.</td>
</tr>
<tr>
<td>LineP State</td>
<td>Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.</td>
</tr>
<tr>
<td># EVCs</td>
<td>Total number of EVCs in the CE-VLAN/EVC map.</td>
</tr>
<tr>
<td>Errors</td>
<td>Total number of reliability and protocol errors encountered since the protocol was enabled on the interface or counters were cleared.</td>
</tr>
<tr>
<td>CE-VLAN/EVC Map</td>
<td>Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values are Bundling, All to One Bundling, or Multiplexing, no bundling.</td>
</tr>
</tbody>
</table>

The following example shows sample output for the `show ethernet lmi interfaces detail` form of the command:

```
RP/0/RSP0/CPU0:router #show ethernet lmi interfaces detail
Interface: GigabitEthernet0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128
  Reliability Errors:
    Status Enq Timeouts 19 Invalid Sequence Number 0
    Invalid Report Type 0
  Protocol Errors:
    Malformed PDUs 0 Invalid Protocol Version 0
    Invalid Message Type 0 Out of Sequence IE 0
    Duplicated IE 0 Mandatory IE Missing 0
    Invalid Mandatory IE 0 Invalid non-Mandatory IE 0
    Unrecognized IE 0 Unexpected IE 0
  Full Status Enq Rcvd 00:00:10 ago Full Status Sent 00:00:10 ago
  PDU Rcvd 00:00:00 ago PDU Sent 00:00:00 ago
  LMI Link Status Changed 10:00:00 ago Last Protocol Error never
  Counters cleared never
  Sub-interface: GigabitEthernet0/0/0/0.1
  VLANs: 1,10,20-30, default, untagged/priority tagged
  EVC Status: New, Partially Active
  EVC Type: Multipoint-to-Multipoint
  OAM Protocol: CFM
    CFM Domain: Global (level 5)
    CFM Service: CustomerA
    Remote UNI Count: Configured = 2, Active = 1
  Remote UNI Id Status
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface:</td>
<td>Name of the interface running the E-LMI protocol.</td>
</tr>
<tr>
<td>Ether LMI Link Status:</td>
<td>Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).</td>
</tr>
<tr>
<td>UNI Id:</td>
<td>Name of the UNI as configured by the <code>ethernet uni id</code> command. This output field does not appear if the UNI ID is not configured.</td>
</tr>
<tr>
<td>Line Protocol State:</td>
<td>Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.</td>
</tr>
<tr>
<td>MTU (x PDUs reqd for full report)</td>
<td>Maximum Transmission Unit of the interface and the number (x) of E-LMI PDUs of that size required to send one full status report.</td>
</tr>
<tr>
<td>CE-VLAN/EVC Map Type: <code>type</code> (x EVCs)</td>
<td>Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible valued for <code>type</code> are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number x of EVCs in the map are displayed in parentheses.</td>
</tr>
<tr>
<td>Configuration: Status counter</td>
<td>Value of the MEF N393 Status Counter as configured by the <code>status-counter</code> command.</td>
</tr>
<tr>
<td>Polling Verification Timer</td>
<td>Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the <code>polling-verification-timer</code> command. Displays &quot;disabled&quot; if the PVT is turned off.</td>
</tr>
<tr>
<td>Last Data Instance Sent:</td>
<td>Current value of the Data Instance.</td>
</tr>
<tr>
<td>Last Sequence Numbers: Sent <code>x</code>, Received <code>y</code></td>
<td>Values of the last sent (<code>x</code>) and received (<code>y</code>) sequence numbers as reported in sent PDUs.</td>
</tr>
<tr>
<td>Reliability Errors:</td>
<td>Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared.</td>
</tr>
<tr>
<td>(Status Enq Timeouts, Invalid Report Type, and Invalid Sequence Number)</td>
<td></td>
</tr>
<tr>
<td>Protocol Errors:</td>
<td>Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.</td>
</tr>
<tr>
<td>(Malformed PDUs, Invalid Message Type, Duplicated IE, and others)</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Full Status Enq Recvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.</td>
<td>Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays &quot;never&quot; if the event has not occurred since the protocol was enabled on the interface or counters were cleared.</td>
</tr>
<tr>
<td>Subinterface:</td>
<td>Name of the subinterface corresponding to the EVC.</td>
</tr>
</tbody>
</table>
| VLANs: | VLAN traffic on the interface that corresponds to the EFPs encapsulation, with the following possible values:  
  - Numbers of the matching VLAN IDs  
  - default—Indicates that Default tagging is configured, or the encapsulation specifies to match "any."  
  - none—No matches for the configured encapsulation have occurred on the interface.  
  - untagged/priority—Traffic is either untagged or has priority tagging.  
  **Note** If Q-in-Q encapsulation is configured, only the outer tag is displayed.  
  **Note** If the message "EVC omitted from Full Status due to encapsulation conflict" is displayed above the VLAN output, a misconfiguration has occurred with two or more EFPs having a conflicting encapsulation. |
| EVC Status: | State of the EVC, with the following possible values:  
  - Active—E-LMI is operational for this EVC.  
  - Inactive—All of the remote UNIs are unreachable or down.  
  - New—The EVC has not yet been reported to the CE device.  
  - Not yet known—E-LMI is still waiting to receive the status from CFM. This condition should not persist for more than a few seconds.  
  - Partially Active—One or more of the remote UNIs is unreachable or down. |
| EVC Type: | Type of the EVC, with the following possible values:  
  - "Point-to-Point," "Multipoint-to-Multipoint," or "EVC type not yet known." |
### Field | Description
--- | ---
OAM Protocol: | The OAM protocol from which the EVC status and type are derived. Possible values are either "CFM" or "None."
CFM Domain: | Name of the CFM domain for this EVC.
CFM Service: | Name of the CFM service for this EVC.
Remote UNI Count: Configured = x, Active = y | Number of configured or expected remote UNIs (x) and the number of active remote UNIs (y) within the EVC.
Remote UNI Id: | ID of each remote UNI, including both configured and active remote UNIs where these two sets are not identical. If the number of configured and active remote UNIs is zero, no table is displayed.
Status | Status of each remote UNI, with the following possible values: "Up," "Down," "Admin Down," "Unreachable (a configured remote UNI is not active or missing)," or "Unknown (a remote UNI is active but not reporting its status)."

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet lmi interfaces, on page 154</td>
<td>Clears Ethernet LMI statistics on one or all interfaces.</td>
</tr>
</tbody>
</table>
show ethernet loopback active

To display the loopback sessions that are currently active, use the `show ethernet loopback active` command in the EXEC mode.

```
show ethernet loopback active {interface interface name | brief}
```

**Syntax Description**

- `interface interface name`: Displays the active loopback sessions for this specified interface.
- `brief`: Displays a brief information of the active loopback sessions on all interfaces.

**Command Default**

Displays the information of active loopback sessions on all interfaces.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output of the `show ethernet loopback active brief` command:

```
RP/0/RSP0/CPU0:router>show ethernet loopback active brief

Interface ID    Direction Time left Status
-----------------------------
GigabitEthernet0/0/0/0 1 External 01:23:45 Starting
TenGigE0/1/0/0.200 1 Internal 00:01:17 Active
TenGigE0/1/0/0.200 2 External 00:00:00 Stopping
```

Each row in the table corresponds to a loopback session which is currently active. For each session, these fields are displayed:

- **Interface**: The interface on which the loopback session is running.
- **ID**: The session ID allocated to the session when it was started.
- **Direction**: The direction of the loopback session.
- **Time left**: The amount of time left until the loopback session is automatically stopped.
- **Status**: The status of the loopback session.
show ethernet loopback permitted

To display all the interfaces which are permitted to run loopback sessions, use the `show ethernet loopback permitted` command in the EXEC mode.

Syntax Description
This command has no keywords or arguments.

Command Default
No default behavior or values

Command Modes
EXEC(#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

Example

This example shows a sample output of the `show ethernet loopback permitted` command:

```
RP/0/RSP0/CPU0:router#show ethernet loopback permitted

Interface          Direction
------------------------------------
GigabitEthernet0/0/0          External
GigabitEthernet0/0/0.100       Internal
TenGigE0/1/0/0.200          External, Internal
```

These are the description of the fields in the command output:

- **Interface**: Specifies the interface on which loopback is permitted.
- **Direction**: Specifies the direction in which the loopback is permitted on that interface.
show ethernet oam configuration

To display the current active Ethernet OAM configuration on an interface, use the `show ethernet oam configuration` command in EXEC mode.

```
show ethernet oam configuration [interface type interface-path-id]
```

**Syntax Description**

- **interface type** (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** (Optional) Physical interface or virtual interface.
  
  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

If no parameters are specified, the configurations for all Ethernet OAM interfaces is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the Ethernet OAM configuration information for all interfaces, or a specified interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display Ethernet OAM configuration information for a specific interface:

```
RP/0/RSP0/CPU0:router# show ethernet oam configuration interface gigabitethernet 0/4/0/0
Thu Aug 5 21:54:34.050 DST
GigabitEthernet0/4/0/0:
  Hello interval: 1s
  Link monitoring enabled: Y
  Remote loopback enabled: N
  Mib retrieval enabled: N
  Uni-directional link-fault detection enabled: N
  Configured mode: Active
  Connection timeout: 5
  Symbol period window: 0
  Symbol period low threshold: 1
  Symbol period high threshold: None
```
The following example shows how to display the configuration for all EOAM interfaces:

```
RP/0/RSP0/CPU0:router# show ethernet oam configuration
Thu Aug 5 22:07:06.870 DST
GigabitEthernet0/4/0/0:
  Hello interval: 1s
  Link monitoring enabled: Y
  Remote loopback enabled: N
  Mib retrieval enabled: N
  Uni-directional link-fault detection enabled: N
  Configured mode: Active
  Connection timeout: 5
  Symbol period window: 0
  Symbol period low threshold: 1
  Symbol period high threshold: None
  Frame window: 1000
  Frame low threshold: 1
  Frame high threshold: None
  Frame period window: 1000
  Frame period low threshold: 1
  Frame period high threshold: None
  Frame seconds window: 60000
  Frame seconds low threshold: 1
  Frame seconds high threshold: None
  High threshold action: None
  Link fault action: Log
  Dying gasp action: Log
  Critical event action: Log
  Discovery timeout action: Log
  Capabilities conflict action: Log
  Wiring conflict action: Error-Disable
  Session up action: Log
  Session down action: Log
  Remote loopback action: Log
  Require remote mode: Ignore
  Require remote MIB retrieval: N
  Require remote loopback support: N
  Require remote link monitoring: N
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam discovery, on page 319</td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td>show ethernet oam statistics, on page 325</td>
<td>Displays the local and remote Ethernet OAM statistics for interfaces.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
### show ethernet oam discovery

To display the currently configured OAM information of Ethernet OAM sessions on interfaces, use the `show ethernet oam discovery` command in EXEC mode.

```
show ethernet oam discovery [ { brief | interface type interface-path-id [remote] }]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>Displays minimal, currently configured OAM information in table form.</td>
</tr>
<tr>
<td>interface type</td>
<td>(Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>remote</td>
<td>(Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.</td>
</tr>
</tbody>
</table>

**Command Default**

Displays detailed information for Ethernet OAM sessions on all interfaces.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to display the minimal, currently configured OAM information for Ethernet OAM sessions on all interfaces:

```
RP/0/RSP0/CPU0:router# show ethernet oam discovery brief
```

```
Sat Jul 4 13:52:42.949 PST
Flags:
   L - Link Monitoring support
   M - MIB Retrieval support
   R - Remote Loopback support
   U - Unidirectional detection support
   * - data is unavailable
```
The following examples show how to display detailed, currently configured OAM information for the Ethernet OAM session on a specific interface:

```
RP/0/RSP0/CPU0:router# show ethernet oam discovery interface gigabitethernet 0/1/5/1
```

```
Sat Jul 4 13:56:49.967 PST
GigabitEthernet0/1/5/1:
Local client
----------
Administrative configuration:
  PDU revision:            1
  Mode:                   Active
  Unidirectional support: N
  Link monitor support:   Y
  Remote loopback support: N
  MIB retrieval support:  N
  Maximum PDU size:       1500
  Mis-wiring detection key: 5E9D

Operational status:
  Port status:             Active send
  Loopback status:         None
  Interface mis-wired:     N

Remote client
----------
MAC address: 0030.96fd.6bfa
Vendor (OUI): 00.00.0C (Cisco)

Administrative configuration:
  PDU revision:            5
  Mode:                   Passive
  Unidirectional support: N
  Link monitor support:   Y
  Remote loopback support: Y
  MIB retrieval support:  N
  Maximum PDU size:       1500
```
show ethernet oam event-log

To display the most recent OAM event logs per interface, use the **show ethernet oam event-log** command in EXEC mode.

**show ethernet oam event-log** [interface interface ] [detail]

**Syntax Description**
- **interface interface** Filters the output to only include events for the specified interface.
- **detail** Displays additional details like threshold value, breaching value, total running errors and window size of a particular interface.

**Command Default**
This command displays event logs for all interfaces which have OAM configured.

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to display the event logs for all interfaces which have OAM configured:

```
RP/0/RSP0/CPU0:router# show ethernet oam event-log
Wed Jan 23 06:16:46.684 PST
Local Action Taken:
    N/A - No action needed         EFD - Interface brought down using EFD
    None - No action taken         Err.D - Interface error-disabled
    Logged - System logged

GigabitEthernet0/1/0/0
------------------------------------------
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Loc'n</th>
<th>Action</th>
<th>Threshold</th>
<th>Breaching Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Jan 23 06:13:25 PST</td>
<td>Symbol period</td>
<td>Local</td>
<td>N/A</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Wed Jan 23 06:13:33 PST</td>
<td>Frame</td>
<td>Local</td>
<td>N/A</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Wed Jan 23 06:13:37 PST</td>
<td>Frame period</td>
<td>Local</td>
<td>None</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Wed Jan 23 06:13:45 PST</td>
<td>Frame seconds</td>
<td>Local</td>
<td>N/A</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Wed Jan 23 06:13:57 PST</td>
<td>Dying gasp</td>
<td>Remote</td>
<td>Logged</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

GigabitEthernet0/1/0/1
------------------------------------------
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Loc'n</th>
<th>Action</th>
<th>Threshold</th>
<th>Breaching Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Jan 23 06:26:14 PST</td>
<td>Dying gasp</td>
<td>Remote</td>
<td>Logged</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Wed Jan 23 06:33:25 PST</td>
<td>Symbol period</td>
<td>Local</td>
<td>N/A</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Wed Jan 23 06:43:33 PST</td>
<td>Frame period</td>
<td>Remote</td>
<td>N/A</td>
<td>9</td>
<td>12</td>
</tr>
</tbody>
</table>
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ethernet oam configuration, on page 316</strong></td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td><strong>show ethernet oam discovery, on page 319</strong></td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td><strong>show ethernet oam interfaces, on page 323</strong></td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
show ethernet oam interfaces

To display the current state of Ethernet OAM interfaces, use the `show ethernet oam interfaces` command in EXEC mode.

```
show ethernet oam interfaces [interface type interface-path-id]
```

**Syntax Description**

- `interface type` (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.

- `interface-path-id` Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No parameters displays the current state for all Ethernet OAM interfaces.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID Operations
--- ------------
ethernet-services read
```

**Examples**

The following example shows how to display the current state for all Ethernet OAM interfaces:

```
RP/0/RSP0/CPU0:router# show ethernet oam interfaces
GigabitEthernet0/0/0/0
In REMOTE_OK state
Local MWD key: 80081234
Remote MWD key: 8F08ABCC
EFD triggered: Yes (link-fault)
```
Table 21: show ethernet oam interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In type state</td>
<td>The possible discovery state type values are:</td>
</tr>
<tr>
<td></td>
<td>• ACTIVE_SEND_LOCAL—The interface is configured in active mode (the default), but no Information PDUs have been received from the peer (except possibly link-fault PDUs). Information PDUs are sent.</td>
</tr>
<tr>
<td></td>
<td>• FAULT—A local unidirectional link fault has been detected. Link-fault PDUs are sent.</td>
</tr>
<tr>
<td></td>
<td>• INACTIVE—The interface is down.</td>
</tr>
<tr>
<td></td>
<td>• PASSIVE_WAIT—The interface is configured in passive mode (mode passive command) but no Information PDUs have been received from the peer (except possibly link-fault PDUs). No PDUs are sent.</td>
</tr>
<tr>
<td></td>
<td>• REMOTE—(Also known as SEND_LOCAL_REMOTE). Information PDUs are being sent and received, but the local device is not satisfied with the remote peer's capabilities (for example, because there is a 'require-remote' configuration and the peer does not have the required capabilities).</td>
</tr>
<tr>
<td></td>
<td>• REMOTE_OK—(Also known as SEND_LOCAL_REMOTE_OK). Information PDUs are being sent and received, and the local device is satisfied with the peer's capabilities, but the remote peer is not satisfied with the local device capabilities (for example, because there is a 'require-remote' configuration on the peer device).</td>
</tr>
<tr>
<td></td>
<td>• SEND_ANY—The discovery process has completed, both devices are satisfied with the configuration and the session is up. All types of PDU can be sent and received.</td>
</tr>
<tr>
<td>EFD triggered</td>
<td>Indicates if an Ethernet Fault Detection (EFD) event has occurred on the interface and the type of fault that triggered the interface to be moved to the down state for the line protocol. The possible EFD trigger events are:</td>
</tr>
<tr>
<td></td>
<td>• capabilities-conflict</td>
</tr>
<tr>
<td></td>
<td>• discovery-timeout</td>
</tr>
<tr>
<td></td>
<td>• link-fault</td>
</tr>
<tr>
<td></td>
<td>• session-down</td>
</tr>
<tr>
<td></td>
<td>• wiring-conflict</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td>show ethernet oam discovery, on page 319</td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td>show ethernet oam statistics, on page 325</td>
<td>Displays the local and remote Ethernet OAM statistics for interfaces.</td>
</tr>
</tbody>
</table>
show ethernet oam statistics

To display the local and remote Ethernet OAM statistics for interfaces, use the `show ethernet oam statistics` command in EXEC mode.

```
show ethernet oam statistics [interface type interface-path-id [remote]]
```

**Syntax Description**

- **interface type** (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **remote** (Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.

**Command Default**

No parameters displays statistics for all Ethernet OAM interfaces.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display Ethernet OAM statistics for a specific interface:

```
RP/0/RSP0/CPU0:router# show ethernet oam statistics interface gigabitethernet 0/1/5/1
```

```
GigabitEthernet0/1/5/1:
Counters
----------
Information OAMPDU Tx  161177
Information OAMPDU Rx  151178
Unique Event Notification OAMPDU Tx  0
Unique Event Notification OAMPDU Rx  0
Duplicate Event Notification OAMPDU Tx  0
Duplicate Event Notification OAMPDU Rx  0
Loopback Control OAMPDU Tx  0
Loopback Control OAMPDU Rx  0
```
show ethernet oam statistics

Variable Request OAMPDU Tx 0
Variable Request OAMPDU Rx 0
Variable Response OAMPDU Tx 0
Variable Response OAMPDU Rx 0
Organization Specific OAMPDU Tx 0
Organization Specific OAMPDU Rx 0
Unsupported OAMPDU Tx 45
Unsupported OAMPDU Rx 0
Frames Lost due to OAM 23
Fixed frames Rx 1

Local event logs
----------------
Errored Symbol Period records 0
Errored Frame records 0
Errored Frame Period records 0
Errored Frame Second records 0

Remote event logs
-----------------
Errored Symbol Period records 0
Errored Frame records 0
Errored Frame Period records 0
Errored Frame Second records 0

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam configuration, on page 316</td>
<td>Displays the current active Ethernet OAM configuration on an interface.</td>
</tr>
<tr>
<td>show ethernet oam discovery, on page 319</td>
<td>Displays the current status of Ethernet OAM sessions.</td>
</tr>
<tr>
<td>show ethernet oam interfaces, on page 323</td>
<td>Displays the current state of Ethernet OAM interfaces.</td>
</tr>
</tbody>
</table>
show ethernet sla configuration-errors

To display information about errors that are preventing configured Ethernet Service Level Agreement (SLA) operations from becoming active, as well as any warnings that have occurred, use the `show ethernet sla configuration-errors` command in EXEC mode.

```
show ethernet sla configuration-errors [domain domain-name] [interface type interface-path-id] [profile profile-name]
```

**Syntax Description**

- **domain domain-name**  Displays information for the specified domain, where `domain-name` is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.

- **interface type**  (Optional) Displays information for the specified interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**  Physical interface or virtual interface.

  **Note**  Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **profile profile-name**  (Optional) Displays information for the specified profile name.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- ethernet-services  read, write

**Examples**

The following example shows how to display information about errors that are preventing configured SLA operations from becoming active:

```
RP/0/RSP0/CPU0:router# show ethernet sla configuration-errors

Errors:
-------
Profile 'gold' is not defined but is used on Gi0/0/0/0.0
```
Profile 'red' defines a test-pattern, which is not supported by the type

The following example shows the errors from configured Ethernet SLA operations that cannot be represented correctly in the MEF-SOAM-PM-MIB:

```
RP/0/RSP0/CPU0:router# show ethernet sla configuration-errors
Mon Aug 18 12:21:31.355 CEST
```

Profile 'gold': This operation cannot be fully represented in the MEF-SOAM-PM-MIB due to burst configuration being present

Profile 'red': This operation cannot be fully represented in the MEF-SOAM-PM-MIB due to the use of bin configuration for loss measurement

---

**Note**

The operations will still work and statistics will still be gathered and retrievable using `show` commands. However, you cannot retrieve all profile data from the MIB.

The following configuration errors reflect profiles that work but have no data retrievable from the MIB:

- This operation cannot be represented in the MEF-SOAM-PM-MIB as not all metrics have the same bucket size
- This operation cannot be represented in the MEF-SOAM-PM-MIB as the probe interval is not the probe duration and there are multiple buckets per probe

The following configuration errors reflect profiles that are only partially represented in the MIB:

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This operation cannot be fully represented in the MEF-SOAM-PM-MIB as the probe interval is not the probe duration and there are multiple probes per bucket</td>
<td>The breakdown of the bucket into multiple probes is not represented in the MIB, but the statistics data is present.</td>
</tr>
<tr>
<td>This operation cannot be fully represented in the MEF-SOAM-PM-MIB as it contains multiple delay/jitter metrics with differing numbers of bins</td>
<td>The bin count (a per-session per-&quot;metric class&quot; parameter in the MIB) is not displayed in the MIB, but all remaining configuration (including per-metric bin configuration) and all statistics (including per-bin statistics) are displayed.</td>
</tr>
<tr>
<td>This operation cannot be fully represented in the MEF-SOAM-PM-MIB due to burst configuration being present</td>
<td>The burst configuration itself cannot be represented in the MIB, but the statistics for the operation are available in the MIB.</td>
</tr>
<tr>
<td>This operation cannot be fully represented in the MEF-SOAM-PM-MIB due to the use of bin configuration for loss measurement</td>
<td>The bin configuration and the per-bin results cannot be exported by the MIB, but the remaining configuration and per-bucket results are available.</td>
</tr>
<tr>
<td>This operation cannot be fully represented in the MEF-SOAM-PM-MIB due to the use of a padding pattern other than all zeros or all ones</td>
<td>The configured padding pattern will not be represented in the MIB.</td>
</tr>
</tbody>
</table>
show ethernet sla operations

To display information about configured Ethernet Service Level Agreement (SLA) operations, use the `show ethernet sla operations` command in EXEC mode.

```
show ethernet sla operations [detail] [domain domain-name] [interface type interface-path-id] [{on-demand {all | id}} | profile {profile-name | all}] ]
```

**Syntax Description**

- **detail** (Optional) Displays detailed information.
- **domain domain-name** (Optional) Displays information for the specified domain, where `domain-name` is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
- **interface type** (Optional) Displays information for the specified interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Displays information for the specified interface.
  
  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **on-demand all** (Optional) Displays information for all on-demand operations.
- **on-demand id** (Optional) Displays information for the specified on-demand operation, where `id` is the number of the operation.
- **profile profile-name** (Optional) Displays information for the specified profile name.
- **profile all** (Optional) Displays information for all profiles.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

- **Release 3.9.0** This command was introduced.
- **Release 4.0.0** The `on-demand {all | id}` and `profile all` keyword options were added.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to display information about configured SLA operations in brief:

RP/0/RSP0/CPU0:router# show ethernet sla operations

<table>
<thead>
<tr>
<th>Profile</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>G10/0/0/0, dom d, to MEP-ID 200 !</td>
</tr>
<tr>
<td>business-gold</td>
<td>G10/0/0/0, dom mydom, to 00ab.cdef.1234</td>
</tr>
<tr>
<td>business-gold</td>
<td>G10/0/0/0, dom mydom, to MEP-ID 2</td>
</tr>
</tbody>
</table>

If the SLA operation has a configuration error, an exclamation point (!) is displayed at the end of the line in the command output.

The following example shows how to display information about configured SLA operations in detail:

RP/0/RSP0/CPU0:router# show ethernet sla operations detail

Source: Interface GigabitEthernet0/0/0/0, Domain d
Destination: Target MEP-ID 200
Profile 'gold'
Profile is not configured

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MAC Address 00ab.cdef.1234
Profile 'business-gold'
Probe type 'cfm-delay-measurement':
- burst sent every 1min, each of 20 packets sent every 100ms
- Measures RT Delay: 5 bins; 1 buckets/probe; 75 of 100 archived
- Measures RT Jitter (interval 1): no aggregation; 5 probes/bucket; 10 of 10 archived
- Scheduled to run every 5min first at 00:02:00 UTC for 2min (2 bursts)
  last run at 07:32:00 PST Tue 19 January 2010

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
Profile 'business-gold'
Probe type 'cfm-delay-measurement':
- burst sent every 1min, each of 20 packets sent every 100ms
- Measures RT Delay: 5 bins; 1 buckets/probe; 75 of 100 archived
- Measures RT Jitter (interval 1): no aggregation; 5 probes/bucket; 10 of 10 archived
- Scheduled to run every 5min first at 00:02:00 UTC for 2min (2 bursts)
  last run at 07:32:00 PST Tue 19 January 2010

The following example shows how to display information about on-demand SLA operations in detail:

RP/0/RSP0/CPU0:router# show ethernet sla operations detail on-demand

Source: Interface GigabitEthernet0/0/0.0, Domain mydom
Destination: Target MAC Address 00ab.cdef.1234
On-demand operation ID #6
Probe type 'cfm-loopback':
burst sent every 10s, each of 10 packets sent every 1s
packets padded to 1024 bytes with pattern 0xabcd56ef
packets use priority value of 3
Measures RT Delay: no aggregation; 1 buckets/probe; 1 of 100 archived
Started at 12:01:49 GMT Tue 02 March 2010, runs every 1hr for 1hr (360 bursts)
repeats 10 times, ends at 22:01:49 GMT Tue 02 March 2010

The following example shows how to display information about configured and on-demand SLA operations on a specific interface:

RP/0/RSP0/CPU0:router# **show ethernet sla operations interface gigabitethernet 0/0/0/0.0 detail**

Interface GigabitEthernet 0/0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234
----------------------------------------------------------------------------
Profile 'business-gold'
Probe type CFM-delay-measurement:
bursts sent every 1min, each of 20 packets sent every 100ms
packets padded to 1500 bytes with zeroes
packets use priority value of 7
Measures RTT: 5 bins 20ms wide; 2 buckets/ probe; 75/100 archived
Measures Jitter (interval 1): 3 bins 40ms wide; 2 buckets/probe; 50 archived
Scheduled to run every Sunday at 4am for 2 hours:
last run at 04:00 25/05/2008
show ethernet sla statistics

To display the contents of buckets containing Ethernet Service Level Agreement (SLA) metrics collected by probes, use the `show ethernet sla statistics` command in EXEC mode.

```
show ethernet sla statistics [{current | history}] [detail] [domain domain-name] [interface type interface-path-id] [{on-demand {allid} | profile {profile-name | all}}] [statistic stat-type]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>(Optional) Displays the content of buckets currently being filled.</td>
</tr>
<tr>
<td>history</td>
<td>(Optional) Displays the content of all full buckets.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed content of buckets.</td>
</tr>
<tr>
<td>domain domain-name</td>
<td>(Optional) Displays the content of buckets for the specified domain, where</td>
</tr>
<tr>
<td></td>
<td><code>domain-name</code> is a string of a maximum of 80 characters that identifies the</td>
</tr>
<tr>
<td></td>
<td>domain where the SLA operation is configured.</td>
</tr>
<tr>
<td>interface type</td>
<td>(Optional) Displays the content of buckets for the specified interface type.</td>
</tr>
<tr>
<td></td>
<td>For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Displays the content of buckets for the specified interface.</td>
</tr>
<tr>
<td>on-demand all</td>
<td>(Optional) Displays the content of buckets for all on-demand operations.</td>
</tr>
<tr>
<td>on-demand id</td>
<td>(Optional) Displays the content of buckets for the specified on-demand operation, where <code>id</code> is the number of the operation.</td>
</tr>
<tr>
<td>profile profile-name</td>
<td>(Optional) Displays the content of buckets for the specified profile name.</td>
</tr>
<tr>
<td>profile all</td>
<td>(Optional) Displays the content of buckets for all profiles.</td>
</tr>
<tr>
<td>statistic stat-type</td>
<td>(Optional) Displays only the specified type of statistic. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-delay-ds</code>—Displays only one-way (destination-to-source) delay.</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-delay-sd</code>—Displays only one-way (source-to-destination) delay.</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-jitter-ds</code>—Displays only one-way (destination-to-source) jitter.</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-jitter-sd</code>—Displays only one-way (source-to-destination) jitter.</td>
</tr>
<tr>
<td></td>
<td>• <code>round-trip-delay</code>—Displays only round-trip delay.</td>
</tr>
<tr>
<td></td>
<td>• <code>round-trip-jitter</code>—Displays only round-trip jitter.</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-loss-ds</code>—Displays only one-way (destination-to-source) loss.</td>
</tr>
<tr>
<td></td>
<td>• <code>one-way-loss-sd</code>—Displays only one-way (source-to-destination) loss.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.
show ethernet sla statistics

Command Default
No default behavior or values

Command Modes
EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The one-way-delay-ds, one-way-delay-sd, one-way-jitter-ds, and one-way-jitter-sd statistics type keywords were added.</td>
</tr>
<tr>
<td></td>
<td>The on-demand all and on-demand id keyword options and arguments were added.</td>
</tr>
<tr>
<td></td>
<td>When the detail keyword is used, the “occurred at” field was added to the display output to show when the last Min/Max statistic happened.</td>
</tr>
<tr>
<td>4.3.0</td>
<td>The one-way-loss-ds, one-way-loss-sd statistic type keywords were added.</td>
</tr>
</tbody>
</table>

Usage Guidelines
See the Usage Guidelines in the buckets size command for a description of buckets.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples
This example shows how to display the current contents of buckets containing SLA metrics collected by probes in brief:

RP/0/RSP0/CPU0:router# show ethernet sla statistics

Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
Profile 'business-gold', packet type 'cfm-delay-measurement'
Scheduled to run every 5min first at 00:02:00 UTC for 2min

Round Trip Delay
~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: 0.24ms; Max: 0.49ms; Mean: 0.34ms; StdDev: 0.05ms

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: 0.24ms; Max: 0.69ms; Mean: 0.34ms; StdDev: 0.12ms

Round Trip Jitter
~~~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
This example shows how to display the current contents of buckets containing SLA metrics collected by probes in detail:

Note

In this example, the round-trip-delay measurement is configured with aggregation (and hence bins are displayed), whereas the round-trip-jitter measurement is configured with no aggregation (and hence individual samples are displayed).

```
RP/0/RSP0/CP00:router# show ethernet sla statistics detail
Source: Interface GigabitEthernet0/0/0/0, Domain mydom
Destination: Target MEP-ID 2
Profile 'business-gold', packet type 'cfm-delay-measurement'
Scheduled to run every 5min first at 00:02:00 UTC for 2min

Round Trip Delay
~~~~~~~~~~~~~~
1 buckets per probe

Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: 0.24ms, occurred at 07:47:29 on Tue 19 Jan 2010 UTC
Max: 0.49ms, occurred at 07:48:04 on Tue 19 Jan 2010 UTC
Mean: 0.34ms; StdDev: 0.05ms

<table>
<thead>
<tr>
<th>Range</th>
<th>Samples</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 20 ms</td>
<td>20 (100.0%)</td>
<td>20 (100.0%)</td>
<td>0.34ms</td>
</tr>
<tr>
<td>20 to 40 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>40 to 60 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>60 to 80 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>&gt; 80 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
</tbody>
</table>

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: 0.24ms, occurred at 07:53:10 on Tue 19 Jan 2010 UTC
Max: 0.69ms, occurred at 07:53:42 on Tue 19 Jan 2010 UTC
Mean: 0.34ms; StdDev: 0.12ms

<table>
<thead>
<tr>
<th>Range</th>
<th>Samples</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 20 ms</td>
<td>20 (100.0%)</td>
<td>20 (100.0%)</td>
<td>0.34ms</td>
</tr>
<tr>
<td>20 to 40 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>40 to 60 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>60 to 80 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
<tr>
<td>&gt; 80 ms</td>
<td>0 (0.0%)</td>
<td>20 (100.0%)</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Round Trip Jitter
~~~~~~~~~~~~~~~~
1 buckets per probe
Bucket started at 07:47:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: -0.25ms, occurred at 07:47:53 on Tue 19 Jan 2010 UTC
Max: 0.13ms, occurred at 07:48:11 on Tue 19 Jan 2010 UTC
Mean: -0.01ms; StdDev: 0.08ms

Samples:
<table>
<thead>
<tr>
<th>Time sent</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:47:00.0</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>07:47:00.1</td>
<td>-0.12ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.2</td>
<td>0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.3</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.4</td>
<td>-0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.5</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.6</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.7</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.8</td>
<td>0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:47:00.9</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.0</td>
<td>0.11ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.1</td>
<td>-0.25ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.2</td>
<td>0.13ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.3</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.4</td>
<td>-0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.5</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.6</td>
<td>0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.7</td>
<td>-0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.8</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:48:00.9</td>
<td>0.00ms</td>
<td></td>
</tr>
</tbody>
</table>

Bucket started at 07:52:00 PST Tue 19 January 2010 lasting 2min
Pkts sent: 20; Lost: 0 (0.0%); Corrupt: 0 (0.0%); Misordered: 0 (0.0%)
Min: -0.38ms, occurred at 07:52:13 on Tue 19 Jan 2010 UTC
Max: 0.38ms, occurred at 07:53:26 on Tue 19 Jan 2010 UTC
Mean: -0.02ms; StdDev: 0.14ms

Samples:
<table>
<thead>
<tr>
<th>Time sent</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:52:00.0</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>07:52:00.1</td>
<td>-0.38ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.2</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.3</td>
<td>-0.05ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.4</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.5</td>
<td>0.05ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.6</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.7</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.8</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:52:00.9</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.0</td>
<td>0.38ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.1</td>
<td>-0.32ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.2</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.3</td>
<td>-0.13ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.4</td>
<td>0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.5</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.6</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.7</td>
<td>0.00ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.8</td>
<td>0.06ms</td>
<td></td>
</tr>
<tr>
<td>07:53:00.9</td>
<td>0.00ms</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to display the current contents of buckets containing SLA metrics collected by probes on a specific interface:
show ethernet sla statistics current interface GigabitEthernet 0/0/0.0

Interface GigabitEthernet 0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234

Profile 'business-gold', packet type 'cfm-superpacket'
Scheduled to run every Sunday at 4am for 2 hours

Round Trip Delay
~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
  Pkts sent: 2342; Lost 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
  Min: 13ms; Max: 154ms; Mean: 28ms; StdDev: 11ms

Round Trip Jitter
~~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
  Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
  Min: -5ms; Max: 8ms; Mean: 0ms; StdDev: 3.6ms

This example shows how to display a history detail of buckets containing SLA metrics collected by probes on a specific interface:

show ethernet sla history detail GigabitEthernet 0/0/0.0

Interface GigabitEthernet 0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234

Profile 'business-gold', packet type 'cfm-loopback'
Scheduled to run every Sunday at 4am for 2 hours

Round Trip Delay
~~~~~~~~~~~~~~~
2 buckets per probe

Bucket started at 04:00 Sun 17 Feb 2008 lasting 1 hour:
  Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
  Min: 13ms, occurred at 04:43:29 on Sun 22 Aug 2010 UTC
  Max: 154ms, occurred at 05:10:32 on Sun 22 Aug 2010 UTC
  Mean: 28ms; StdDev: 11ms

Results suspect as more than 10 seconds time drift detected
Results suspect as scheduling latency prevented some packets being sent

Samples:

<table>
<thead>
<tr>
<th>Time sent</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:00:01.324</td>
<td>23ms</td>
<td></td>
</tr>
<tr>
<td>04:00:01.425</td>
<td>36ms</td>
<td></td>
</tr>
<tr>
<td>04:00:01.525</td>
<td></td>
<td>Timed Out</td>
</tr>
</tbody>
</table>

Round Trip Jitter
~~~~~~~~~~~~~~~~
2 buckets per probe
Bucket started at 04:00 Sun 17 Feb 2008, lasting 1 hour:
Pkts sent: 2342; Lost: 2 (0%); Corrupt: 0 (0%); Misordered: 0 (0%)
Min: -5ms, occurred at 04:15:03 on Sun 22 Aug 2010 UTC
Max: 10ms, occurred at 05:29:15 on Sun 22 Aug 2010 UTC
Mean: 0ms; StdDev: 3.6ms

Samples:
<table>
<thead>
<tr>
<th>Time sent</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:00:01.324</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>04:00:01.425</td>
<td>13ms</td>
<td></td>
</tr>
<tr>
<td>04:00:01.525</td>
<td>- Timed out</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to display statistics for all full buckets for on-demand operations in detail:

RP/0/RSP0/CPU0:router# show ethernet sla statistics history detail on-demand

Interface GigabitEthernet0/0/0.1
Domain mydom Service myser to 0123.4567.890A

On-demand operation ID #1, packet type 'cfm-delay-measurement'
Started at 15:38 on 06 July 2010 UTC, runs every 1 hour for 1 hour

Round Trip Delay
~~~~~~~~~~~~~~~~
1 bucket per probe

Bucket started at 15:38 on Tue 06 Jul 2010 UTC, lasting 1 hour:
Pkts sent: 1200; Lost: 4 (0%); Corrupt: 600 (50%); Misordered: 0 (0%)
Min: 13ms, occurred at 15:43:29 on Tue 06 Jul 2010 UTC
Max: 154ms, occurred at 16:15:34 on Tue 06 Jul 2010 UTC
Mean: 28ms; StdDev: 11ms

Bins:
<table>
<thead>
<tr>
<th>Range</th>
<th>Samples</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 20 ms</td>
<td>194 (16%)</td>
<td>194 (16%)</td>
<td>17ms</td>
</tr>
<tr>
<td>20 - 40 ms</td>
<td>735 (61%)</td>
<td>929 (77%)</td>
<td>27ms</td>
</tr>
<tr>
<td>40 - 60 ms</td>
<td>212 (18%)</td>
<td>1141 (95%)</td>
<td>45ms</td>
</tr>
<tr>
<td>&gt; 60 ms</td>
<td>55 (5%)</td>
<td>1196</td>
<td>70ms</td>
</tr>
</tbody>
</table>

Bucket started at 16:38 on Tue 01 Jul 2008 UTC, lasting 1 hour:
Pkts sent: 3600; Lost: 12 (0%); Corrupt: 1800 (50%); Misordered: 0 (0%)
Min: 19ms, occurred at 17:04:08 on Tue 06 Jul 2010 UTC
Max: 70ms, occurred at 16:38:00 on Tue 06 Jul 2010 UTC
Mean: 28ms; StdDev: 11ms

Bins:
<table>
<thead>
<tr>
<th>Range</th>
<th>Samples</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 20 ms</td>
<td>194 (16%)</td>
<td>194 (16%)</td>
<td>19ms</td>
</tr>
<tr>
<td>20 - 40 ms</td>
<td>735 (61%)</td>
<td>929 (77%)</td>
<td>27ms</td>
</tr>
<tr>
<td>40 - 60 ms</td>
<td>212 (18%)</td>
<td>1141 (95%)</td>
<td>45ms</td>
</tr>
<tr>
<td>&gt; 60 ms</td>
<td>55 (5%)</td>
<td>1196</td>
<td>64ms</td>
</tr>
</tbody>
</table>

This example shows how to display the current contents of buckets containing SLM metrics collected by probes on a specific interface:

RP/0/RSP0/CPU0:router# show ethernet sla statistics current interface GigabitEthernet 0/0/0/0.0

Interface GigabitEthernet0/0/0.0
Domain mydom Service myser to 00AB.CDEF.1234

Profile 'business-gold', packet type 'cfm-synthetic-loss-measurement'

Scheduled to run every day at 11:50 UTC for 10min (10 bursts)
Frame Loss Ratio calculated every 1min

One-Way Frame Loss (Source->Dest)

1 probes per bucket

Bucket started at 11:50:00 UTC Fri 01 January 2010 lasting 10min
  Pkts sent: 600; Lost: 62 (10.3%); Corrupt: 0 (0.0%);
  Misordered: 56 (9.3%); Duplicates: 0 (0.0%)
  Min: 1.67%; Max: 21.67%; Mean: 10.05%; StdDev: 2.34%; Overall: 10.03%

Bucket started at 11:50:00 UTC Sat 02 January 2010 lasting 10min
  Pkts sent: 600; Lost: 23 (3.8%); Corrupt: 0 (0.0%);
  Misordered: 56 (9.3%); Duplicates: 0 (0.0%)
  Min: 1.67%; Max: 11.67%; Mean: 3.08%; StdDev: 1.34%; Overall: 3.03%

This example shows how to display statistics for all full buckets for on-demand operations in detail:

RP/0/RSP0/CPU0:router#show ethernet sla statistics history detail on-demand

Interface GigabitEthernet0/0/0.1
Domain mydom Service myser to 0123.4567.890A

On-demand operation ID #1, packet type 'cfm-synthetic-loss-measurement'
Started at 15:38 on 01 July 2008, runs every 1 hour for 1 hour
Frame Loss Ratio calculated every 10min

One-Way Frame Loss (Source->Dest)

1 probes per bucket

Bucket started at 15:38 on Tue 01 Jul 2008, lasting 1 hour:
  Pkts sent: 1200; Lost: 132 (11%); Corrupt: 0 (0%);
  Misordered: 129 (10.8%); Duplicate: 0 (0%)
  Min: 8.00%, occurred at 15:43:29 on Tue 01 Jul 2008 UTC
  Max: 12.12%, occurred at 16:15:34 on Tue 01 Jul 2008 UTC
  Mean: 10.02%; StdDev: 0.98%; Overall: 10.00%

Bins:

<table>
<thead>
<tr>
<th>Range</th>
<th>Count</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5%</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>-------</td>
</tr>
<tr>
<td>5 to 10%</td>
<td>2 (33%)</td>
<td>2 (33%)</td>
<td>9.4%</td>
</tr>
<tr>
<td>10 to 15%</td>
<td>4 (67%)</td>
<td>6 (100%)</td>
<td>10.5%</td>
</tr>
<tr>
<td>&gt; 15%</td>
<td>0 (0%)</td>
<td>6 (100%)</td>
<td></td>
</tr>
</tbody>
</table>

Bucket started at 16:38 on Tue 01 Jul 2008, lasting 1 hour:
  Pkts sent: 1200; Lost: 32 (2.6%); Corrupt: 0 (0%);
  Misordered: 129 (10.8%); Duplicate: 0 (0%)
  Min: 0.60%, occurred at 16:43:29 on Tue 01 Jul 2008 UTC
  Max: 5.12%, occurred at 17:15:34 on Tue 01 Jul 2008 UTC
  Mean: 2.02%; StdDev: 0.58%; Overall: 2.00%

Bins:

<table>
<thead>
<tr>
<th>Range</th>
<th>Count</th>
<th>Cum. Count</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5%</td>
<td>5 (83%)</td>
<td>5 (83%)</td>
<td>1.8%</td>
</tr>
<tr>
<td>5 to 10%</td>
<td>1 (17%)</td>
<td>6 (100%)</td>
<td>5.12%</td>
</tr>
<tr>
<td>10 to 15%</td>
<td>0 (0%)</td>
<td>6 (100%)</td>
<td></td>
</tr>
<tr>
<td>&gt; 15%</td>
<td>0 (0%)</td>
<td>6 (100%)</td>
<td></td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets size, on page 144</td>
<td>Configures the size of the buckets in which statistics are collected.</td>
</tr>
</tbody>
</table>
show ethernet udld interfaces

To display the ethernet interfaces configured with unidirectional link detection protocol, use the `show ethernet udld interfaces` in the ethernet interface configuration mode.

```
show ethernet udld interfaces {brief}
```

**Syntax Description**

- `brief` Displays a brief summary of the ethernet udld interfaces.

**Command Default**

No parameters displays the current state for all udld interfaces.

**Command Modes**

Ethernet Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output of the `show ethernet udld interfaces` command:

```
RP/0/RSP0/CPU0:router# show ethernet udld interfaces

Device ID: 00:0c:cc:cc:01:02
Device name: harpenden2.cisco.com
GigabitEthernet0/1/0/2
 Port state: Up
 Main FSM state: Advertisement
 Detection FSM state: Bidirectional
 Message interval: 60 seconds
 Timeout interval: 5 seconds
Neighbor 1
 Device ID: 00:0a:0b:0c:cc:cc
 Device name: cambridge53.cisco.com
 Port ID: Gi0/12
 Message interval: 7 seconds
 Timeout interval: 4 seconds
 Echo 1: 00:0c:cc:cc:01:02, Gi0/1/0/2
 Echo 2: 00:0a:0b:0c:dd:dd, GE100
Neighbor 2
 Device ID: 00:0a:0b:0c:dd:dd
 Device name: cambridge54.cisco.com
 Port ID: GE100
 Message interval: 7 seconds
```
This example shows a sample output of the `show ethernet udld interfaces` command with the `brief` keyword:

```
RP/0/RSP0/CPU0:router# show ethernet udld interfaces brief

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Neighbor Device</th>
<th>N'bor port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1/0/1</td>
<td>Bidirectional</td>
<td>london-xr22.cisco.com</td>
<td>Gi3/12/0/24</td>
</tr>
<tr>
<td>Gi0/1/0/2</td>
<td>Bidirectional</td>
<td>[2 neighbors]</td>
<td>-</td>
</tr>
<tr>
<td>Gi0/1/0/3</td>
<td>Unknown</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gi0/1/0/4</td>
<td>Unidirectional</td>
<td>sj-ios25.cisco.com</td>
<td>Gi3/5</td>
</tr>
<tr>
<td>Te0/12/0/10</td>
<td>Admin Down</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Te0/12/0/11</td>
<td>N’bor Mismatch</td>
<td>long-device.cisco.com</td>
<td>LongPortNam&gt;&gt;</td>
</tr>
</tbody>
</table>
```

**Table 22: show ethernet udld interfaces Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Down</td>
<td>Indicates that the port is administratively down (shutdown configuration is in effect).</td>
</tr>
<tr>
<td>Error Disabled</td>
<td>Specifies that the port is in Error Disabled state for a non-UDLD reason, or the port has been disabled by UDLD but the daemon has restarted and does not have a record of the cause.</td>
</tr>
<tr>
<td>Down</td>
<td>Indicates that the port is operationally down but not Error Disabled.</td>
</tr>
<tr>
<td>Initializing</td>
<td>Indicates that the port is not yet operating the UDLD protocol.</td>
</tr>
<tr>
<td>Detecting</td>
<td>Indicates that the port is in the detection phase and is synchronizing the data with its peers.</td>
</tr>
<tr>
<td>Loopback</td>
<td>Specifies that the port has been detected to be in loopback.</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>Indicates that the port was unidirectional and was disabled by UDLD.</td>
</tr>
<tr>
<td>N’bor Mismatch</td>
<td>Indicates that the port has been disabled by UDLD due to mismatched neighbors.</td>
</tr>
<tr>
<td>No Neighbors</td>
<td>Specified that the port does not have an active UDLD session with any of the neighbors.</td>
</tr>
<tr>
<td>Bidirectional</td>
<td>Indicates that the port is up and has been detected to be bidirectional.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Specifies the ID advertised by the device to its peers. This is a MAC address.</td>
</tr>
<tr>
<td>Device name</td>
<td>Specifies the string identifier for the device sent to peers. This is a concatenation of the hostname with the configured IP domain (if present), separated by a dot.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet udld statistics</code>, on page 342</td>
<td>Displays statistics on state machine transitions and packets sent and received for an UDLD interface.</td>
</tr>
</tbody>
</table>
show ethernet udld statistics

To display the statistics of state machine transitions and packets exchanged on an interface running UDLD protocol, use the `show ethernet udld statistics` command in the ethernet interface configuration mode.

```
show ethernet udld statistics[interface  type  |unaccounted-drops ]
```

**Syntax Description**

- `interface type` *(Optional)* Displays information about the specified interface type. If an interface is specified, only the interface-specific counters are shown and not the node counters.
- `unaccounted-drops` *(Optional)* Displays information for only the node counters.

**Command Default**

No default behavior or values

**Command Modes**

Ethernet Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output of the `show ethernet udld statistics` command:

```
RP/0/RSP0/CP00:router# show ethernet udld statistics interface GigabitEthernet 0/10/0/11

Interface GigabitEthernet0/10/0/11
Counters last cleared: 01:12:11 ago
Main FSM transitions (to each state)
  Link up: 1
  Detection: 12
  Advertize: 12
  Port shutdown: 0
  UDLD inactive: 0
Detection FSM transitions (to each state)
  Unknown: 12
  Bidirectional: 12
  Unidirectional: 0
  Neighbor mismatch: 0
  Loopback: 0
Rx packet counts
  Probe: 1
  Echo: 1819
  Flush: 5
  Invalid packets (dropped): 154
```
Tx packet counts
    Probe: 1
    Echo: 1824
    Flush: 0
    Unable to send (dropped): 0

Node 0/10/CPU0
    Counters last cleared: 01:12:11 ago
    Received on ports without UDLD configured
        Total packet count: 12
        Last port: Gi0/10/0/5
    Rx port could not be determined: 0
sla operation

To create an operation instance from a maintenance end point (MEP) to a specified destination, use the `sla operation` command in interface CFM MEP configuration mode. To remove the operation, use the `no` form of this command.

```
sla operation profile profile-name target {mep-id id | mac-address mac-address}
```

**Syntax Description**
- **profile profile-name**: Name of the profile to assign this operation.
- **target mep-id id**: Destination MEP ID. The range is 1 to 8191.

**Command Default**
No operations are configured

**Command Modes**
Interface CFM MEP configuration (config-if-cfm-mep)

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `sla operation` command is supported on all Ethernet interfaces.

Multiple SLA operation instances may be configured under each MEP, and may have different targets, and may be assigned to different profiles.

If an operation is assigned to a nonexistent profile, a warning message is issued, and the offending configuration is shown in the output of the related show commands.

Changing the configuration of an SLA operation is equivalent to deleting the operation and creating a new operation. All stored data for the operation is discarded.

When `target mep-id` is specified, the operation is activated only if that MEP is in the peer MEP database. You can verify that a MEP is in the database, using the `show ethernet cfm peer meps` command.

**Examples**
The following example shows how to create an SLA operation instance using a profile named “Profile_1” to a destination MEP with the specified MAC address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ethernet cfm
RP/0/RSP0/CPU0:router(config-if-cfm)# mep domain Dml service Sv1 mep-id 1
```
RP/0/RSP0/CPU0:router(config-if-cfm-mep)# sla operation profile Profile_1 target mac-address 01:23:45:67:89:ab

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm peer meps, on page 292</td>
<td>Displays information about maintenance end points (MEPs) for peer MEPs.</td>
</tr>
</tbody>
</table>
**snmp-server traps ethernet cfm**

To enable SNMP traps for Ethernet Connectivity Fault Management (CFM), use the `snmp-server traps ethernet cfm` command in Global Configuration mode.

### Syntax Description

This command has no keywords or arguments.

### Command Default

Ethernet OAM event traps are not enabled.

### Command Modes

Global Configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# snmp-server traps ethernet cfm
```
**snmp-server traps ethernet oam events**

To enable SNMP traps for Ethernet OAM events, use the `snmp-server traps ethernet oam events` command in Global Configuration mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Ethernet OAM event traps are not enabled.

**Command Modes**
Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server traps ethernet oam events
```
statistics measure

To enable the collection of Ethernet Service Level Agreement (SLA) statistics, and enter the SLA profile statistics configuration mode, use the `statistics measure` command in SLA profile configuration mode. To disable statistics collection, use the `no` form of this command.

```
statistics measure {one-way-delay-ds | one-way-delay-sd | one-way-jitter-ds | one-way-jitter-sd |
round-trip-delay | round-trip-jitter | one-way-loss-sd | one-way-loss-ds}
no statistics measure {one-way-delay-ds | one-way-delay-sd | one-way-jitter-ds | one-way-jitter-sd |
round-trip-delay | round-trip-jitter | one-way-loss-sd | one-way-loss-ds}
```

### Syntax Description

- **one-way-delay-ds** (CFM delay measurement profile type only) Enables the collection of statistics that measure delay in one direction, from destination to source.
- **one-way-delay-sd** (CFM delay measurement profile type only) Enables the collection of statistics that measure delay in one direction, from source to destination.
- **one-way-jitter-ds** (CFM delay measurement profile type only) Enables the collection of statistics that measure delay variance in one direction, from destination to source.
- **one-way-jitter-sd** (CFM delay measurement profile type only) Enables the collection of statistics that measure delay variance in one direction, from source to destination.
- **round-trip-delay** (CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the delay in the round trip of a packet.
- **round-trip-jitter** (CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the amount of delay variance in the round trip of a packet.
- **one-way-loss-sd** (CFM loss measurement profile type only) Enables the collection of statistics that measure the synthetic loss in one direction, from source to destination.
- **one-way-loss-ds** (CFM loss measurement profile type only) Enables the collection of statistics that measure the synthetic loss in one direction, from destination to source.

### Command Default

No statistics are collected

### Command Modes

SLA profile configuration (config-sla-prof)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Release 4.0.0  These keyword options were added:

- one-way-delay-ds
- one-way-delay-sd
- one-way-jitter-ds
- one-way-jitter-sd
Release | Modification
--- | ---
Release 4.3.0 | • one-way-loss-sd
 | one-way-loss-ds

These keyword options were added:

Usage Guidelines

For statistics to be collected, at least one statistics entry must be present in each profile. To measure more than one type of statistic, this command may be configured more than once in a single profile.

The one-way delay and jitter statistics are available for CFM delay measurement profile types only (profile (SLA) command with the type cfm-delay-measurement keywords).

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

This example shows how to enable the collection of round-trip-delay statistics, and enter the SLA profile statistics configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla)# profile Prof1 type cfm-loopback
RP/0/RSP0/CPU0:router(config-sla-prof)# statistics measure round-trip-delay
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet sla, on page 190</td>
<td>Enters the Ethernet SLA configuration mode.</td>
</tr>
<tr>
<td>profile (SLA), on page 258</td>
<td>Creates an SLA operation profile and enter the SLA profile configuration mode.</td>
</tr>
</tbody>
</table>
**status-counter**

To set the Metro Ethernet Forum (MEF) N393 Status Counter value that is used to determine Ethernet Local Management Interface (E-LMI) operational status, use the `status-counter` command in interface Ethernet LMI configuration mode. To return to the default, use the `no` form of the command.

```
status-counter  threshold
```

**Syntax Description**

| `threshold` | Number from 2 to 10. The default is 4. |

**Command Default**

The N393 Status Counter is set to 4.

**Command Modes**

Interface Ethernet LMI configuration (config-if-elmi)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the E-LMI protocol status is currently Up, the Status Counter specifies how many consecutive times the PVT must expire before the status is changed to Down. If the E-LMI status is currently Down, the Status Counter specifies how many STATUS ENQUIRY messages must be received without the PVT expiring before the status is changed to Up. If the PVT is disabled, the status counter has no effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to set the MEF Status Counter for E-LMI to 6:

```
RP/0/RSP0/CP00:router# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CP00:router(config-if)# ethernet lmi
RP/0/RSP0/CP00:router(config-if-elmi)# status-counter 6
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface (Ethernet), on page 72</code></td>
<td>Specifies or creates an Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>ethernet lmi, on page 185</code></td>
<td>Enables E-LMI operation on an interface and enters interface Ethernet LMI configuration mode.</td>
</tr>
<tr>
<td><code>show ethernet lmi interfaces, on page 306</code></td>
<td>Displays E-LMI information for an interface, including protocol status and error and event statistics.</td>
</tr>
</tbody>
</table>
symbol-period threshold

To configure the thresholds that trigger an Ethernet OAM symbol-period error event, use the `symbol-period threshold` command in Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the `no` form of this command.

```
symbol-period threshold low threshold [high threshold]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>low threshold</td>
<td>Low threshold value, in symbols, that triggers a symbol-period error event. The range is 0 to 60000000.</td>
</tr>
<tr>
<td>high threshold</td>
<td>(Optional) High threshold value, in symbols, that triggers a symbol-period error event. The range is 0 to 60000000. The high threshold value can be configured only in conjunction with the low threshold value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The default low threshold is 1 symbol.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet OAM link monitor configuration (config-eoam-lm)</td>
<td></td>
</tr>
<tr>
<td>Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>Allowed high threshold without low threshold.</td>
</tr>
<tr>
<td></td>
<td>Added choice of units.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>When the low threshold is passed, a symbol-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task ID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example shows how to configure the symbol-period low and high thresholds that trigger a symbol-period error event:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-eoam)# link-monitor</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-eoam-lm)# symbol-period threshold low 100 high 6000</td>
<td></td>
</tr>
</tbody>
</table>
symbol-period window

To configure the window size for an Ethernet OAM symbol-period error event, use the `symbol-period window` command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the `no` form of this command.

```
symbol-period window window
```

**Syntax Description**
window Size of the window for symbol-period error in milliseconds. The range is 1000 to 60000.

**Command Default**
The default value is 1000 milliseconds.

**Command Modes**
- Ethernet OAM link monitor configuration (config-eoam-lm)
- Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

**Command History**
Release 3.9.0  This command was introduced.

**Usage Guidelines**
The IEEE 802.3 standard defines the window size as a number of symbols rather than a time duration. These two formats can be converted either way by using a knowledge of the interface speed and encoding.

**Task ID**
- ethernet-services read, write

**Examples**
The following example shows how to configure the window size for a symbol-period error.

```
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# link-monitor
RP/0/RSP0/CPU0:router(config-eoam-lm)# symbol-period window 60000
```
**synthetic loss calculation packets**

To configure the number of packets that must be used to calculate each Frame Loss Ratio (FLR) calculation, use the `synthetic loss calculation packets` command in the Ethernet SLA profile probe configuration mode.

```
synthetic loss calculation packets number
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>number</code></th>
<th>Specifies the number of packets that must be used to calculate each FLR. The range is 10 – 1209600.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The value must be a divisor of the number of packets per probe. If bursts are configured, the value must be a multiple of the number of packets per burst.</td>
</tr>
</tbody>
</table>

**Command Default**

The default value is the number of packets in the probe, that is each probe results in a single FLR calculation.

**Command Modes**

SLA profile probe configuration (config-sla-prof-pb)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `synthetic loss calculation packets` command can only be configured for packet types that support synthetic loss measurement.

**Note**

An FLR value is calculated for each discrete block of packets. For instance, if a value of 10 is configured, then the first FLR value is calculated based on packets 0 to 9, the second FLR value is calculated based on packets 10 to 19, and so on.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure the number of packets to be used to calculate FLR using the `synthetic loss calculation packets` command:

```
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# configure
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# ethernet sla
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# profile Prof1 type cfm-synthetic-loss-measurement
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# probe
RP/0/RSP0/CPU0:router(config-sla-prof-pb)# synthetic loss calculation packets 1250
```
tags

To set the number of outer tags in CFM packets sent from up MEPs in a CFM domain service, use the `tags` command in CFM domain service configuration mode. To return the number of tags in CFM packets to the default value, use the `no` form of this command.

```
tag number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the number of tags in CFM packets from up MEPs. Currently, the only valid value is 2.</td>
</tr>
</tbody>
</table>

**Command Default**

When not configured, CFM packets are sent with the same number of tags as customer data traffic, according to the encapsulation and rewrite configuration.

**Command Modes**

CFM domain service configuration (config-cfm-dmn-svc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows you to set the number of tags in CFM packets from up MEPs to 1, so that the system can differentiate between CFM packets and data packets. When not configured, CFM packets from UP MEPs have the same number of tags as data packets, and consequently, may not be forwarded to the appropriate route.

Tags can be configured only for services that are associated with a bridge domain or cross-connect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the number of tags in CFM packets from up MEPs in a CFM domain service:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain D1 level 1
RP/0/RSP0/CPU0:router(config-cfm-dmn)# service S2 bridge group BG1 bridge-domain BD2
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# tags 1
```
traceroute cache

To set the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries, use the `traceroute cache` command in CFM configuration mode. To return the traceroute cache to its default limits, use the `no` form of this command.

```
traceroute cache hold-time minutes size entries
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hold-time minutes</strong></td>
<td>Timeout value in minutes that entries are held in the Ethernet CFM traceroute cache table before being cleared. Range is 1 minute or greater.</td>
</tr>
<tr>
<td><strong>size entries</strong></td>
<td>Maximum number of entries that are stored in the Ethernet CFM traceroute cache table. An entry is a single traceroute reply. Range is 1 to 5000.</td>
</tr>
</tbody>
</table>

**Command Default**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hold-time</strong></td>
<td>100</td>
</tr>
<tr>
<td><strong>size</strong></td>
<td>100</td>
</tr>
</tbody>
</table>

**Command Modes**

CFM configuration (config-cfm)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A separate cache is managed for each node that sends a traceroute request. All replies to a single traceroute request are cached at once. The `hold-time` begins when the last reply to a request is received. When the `hold-time` limit is reached, all replies to that request are cleared. The size of each traceroute reply is limited by the MTU of the interface.

When the maximum number of entries (`size entries`) is exceeded, all replies for the oldest request are deleted.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the `hold-time` and the `size` of a traceroute cache.

```
RP/0/RSP0/CPU0# configure
RP/0/RSP0/CPU0(config)# ethernet cfm
RP/0/RSP0/CPU0(config-cfm)# traceroute cache hold-time 1 size 3000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm (global), on page 182</td>
<td>Enters CFM configuration mode.</td>
</tr>
<tr>
<td>traceroute ethernet cfm, on page 356</td>
<td>Sends Ethernet CFM traceroute messages to generate a basic.</td>
</tr>
</tbody>
</table>
**traceroute ethernet cfm**

To send Ethernet connectivity fault management (CFM) traceroute messages to generate a basic, targeted, or exploratory traceroute, use the `traceroute ethernet cfm` command in EXEC mode.

```
traceroute ethernet cfm domain domain-name service service-name [mac-address target-mac-address | mep-id target-mep-id] | explore [all-ports] [from from-mac-address]] source [mep-id source-mep-id] interface type interface-path-id [asynchronous] [timeout seconds] [filtering-db-only] [cos cos-no] [ttl ttl] [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain domain-name</td>
<td>String of a maximum of 80 characters that identifies the domain in which the destination MEP resides. (Basic traceroute)</td>
</tr>
<tr>
<td>service service-name</td>
<td>String of a maximum of 80 characters that identifies the maintenance association to which the destination MEP belongs. (Basic traceroute)</td>
</tr>
<tr>
<td>mac-address target-mac-address</td>
<td>Identifies the 6-byte MAC address (in hexadecimal H.H.H format) of the destination MEP. (Targeted traceroute)</td>
</tr>
<tr>
<td>mep-id target-mepid</td>
<td>Destination maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191. (Targeted traceroute)</td>
</tr>
<tr>
<td>explore</td>
<td>(Optional) Specifies that an exploratory traceroute is performed.</td>
</tr>
<tr>
<td>all-ports</td>
<td>(Optional) Specifies an exploratory traceroute of all ports.</td>
</tr>
<tr>
<td>from from-mac-address</td>
<td>(Optional) Specifies an exploratory traceroute beginning at the specified MAC address (in hexadecimal H.H.H format).</td>
</tr>
<tr>
<td>source</td>
<td>Specifies source information for the traceroute.</td>
</tr>
<tr>
<td>mep-id source-mep-id</td>
<td>(Optional) Source maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.</td>
</tr>
<tr>
<td>interface type</td>
<td>Source interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>asynchronous</td>
<td>(Optional) Specifies that the traceroute is performed asynchronously, where control is returned to the command prompt immediately, and no results are displayed. The results can be displayed later using the <code>show ethernet cfm traceroute-cache</code> command.</td>
</tr>
</tbody>
</table>

*Note* Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.
### Ethernet OAM Commands

**traceroute ethernet cfm**

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Command Modes</th>
<th>Command History</th>
<th>Usage Guidelines</th>
<th>Task ID</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>timeout</strong> seconds</td>
<td>(Optional) Timeout value (in seconds) for the specified interface. For a basic traceroute, the timeout is a fixed value that defaults to 5 seconds. For an exploratory traceroute, a logarithmic algorithm is used unless this value is specified.</td>
<td>EXEC mode</td>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
<td>interface</td>
<td>The following example shows how generate a basic traceroute:</td>
</tr>
<tr>
<td><strong>filtering-db-only</strong></td>
<td>(Optional) Sets whether or not the remote maintenance points should base their responses on the filtering database only. The default is no—use both the filtering and MIP-CCM databases.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>RP/0/RSP0/CP0# traceroute ethernet cfm domain bar service bar mep-id 1 source interface gigabitethernet 0/0/0/0</strong></td>
</tr>
<tr>
<td><strong>cos cos-no</strong></td>
<td>(Optional) Identifies the class of traffic of the source MEP by setting a Class of Service (CoS) value. The valid values are from 0 to 7.</td>
<td></td>
<td></td>
<td>uko-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ttl ttl</strong></td>
<td>Specifies the initial time-to-live (TTL) value (from 1 to 255) for the traceroute message. The default is 64.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Specifies that details are displayed in the output for the traceroute.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402, TTL 64, Trans ID 2:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Hostname/Last Ingress MAC/name</th>
<th>Egress MAC/Name</th>
<th>Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ios 0000-0001.0203.0400</td>
<td>0001.0203.0400 [Down]</td>
<td>FDB</td>
</tr>
<tr>
<td>2</td>
<td>abc ios</td>
<td>0001.0203.0401 [Ok]</td>
<td>FDB</td>
</tr>
<tr>
<td>3</td>
<td>bcd abc</td>
<td>0001.0203.0402 [Ok]</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Replies dropped: 0

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>traceroute cache</code>, on page 355</td>
<td>Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries.</td>
</tr>
<tr>
<td><code>clear ethernet cfm traceroute-cache</code>, on page 153</td>
<td>Removes the contents of the traceroute cache.</td>
</tr>
<tr>
<td><code>show ethernet cfm traceroute-cache</code>, on page 300</td>
<td>Displays the contents of the traceroute cache.</td>
</tr>
</tbody>
</table>
uni-directional link-fault detection

To enable detection of a local, unidirectional link fault and send notification of that fault to an Ethernet OAM peer, use the `uni-directional link-fault detection` command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode.

`uni-directional link-fault detection [disable]`

**Syntax Description**

`disable` (Optional, Interface Ethernet OAM configuration only) Overrides the setting of unidirectional link fault detection from an Ethernet OAM profile, and disables it for this interface only.

**Command Default**

Detection and sending notification of local, unidirectional link faults is disabled.

**Command Modes**

- Ethernet OAM configuration (config-eoam)
- Interface Ethernet OAM configuration (config-if-eoam)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 6.1.2</td>
<td>Removed restriction disallowing <code>disable</code> keyword in Ethernet OAM configuration mode.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command does not affect how the receipt of link-fault messages are handled by the router. Actions to be taken for the receipt of link-fault messages are configured using the `action uni-directional link-fault` command.

Consider the following guidelines when configuring the `uni-directional link-fault detection` command:

- You can configure unidirectional link-fault detection for multiple interfaces that share a similar configuration using the command within an Ethernet OAM profile and attaching the profile to the interfaces to which it applies.
- You can override the profile configuration for unidirectional link-fault detection using the command in interface Ethernet OAM configuration.
- The `disable` keyword is only available in interface Ethernet OAM configuration mode, and it allows you to override the feature set by the profile, and disable it for a particular interface. For example, if unidirectional link-fault detection is enabled within a profile that is attached to an interface, you can override that configuration to disable it at the interface using the `uni-directional link-fault detection disable` command in interface Ethernet OAM configuration mode.
- You can use the `no` form of the command in either the profile or interface configuration:
  - Running the `no` form of the command within the profile removes the configuration of the uni-directional command in the profile, effectively disabling the feature for all interfaces.
  - Running the `no` form of the command within interface Ethernet OAM configuration removes the override setting of the command at the interface and uses the profile setting.

- The `show ethernet oam configuration` command output will show either Y or N and (Overridden) depending on whether the interface is driving the configuration of the feature, or the profile is driving it. “Overridden” means that the configuration is being applied by the interface.
The following example shows how to enable detection of a local, unidirectional link fault and send notification of that fault to an Ethernet OAM peer within an Ethernet OAM profile that can be attached to multiple interfaces:

```sh
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ethernet oam profile Profile_1
RP/0/RSP0/CPU0:router(config-eoam)# uni-directional link-fault detection
```

The same profile can be applied to multiple interfaces. The following example shows how to attach the Ethernet OAM profile to an interface:

```sh
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# profile Profile_1
RP/0/RSP0/CPU0:router(config-if-eoam)# commit
```

Consider that you have decided that you do not want unidirectional link-fault detection enabled at this particular interface, but you do want to keep the other attached profile settings. The following example shows how to disable link-fault detection at this interface only:

```sh
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet oam
RP/0/RSP0/CPU0:router(config-if-eoam)# uni-directional link-fault detection disable
RP/0/RSP0/CPU0:router(config-if-eoam)# commit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action uni-directional link-fault, on page 133</td>
<td>Configures what action is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer.</td>
</tr>
<tr>
<td>ethernet oam profile, on page 189</td>
<td>Creates an EOAM profile and enters EOAM configuration mode.</td>
</tr>
<tr>
<td>ethernet oam, on page 186</td>
<td>Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.</td>
</tr>
<tr>
<td>profile (EOAM), on page 257</td>
<td>Attaches an Ethernet OAM profile to an interface.</td>
</tr>
</tbody>
</table>
Frame Relay Commands

This module provides CLI commands for configuring Frame Relay services on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- clear frame-relay multilink interface, on page 362
- clear frame-relay lmi interface, on page 364
- encap (PVC), on page 365
- encapsulation frame-relay, on page 366
- frame-relay intf-type, on page 368
- frame-relay lmi disable, on page 369
- frame-relay lmi-n391dte, on page 370
- frame-relay lmi-n392dce, on page 371
- frame-relay lmi-n392dte, on page 372
- frame-relay lmi-n393dce, on page 373
- frame-relay lmi-n393dte, on page 374
- frame-relay lmi-t391dte, on page 375
- frame-relay lmi-t392dce, on page 376
- frame-relay lmi-type, on page 377
- frame-relay multilink ack, on page 378
- frame-relay multilink bandwidth-class, on page 380
- frame-relay multilink bid, on page 382
- frame-relay multilink hello, on page 384
- frame-relay multilink lid, on page 386
- frame-relay multilink retry, on page 388
- pvc (frame relay), on page 390
- show frame-relay lmi, on page 391
- show frame-relay lmi-info, on page 393
- show frame-relay multilink, on page 396
- show frame-relay pvc, on page 409
- show frame-relay vcm-info interface, on page 412
- show interfaces (frame relay), on page 414
- snmp-server traps frame-relay pvc, on page 418
clear frame-relay multilink interface

To clear the multilink frame-relay (MFR) statistics for the given interface or location, use the `clear frame-relay multilink interface` command in EXEC mode.

`clear frame-relay multilink interface {type interface-path-id | all [location node-id]}`

**Syntax Description**

- **type**
  Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**
  Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **all**
  Clears MFR statistics for all interfaces

- **location node-id**
  (Optional) Clears MFR statistics for all interfaces at the location specified by `node-id`. The `node-id` argument is entered in the `rack/slot/module` notation.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

- **Release**
  - **Modification**
  - Release 4.0.0  This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**
  - **Operations**
  - fr  execute

**Examples**

The following example shows how to use the `clear frame-relay multilink interface` command to clear the multilink frame-relay protocol and internal statistics on an interface:

```
RP/0/RSP0/CPU0:router# clear frame-relay multilink interface serial 0/1/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show frame-relay lmi-info, on page 393</code></td>
<td>Displays Frame Relay information for the LMI.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show interfaces multilink, on page 599</code></td>
<td>Displays information about a multilink interface.</td>
</tr>
</tbody>
</table>
clear frame-relay lmi interface

To clear the LMI statistics for the given interface or location, use the **clear frame-relay lmi** command in EXEC mode.

**clear frame-relay lmi interface** \{type interface-path-id | all [location node id]\}

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>type</th>
<th>Interface type. For more information, use the question mark (?) online help function.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>Note</td>
<td>use the <strong>show interfaces</strong> command to see a list of all interfaces currently configured on the router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about the syntax for the router, use the question mark (?) online help function.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all</td>
<td>Clears LMI statistics for all interfaces</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Clears LMI statistics for all interfaces at the location specified by node-id. The node-id argument is entered in the rack/slot/module notation.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to use the **clear frame-relay lmi** command to clear the LMI counters on an interface:

```
RP/0/RSP0/CP00:router# clear frame-relay lmi interface pos 0/1/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show frame-relay lmi, on page 391</td>
<td>Displays Frame Relay statistics for the LMI.</td>
</tr>
</tbody>
</table>
encap (PVC)

To change the encapsulation for a Frame Relay permanent virtual circuit (PVC), use the `encap` command in Frame Relay PVC configuration mode. To restore default encapsulation from the Frame Relay main interface, use the `no` form of this command.

```
encap {cisco | ietf}
```

**Syntax Description**
- `cisco` (Optional) Uses Cisco encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.
- `ietf` (Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment that belongs to a vendor other than Cisco across a Frame Relay network.

**Command Default**
The default encapsulation keyword is Cisco. When this command is not configured, encapsulation is inherited from the Frame Relay main interface.

**Command Modes**
Frame Relay PVC configuration (config-fr-vc)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set encapsulation on PVC data-link connection identifier (DLCI) 16 for Packet-over-SONET/SDH (POS) subinterface 0/4/0/1.1:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/4/0/1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# pvc 16
RP/0/RSP0/CPU0:router(config-fr-vc)# encap ietf
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>encapsulation frame-relay</code>, on page 366</td>
<td>Enables Frame Relay encapsulation.</td>
</tr>
</tbody>
</table>
 encapsulation frame-relay

To enable Frame Relay encapsulation, use the `encapsulation frame-relay` command in interface configuration mode. To disable Frame Relay encapsulation, use the `no` form of this command.

```
encapsulation frame-relay [ietf]
```

**Syntax Description**

- **ietf** (Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to equipment from another vendor across a Frame Relay network.

**Command Default**

The default encapsulation method is Cisco.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `encapsulation frame-relay` command to connect an interface to a Frame Relay network. When this command is configured, outgoing packets are encapsulated with a Frame Relay header and Frame Relay headers are removed from incoming packets to the interface.

A Cisco or IETF encapsulation method controls the Network Layer Protocol Identifier (NLPID) that is added to outgoing packets on the interface. The encapsulation method enabled for an outgoing packet can be changed for each data-link connection identifier (DLCI) per subinterface by using the `encap (PVC)` command in Frame Relay PVC configuration mode.

When the `encapsulation frame-relay` command is configured, LMI is enabled by default. To disable LMI use the `frame-relay lmi disable` command.

The following restrictions apply to the `encapsulation frame-relay` command upon configuration or removal of the command on an interface:

- When configuring this command, Layer 3 and Layer 2 configurations are not allowed on the interface.
- Before removing this command, all Frame Relay subinterfaces and LMI configuration should be deleted from the interface.

The `encapsulation frame-relay` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows Frame Relay encapsulation configured on Packet-over-SONET/SDH (POS) 0/3/0/1:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation frame-relay ietf
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>encap (PVC), on page 365</code></td>
<td>Changes the encapsulation for a Frame Relay PVC.</td>
</tr>
<tr>
<td><code>frame-relay lmi disable, on page 369</code></td>
<td>Disables the Frame Relay LMI.</td>
</tr>
</tbody>
</table>
frame-relay intf-type

To configure the interface type of the User-Network Interface (UNI), use the **frame-relay intf-type** command in interface configuration mode. To change the configuration, use the **no** form of this command.

```
frame-relay intf-type {dce | dte | nni}
```

**Syntax Description**

- **dce**: Router functions as a switch connected to a router.
- **dte**: Router is connected to a Frame Relay network.
- **nni**: Router is connected to a NNI signaling interface.

**Command Default**

DTE

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.1</td>
<td>The <strong>nni</strong> keyword was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **frame-relay intf-type** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a DCE switch type on the interface:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dce
```
frame-relay lmi disable

To disable the Frame Relay Local Management Interface (LMI), use the `frame-relay lmi disable` command in interface configuration mode. To reenable LMI, use the `no` form of this command.

**frame-relay lmi disable**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

LMI is enabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `frame-relay lmi disable` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

- **Task ID**: fr
- **Operations**: read, write

**Examples**

The following example shows how to configure a DCE switch type on the interface:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi disable
```
frame-relay lmi-n391dte

To set the full status polling interval, use the `frame-relay lmi-n391dte` command in interface configuration mode. To restore the default interval value, use the `no` form of this command.

```
frame-relay lmi-n391dte polling-cycles
```

### Syntax Description

- **polling-cycles**
  
  Number of Line Integrity Verification (LIV) exchanges performed before requesting a full status message. Range is from 1 to 255. The default is 6.

### Command Default

The full status polling interval is 6.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `frame-relay lmi-n391dte` command to set the full status message polling interval. This command is relevant only when the interface type is data terminal equipment (DTE).

Two message types are supported: status inquiry and status. Status inquiry messages are sent from DTE to DCE. Status messages are sent from DCE to DTE (in response to a status inquiry). The Status (Full) and LIV report types are contained within these messages, and typically there is one status transaction for every five LIV transactions.

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows that one out of every four status inquiries generated requests a full status response from the DCE on the interface:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-n391dte 4
```
frame-relay lmi-n392dce

To set the error threshold on a DCE interface, use the `frame-relay lmi-n392dce` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-n392dce  threshold
```

**Syntax Description**

- `threshold`  Error threshold value. Range is from 1 to 10. Default is 3.

**Command Default**

The DCE error threshold is 3.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N392 errors must occur within the number defined by the N393 event count for the link to be declared down. Therefore, the threshold value for this command must be less than the count value defined in the `frame-relay lmi-n393dce` command.

The `frame-relay lmi-n392dce` command is relevant only when the interface type is data communication equipment (DCE).

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DCE switch:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-n392dce 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>frame-relay lmi-n393dce</code>, on page 373</td>
<td>Sets the DCE monitored events count.</td>
</tr>
</tbody>
</table>
frame-relay lmi-n392dte

To set the error threshold on a DTE interface, use the `frame-relay lmi-n392dte` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-n392dte threshold
```

**Syntax Description**

- `threshold` Error threshold value. Range is from 1 to 10. The default is 3.

**Command Default**

The DTE error threshold is 3.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `frame-relay lmi-n392dte` command is relevant only when the interface type is data terminal equipment (DTE).

This command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Examples**

The following example shows how to set the Local Management Interface (LMI) failure threshold to 4. The router acts as a Frame Relay DTE switch.

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-n392dte 4
```
frame-relay lmi-n393dce

To set the DCE monitored events count, use the `frame-relay lmi-n393dce` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-n393dce  events
```

**Syntax Description**

- `events` Monitored events count. Range is from 1 to 10. The default is 4.

**Command Default**

The number of DCE monitored events is 4.

**Command Modes**

- Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `frame-relay lmi-n393dce` command is used along with the `frame-relay lmi-n392dce` command to define the condition that causes the link to be declared down.

N392 errors must occur within the `events` argument count in order for the link to be declared down. Therefore, the `events` value defined in this command must be greater than the threshold value defined in the `frame-relay lmi-n392 dce` command.

The `frame-relay lmi-n393dce` command is relevant only when the interface type is data communication equipment (DCE).

This `frame-relay lmi-n393dce` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-n393dce 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>frame-relay lmi-n392dce</code>, on page 371</td>
<td>Sets the error threshold on a DCE interface.</td>
</tr>
</tbody>
</table>
frame-relay lmi-n393dte

To set the monitored event count on a DTE interface, use the `frame-relay lmi-n393dte` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-n393dte events
```

### Syntax Description

- `events` Monitored events count. Range is from 1 to 10. The default is 4.

### Command Default

The number of DTE monitored events is 4.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `frame-relay lmi-n393dte` command is relevant only when the interface type is data terminal equipment (DTE).

This `frame-relay lmi-n393dte` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set the Local Management Interface (LMI) monitored events count to 5.

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-n393dte 5
```
**frame-relay lmi-t391dte**

To set the Local Management Interface (LMI) polling interval, use the **frame-relay lmi-t391dte** command in interface configuration mode. To restore the default interval value, use the **no** form of this command.

```
frame-relay lmi-t391dte seconds
```

**Syntax Description**

`seconds`  Polling interval between each status inquiry from the DTE end, in seconds. Range is from 5 to 30. The default is 10.

**Command Default**

The LMI polling interval is 10 seconds.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This **frame-relay lmi-t391dte** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

The `seconds` value defined in this command must be less than the polling verification timer defined in the **frame-relay lmi-t392 dce** command.

The **frame-relay lmi-t391dte** command is relevant only when the interface type is data terminal equipment (DCE).

**Examples**

The following example shows how to set the LMI polling timer interval to 15 seconds:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dte
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-t391dte 15
```
frame-relay lmi-t392dce

To set the Local Management Interface (LMI) polling verification timer on the DCE, use the `frame-relay lmi-t392dce` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-t392dce seconds
```

**Syntax Description**

- `seconds`  Polling verification timer, in seconds. The range is from 5 to 30. The default is 15.

**Command Default**

The LMI polling verification timer is 15 seconds.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `frame-relay lmi-t392dce` command is used along with the `frame-relay lmi-t391dte` command to define the condition that causes the link to be declared down.

The `seconds` value defined in this command must be greater than the polling verification timer defined in the `frame-relay lmi-t391 dte` command.

This `frame-relay lmi-n392dce` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the Local Management Interface (LMI) polling timer interval to 30 seconds:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay intf-type dce
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-t392dce 30
```
frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the `frame-relay lmi-type` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay lmi-type [{ansi | cisco | q933a}]
```

**Syntax Description**

ansi (Optional) Uses LMI as defined by ANSI T1.617a-1994 Annex D.

cisco (Optional) Uses LMI as defined by Cisco (not standard).

q933a (Optional) Uses LMI as defined by ITU-T Q.933 (02/2003) Annex A.

**Command Default**
The default is cisco.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If the DTE is not explicitly configured or the `no` form is not used after explicit configuration, then the DTE automatically senses the LMI type of the DCE and use that type of LMI.

This `frame-relay lmi-type` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set the Local Management Interface (LMI) type to Q.933, Annex A:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# frame-relay lmi-type q933a
```
frame-relay multilink ack

To configure the MFR acknowledge timeout value for a Frame Relay multilink bundle link, use the frame-relay multilink ack command in interface configuration mode. To revert to the default settings, use the no form of this command.

```
frame-relay multilink ack ack-timeout
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ack-timeout</td>
<td>Ack timeout value, in seconds. The range is from 1 to 10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The default MFR acknowledge timeout value is 4 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

The `frame-relay multilink ack` command is supported only on serial interfaces. The `frame-relay multilink ack` command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The `frame-relay multilink ack` command can be configured only on bundle link interfaces that have been associated with a bundle using the `encapsulation frame-relay mfr` command.

**Note**

You can enter the `frame-relay multilink ack` command at any time without affecting the current state of the interface; however, the configured timeout value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the `shutdown` and `no shutdown` commands in interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the MFR acknowledge timeout value as 2 seconds for the serial interface 0/3/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/1/0
```
frame-relay multilink ack 2

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation frame-relay, on page 366</td>
<td>Enables Frame Relay encapsulation.</td>
</tr>
<tr>
<td>frame-relay multilink bid, on page 382</td>
<td>Assigns a BID name to a multilink Frame Relay bundle.</td>
</tr>
<tr>
<td>show frame-relay lmi-info, on page 393</td>
<td>Displays frame relay information for the LMI.</td>
</tr>
<tr>
<td>shutdown (interface)</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>
To configure the bandwidth class for a Frame Relay multilink bundle interface, use the `frame-relay multilink bid bandwidth-class` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay multilink bandwidth-class \{a | b | c \} threshold
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Configures bandwidth class A. When one or more member links are up, the bundle interface is up. When all the member links are down, the bundle interface is down.</td>
</tr>
<tr>
<td>b</td>
<td>Configures bandwidth class B. When all the member links are up, the bundle interface is up. When any member link is down, the bundle interface is down.</td>
</tr>
<tr>
<td>c</td>
<td>Configures bandwidth class C. The bundle link <code>threshold</code> must be configured.</td>
</tr>
</tbody>
</table>

`threshold` Minimum number of links that must be up for the bundle interface to be up. The range is 1 to 255.

### Command Default

The default is a (Bandwidth Class A).

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Bandwidth class is configurable only under Frame Relay Forum 16.1 (FRF 16.1).

#### Note

The `frame-relay multilink bandwidth-class` command is supported only on multilink frame relay interfaces. The `frame-relay multilink bandwidth-class` command is not supported on Packet-over-SONET/SDH (POS) or serial interfaces.

### Task ID

- **Task ID**
  - `fr` read, write

### Examples

The following example shows how to set a multilink frame relay interface to bandwidth Class C with a threshold of 3:

```
RP/0/RSP0/CPU0:router(config)# interface Multilink 0/3/1/0/100
RP/0/RSP0/CPU0:router(config-if)# frame-relay multilink bandwidth-class c 3
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show frame-relay lmi-info, on page 393</td>
<td>Displays Frame Relay information for the LMI.</td>
</tr>
</tbody>
</table>
To create a name for a Frame Relay multilink bundle interface, use the `frame-relay multilink bid` command in interface configuration mode. To restore the default setting, use the `no` form of this command.

```
frame-relay multilink bid bundle-id-name
```

**Syntax Description**

- `bundle-id-name`: Name for the Frame Relay multilink bundle. The bundle identifier (bid) name identifies the bundle interface at both endpoints. The bid name is exchanged in the information elements to ensure consistent link assignments. The bid name can be up to 50 characters including the null termination character. The bid name is configured at the bundle interface level and is applied to each member link.

**Command Default**

By default, the interface name, for example, Multilink 0/4/1/0/1, is used as the bundle identifier.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The `frame-relay multilink bid` command is supported only on multilink frame relay interfaces. The `frame-relay multilink bid` command is not supported on Packet-over-SONET/SDH (POS) or serial interfaces.

- Regardless of whether you create a bundle identifier name using the `frame-relay multilink bid` command or whether the system uses the default name for the interface, each bundle should have a unique name.

**Examples**

The following example shows how to create a Frame Relay multilink interface bundle identifier name:

```
RP/0/RSP0/CPU0:router(config)# interface Multilink 0/3/1/0/100
RP/0/RSP0/CPU0:router(config-if)# frame-relay multilink bid MFRBundle
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show frame-relay lmi-info</code>, on page 393</td>
<td>Displays Frame Relay information for the LMI.</td>
</tr>
</tbody>
</table>
frame-relay multilink hello

To configure the hello interval used by a Frame Relay multilink bundle link, use the `frame-relay multilink hello` command in interface configuration mode. To reset the name to the default, use the `no` form of this command.

```
frame-relay multilink hello hello-interval
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hello-interval</code></td>
<td>Hello interval for the Frame Relay multilink bundle link, in seconds. The range is from 1 to 180.</td>
</tr>
</tbody>
</table>

**Command Default**

The default hello interval is 10 seconds.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note**
  The `frame-relay multilink hello` command is supported only on serial interfaces. The `frame-relay multilink hello` command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

- **Note**
  The `frame-relay multilink hello` command can be configured only on bundle link interfaces that have been associated with a bundle using the `encapsulation frame-relay mfr` command.

- **Note**
  You can enter the `frame-relay multilink hello` command at any time without affecting the current state of the interface; however, the configured hello interval value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the `shutdown` and `no shutdown` commands in interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the hello interval value as 10 seconds for the serial interface 0/3/1/0:

```
RP/0/RSP0/CP00:router(config)# interface serial 0/3/1/0
```
### Frame Relay Commands

**frame-relay multilink hello**

```bash
RP/0/RSP0/CP00:router(config-if)# frame-relay multilink hello 10
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>encapsulation frame-relay, on page 366</td>
<td>Enables Frame Relay encapsulation.</td>
</tr>
<tr>
<td></td>
<td>frame-relay multilink bid, on page 382</td>
<td>Assigns a BID name to a multilink Frame Relay bundle.</td>
</tr>
<tr>
<td></td>
<td>show frame-relay lmi-info, on page 393</td>
<td>Displays frame relay information for the LMI.</td>
</tr>
<tr>
<td></td>
<td>shutdown (interface)</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>
frame-relay multilink lid

To create a name for a Frame Relay multilink bundle link, use the `frame-relay multilink lid` command in interface configuration mode. To reset the name to the default, use the `no` form of this command.

```
frame-relay multilink lid link-id name
```

**Syntax Description**

- `link-id` Specifies the name for the Frame Relay multilink bundle link. The link identifier (lid) name can be up to 49 characters long.
- `name` The name of the physical interface, for example, Serial 0/3/0/1/2:0, is used as the lid.

**Command Default**

The name of the physical interface, for example, Serial 0/3/0/1/2:0, is used as the lid.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

The `frame-relay multilink lid` command is supported only on serial interfaces. The `frame-relay multilink lid` command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces.

The `frame-relay multilink lid` command can be configured only on bundle link interfaces that have been associated with a bundle using the `encapsulation frame-relay mfr` command.

**Note**

You can enter the `frame-relay multilink lid` command at any time without affecting the current state of the interface; however, the link identifier name does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the `shutdown` and `no shutdown` commands in interface configuration mode.

The lid name is used to identify the bundle link to peer devices and to enable the devices to identify which bundle links are associated with which bundles. The lid name can also be assigned when the bundle link is created using the `encapsulation frame-relay mfr` command with the `name` argument. If a lid name is not assigned, the default lid is the name of the physical interface.

The local and peer lid names do not have to be unique. However, regardless of whether you create a lid name using the `frame-relay multilink lid` command or the systems uses the default name for the bundle link, each link within a bundle must have a unique name. If the same name is used by different links in the same bundle, the bundles will flap indefinitely.
Task ID | Task ID | Operations
-------|--------|----------
fr     | fr     | read,    
       |        | write    

Examples

The following example shows how to configure the lid name as 'BL1' for the serial interface 0/3/1/0:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/1/0
RP/0/RSP0/CPU0:router(config-if)# frame-relay multilink lid BL1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation frame-relay, on page 366</td>
<td>Enables Frame Relay encapsulation.</td>
</tr>
<tr>
<td>frame-relay multilink bid, on page 382</td>
<td>Assigns a BID name to a multilink Frame Relay bundle.</td>
</tr>
<tr>
<td>show frame-relay lmi-info, on page 393</td>
<td>Displays frame relay information for the LMI.</td>
</tr>
<tr>
<td>shutdown (interface)</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>
frame-relay multilink retry

To configure the retry count for retransmissions for a Frame Relay multilink bundle link, use the `frame-relay multilink retry` command in interface configuration mode. To reset the name to the default, use the `no` form of this command.

```
frame-relay multilink retry retry-count
```

**Syntax Description**

- `retry-count`  
  Retry count for retransmissions. The range is from 1 to 5.

**Command Default**

The default retry count for retransmissions is 2.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

The `frame-relay multilink retry` command is supported only on serial interfaces. The `frame-relay multilink retry` command is not supported on Packet-over-SONET/SDH (POS) or multilink frame relay interfaces. The `frame-relay multilink retry` command can be configured only on bundle link interfaces that have been associated with a bundle using the `encapsulation frame-relay mfr` command.

**Note**

You can enter the `frame-relay multilink retry` command at any time without affecting the current state of the interface; however, the configured retry count value does not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the `shutdown` and `no shutdown` commands in interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the retry count for retransmissions as 2 on the serial interface 0/3/1/0:

```
RP/0/RSP0/CPU0:router# interface serial 0/3/1/0
```
frame-relay multilink retry 2

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>encapsulation frame-relay, on page 366</td>
<td>Enables Frame Relay encapsulation.</td>
</tr>
<tr>
<td></td>
<td>frame-relay multilink bid, on page 382</td>
<td>Assigns a BID name to a multilink Frame Relay bundle.</td>
</tr>
<tr>
<td></td>
<td>show frame-relay lmi-info, on page 393</td>
<td>Displays frame relay information for the LMI.</td>
</tr>
<tr>
<td></td>
<td>shutdown (interface)</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>
pvc (frame relay)

To associate a data-link connection identifier (DLCI) number to a permanent virtual circuit (PVC), and to enter Frame Relay PVC configuration mode, use the `pvc` command in subinterface configuration mode. To delete the PVC, use the `no` form of this command.

```
pvc dlci-number
```

**Syntax Description**

- `dlci-number`: DLCI number used to identify the PVC. The range is from 16 to 1007.

**Command Default**

No PVC is defined.

**Command Modes**

Subinterface configuration (config-subif)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Commands available in Frame Relay PVC configuration mode are:

```
commit           Commit the configuration changes to running
describe         Describe a command without taking real actions
do               Run an exec command
encap            Set the Encapsulation of this PVC
exit             Exit from this submode
no               Negate a command or set its defaults
show             Show contents of configuration
```

The `pvc` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Examples**

The following example shows how to create a PVC with DLCI 16:

```
RP/0/RSP0/CPU0:router (config) # interface pos 0/4/0/0.1 l2transport
RP/0/RSP0/CPU0:router (config-subif) # pvc 16
RP/0/RSP0/CPU0:router (config-fr-vc) #
```
show frame-relay lmi

To display Frame Relay statistics for the Local Management Interface (LMI), use the `show frame-relay lmi` command in EXEC mode.

```
show frame-relay lmi [{interface type interface-path-id | location node-id}]
```

**Syntax Description**

- `interface` (Optional) Interface for which information is to be displayed. Use the `interface-path-id` argument to specify the interface.
- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` (Optional) Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- `location node-id` (Optional) Displays information about all interfaces on the specified node. The `node-id` argument is entered in the `rack/slot/module` notation.

**Command Default**

Frame Relay LMI statistics are displayed for all interfaces enabled for LMI.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show frame-relay lmi` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status enquiry and status message between DCE and DTE.

**Task ID**

- `fr` read

**Examples**

The following example shows the output from the `show frame-relay lmi` command:

```
RP/0/RSP0/CPU0::router# show frame-relay lmi
LMI Statistics for interface POS0/1/0/0/ (Frame Relay DCE) LMI TYPE = ANSI
Invalid Unnumbered Info 0  Invalid Prot Disc 0
```
show frame-relay lmi

Table 23: show frame-relay lmi Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMI Statistics</td>
<td>Signaling or LMI specification: CISCO, ANSI, or CCITT.</td>
</tr>
<tr>
<td>Note</td>
<td>CCITT is LMI as defined by ITU-T Q.933 (02/2003) Annex A.</td>
</tr>
<tr>
<td>Invalid Unnumbered Info</td>
<td>Number of received LMI messages with invalid unnumbered information field.</td>
</tr>
<tr>
<td>Invalid Dummy Call</td>
<td>Number of received LMI messages with invalid dummy calls.</td>
</tr>
<tr>
<td>Invalid Status Message</td>
<td>Number of received LMI messages with invalid status message.</td>
</tr>
<tr>
<td>Invalid Information ID</td>
<td>Number of received LMI messages with invalid information identifier.</td>
</tr>
<tr>
<td>Invalid Report Request</td>
<td>Number of received LMI messages with invalid report request.</td>
</tr>
<tr>
<td>Num Status Enq. Rcvd</td>
<td>Number of LMI status enquiry messages received.</td>
</tr>
<tr>
<td>Num Link Timeouts</td>
<td>Number of link timeouts.</td>
</tr>
<tr>
<td>Invalid Prot Disc</td>
<td>Number of received LMI messages with invalid protocol discriminator.</td>
</tr>
<tr>
<td>Invalid Msg Type</td>
<td>Number of received LMI messages with invalid message type.</td>
</tr>
<tr>
<td>Invalid Lock Shift</td>
<td>Number of received LMI messages with invalid lock shift type.</td>
</tr>
<tr>
<td>Invalid Report IE Len</td>
<td>Number of received LMI messages with invalid report IE Length.</td>
</tr>
<tr>
<td>Invalid Keep IE Len</td>
<td>Number of received LMI messages with invalid report IE Length.</td>
</tr>
<tr>
<td>Num Status Msgs Sent</td>
<td>Number of LMI status enquiry messages sent.</td>
</tr>
<tr>
<td>Num St Enq. Timeouts</td>
<td>Number of times the status enquiry message was not received within the T392 DCE timer value.</td>
</tr>
</tbody>
</table>
show frame-relay lmi-info

To display Frame Relay information for the Local Management Interface (LMI), use the **show frame-relay lmi-info** command in EXEC mode.

```
show frame-relay lmi-info [[interface type interface-path-id | location node-id] | [detail]]
```

**Syntax Description**

- **interface** (Optional) Displays information on the the interface specified by the **type interface-path-id** argument.
- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.
  - **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
  - For more information about the syntax for the router, use the question mark (?) online help function.
- **location node-id** (Optional) Displays information about all interfaces on the specified node. The **node-id** argument is entered in the rack/slot/module notation.
- **detail** (Optional) Displays managed deli list.

**Command Default**
Displays LMI information for all Frame Relay interfaces enabled for LMI.

**Command Modes**
EXEC mode

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **show frame-relay lmi-info** command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status enquiry and status message between DCE and DTE.

**Task ID**

- **Task ID**
- **Operations**
  - fr read

**Examples**
The following example shows sample output for the **show frame-relay lmi-info** command:

```
RP/0/RSP0/CPU0:router# show frame-relay lmi-info
LMI IDB Info for interface Multilink0/3/0/0/2
```
show frame-relay lmi-info

Table 24: show frame-relay lmi-info Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTE</td>
<td>Local Management Interface polling interval</td>
</tr>
<tr>
<td>N391</td>
<td>Full status polling interval</td>
</tr>
<tr>
<td>N392</td>
<td>Error threshold value</td>
</tr>
<tr>
<td>N393</td>
<td>DTE monitored events count</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>T392</td>
<td>Local Management Interface polling verification timer</td>
</tr>
<tr>
<td>N392</td>
<td>Error threshold value</td>
</tr>
<tr>
<td>N08</td>
<td>DCE monitored events count</td>
</tr>
</tbody>
</table>
show frame-relay multilink

To display the multilink Frame-Relay (MFR) information about the given interface along with MFR protocol and internal statistics, use the **show frame-relay multilink interface** command in EXEC mode.

```
show frame-relay multilink [{detail [location node id] | interface type interface-path-id [{detail | verbose}] | location node id | verbose [location node id]}]
```

**Syntax Description**

- **detail**: (Optional) Displays Interface Descriptor Block (IDB) information and Feasible Successor Metrics (FSM) statistics.
- **location node-id**: (Optional) Displays information about all interfaces on the specified node. The node-id argument is entered in the rack/slot/module notation.
- **interface**: (Optional) Interface for which you want to display information.
- **type**: Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id**: Physical interface or virtual interface.
  
  **Note**: Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **verbose**: (Optional) Displays IDB information, FSM statistics and internal statistics.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**: fr
- **Operations**: read

**Examples**

The following example shows how to display the multilink Frame-Relay information for all interfaces:

```
RP/0/RSP0/CPU0:router# show frame-relay multilink

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
```
Member Links: 2 active, 0 inactive
State = Up, BW Class = A

Member Links:
Serial0/3/0/0/1/2:0, HW state = Up, link state = Up
Serial0/3/0/0/1/1:0, HW state = Up, link state = Up

Bundle interface: Multilink0/3/0/0/2, ifhandle 0x06032280
Member Links: 2 active, 0 inactive
State = Up, BW Class = A

Member Links:
Serial0/3/0/0/1/4:0, HW state = Up, link state = Up
Serial0/3/0/0/1/3:0, HW state = Up, link state = Up

Member interface: Serial0/3/0/0/1/1:0, ifhandle 0x060323c0
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0

Member interface: Serial0/3/0/0/1/2:0, ifhandle 0x06032380
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0

Member interface: Serial0/3/0/0/1/3:0, ifhandle 0x06032340
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280

Member interface: Serial0/3/0/0/1/4:0, ifhandle 0x06032300
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280

The following example shows how to display detailed multilink Frame-Relay information for all interfaces, including IDB information and FSM statistics:

RP/0/RSP0/CPU0:router# show frame-relay multilink detail

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
Member Links: 2 active, 0 inactive
State = Up, BW Class = A
nodeid: 0x838
group: 1
my_bid: Multilink0/3/0/0/1
peer_bid: Multilink0/6/0/0/1
magic: 0x696d8a95
flags: 0x0
im_state: 3 [Up]
sfm_req_state: 3 [Up]
is_owned_resource: Y
is_zombie: N
active_mbr_count: 2
cfg_bid:
bw_class: 1
bw_class_threshold: 0

------------- Member Links -------------
for Cisco ASR 9000 Series Routers

Frame Relay Commands

show frame-relay multilink

Serial0/3/0/0/1/2:0,   HW state = Up, link state = Up
my_lid:   Serial0/3/0/0/1/2:0
peer_lid: Serial0/6/0/0/1/2:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:09 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 3 Add Link Rx: 2
Add Link Ack Tx: 2 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 6235 Hello Rx: 6236
Hello Ack Tx: 6236 Hello Ack Rx: 6235
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 6236 Ack Timer expiry: 1

Serial0/3/0/0/1/1:0,   HW state = Up, link state = Up
my_lid:   Serial0/3/0/0/1/1:0
peer_lid: Serial0/6/0/0/1/1:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:01 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 3 Add Link Rx: 2
Add Link Ack Tx: 2 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 6234 Hello Rx: 6237
Hello Ack Tx: 6237 Hello Ack Rx: 6234

--------- Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers ---------
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 6235 Ack Timer expiry: 1

Bundle interface: Multilink0/3/0/0/2, ifhandle 0x06032280
Member Links: 2 active, 0 inactive
State = Up, BW Class = A
nodeid: 0x838
group: 2
my_bid: Multilink0/3/0/0/2
peer_bid: Multilink0/6/0/0/2
magic: 0x303c008f
flags: 0x0
im_state: 3 [Up]
fsm_req_state: 3 [Up]
is_owned_resource: Y
is_zombie: N
active_mbr_count: 2
cfg_bid:
bw_class: 1
bw_class_threshold: 0

-------------- Member Links --------------
Serial0/3/0/0/1/4:0, HW state = Up, link state = Up
my_lid: Serial0/3/0/0/1/4:0
peer_lid: Serial0/6/0/0/1/4:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:00 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

-------------- Member Link Statistics --------------
Add Link Tx: 3 Add Link Rx: 2
Add Link Ack Tx: 2 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 6236 Hello Rx: 6235
Hello Ack Tx: 6235 Hello Ack Rx: 6236
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 6237 Ack Timer expiry: 1

Serial0/3/0/0/1/3:0, HW state = Up, link state = Up
my_lid: Serial0/3/0/0/1/3:0
peer_lid: Serial0/6/0/0/1/3:0
show frame-relay multilink

flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:01 ago
Round trip: 00:00.000 (0 secs 999999 nsecs)
Min Round trip: 00:00.000 (0 secs 999999 nsecs)
Max Round trip: 00:00.003 (0 secs 999999 nsecs)

cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 3 Add Link Rx: 2
Add Link Ack Tx: 2 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 6236 Hello Rx: 6237
Hello Ack Tx: 6237 Hello Ack Rx: 6236
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 6237 Ack Timer expiry: 1

Member interface: Serial0/3/0/1/1:0, ifhandle 0x060323c0
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0
Local bid: Multilink0/3/0/0/1 Peer bid: Multilink0/6/0/0/1
my_lid: Serial0/3/0/1/1:0
peer_lid: Serial0/6/0/0/1/1:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:00 ago
Round trip: 00:00.000 (0 secs 999999 nsecs)
Min Round trip: 00:00.000 (0 secs 999999 nsecs)
Max Round trip: 00:00.004 (0 secs 999999 nsecs)

cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 3 Add Link Rx: 2
Add Link Ack Tx: 2 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 6235 Hello Rx: 6237
Hello Ack Tx: 6237 Hello Ack Rx: 6235
Member interface: Serial0/3/0/0/1/2:0, ifhandle 0x06032380
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/1 with ifhandle 0x060322c0
Local bid: Multilink0/3/0/0/1  Peer bid: Multilink0/6/0/0/1
  my_lid:                  Serial0/3/0/0/1/2:0
  peer_lid:                Serial0/6/0/0/1/2:0
  flags:                   0x0
  fsm_state: 3 [Up]
  im_state: 3 [Up]
  fsm_req_state: 3 [Up]
  cause:   0 [None]
  retry_count: 0
  in_loopback: No
  bc_init_rcvd: Yes
  bc_owned_res: Yes
  cc_owned_res: Yes
  is_parent_up: Yes
  Last Packet Tx: 00:00:00 ago
  Round trip: 00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
  cfg_lid:
    mfr_t_hello: 10
    mfr_t_ack: 4
    mfr_retry_max: 2

------------- Member Link Statistics -------------

Add Link Tx: 3  Add Link Rx: 2
Add Link Ack Tx: 2  Add Link Ack Rx: 1
Add Link Rej Tx: 0  Add Link Rej Rx: 0
Remove Link Tx: 0  Remove Link Rx: 0
Remove Link Ack Tx: 0  Remove Link Ack Rx: 0
Hello Tx: 6236  Hello Rx: 6237
Hello Ack Tx: 6237  Hello Ack Rx: 6236
Loopback Detected: 0  Invalid Pkts Rx: 0
Bundle Mismatch: 0  Expired Ack Rx: 0
Hello Timer expiry: 6237  Ack Timer expiry: 1

Member interface: Serial0/3/0/0/1/3:0, ifhandle 0x06032340
HW state = Up, link state = Up
Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280
Local bid: Multilink0/3/0/0/2  Peer bid: Multilink0/6/0/0/2
  my_lid:                  Serial0/3/0/0/1/3:0
  peer_lid:                Serial0/6/0/0/1/3:0
  flags:                   0x0
  fsm_state: 3 [Up]
  im_state: 3 [Up]
  fsm_req_state: 3 [Up]
  cause:   0 [None]
  retry_count: 0
  in_loopback: No
  bc_init_rcvd: Yes
  bc_owned_res: Yes
  cc_owned_res: Yes
  is_parent_up: Yes
  Last Packet Tx: 00:00:02 ago
  Round trip: 00:00.000 (0 secs 999997 nsecs)
  Min Round trip: 00:00.000 (0 secs 999997 nsecs)
  Max Round trip: 00:00.003 (0 secs 3999988 nsecs)
  cfg_lid:
    mfr_t_hello: 10

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
The following example shows how to display detailed multilink Frame Relay information for all interfaces, including IDB information and FSM statistics, on a Cisco 2-Port Channelized OC-12c/DS0 SPA:

```
RP/0/RSP0/CPU0:router# show frame-relay multilink detail
Fri Mar 25 14:04:05.425 UTC
Bundle interface: Multilink0/2/1/0/1, ifhandle 0x04002840
   Member Links: 2 active, 0 inactive
   State = Up,  BW Class = A
     nodeid: 0x829
     group: 1
     my_bid: Multilink0/2/1/0/1
```

```
Member interface: Serial0/3/0/0/1/4:0, ifhandle 0x06032300
   HW state = Up, link state = Up
   Member of bundle interface Multilink0/3/0/0/2 with ifhandle 0x06032280
   Local bid: Multilink0/3/0/0/2  Peer bid: Multilink0/6/0/0/2
   my_lid: Serial0/3/0/0/1/4:0
   peer_lid: Serial0/6/0/0/1/4:0
   flags: 0x0
   fsm_state: 3 [Up]
   im_state: 3 [Up]
   fsm_req_state: 3 [Up]
   cause: 0 [None]
   retry_count: 0
   in_loopback: No
   bc_init_rcvd: Yes
   bc_owned_res: Yes
   cc_owned_res: Yes
   is_parent_up: Yes
   Last Packet Tx: 00:00:01 ago
   Round trip: 00:00.000 (0 secs 999997 nsecs)
   Min Round trip: 00:00.000 (0 secs 999997 nsecs)
   Max Round trip: 00:00.004 (0 secs 4999985 nsecs)
   cfg_lid:
```
peer_bid: Multilink0/2/1/0/1
magic: 0x75b06726
flags: 0x0
im_state: 3 [Up]
fsm_req_state: 3 [Up]
is_owned_resource: Y
is_zombie: N
active_mbr_count: 2
cfg_bid:
bw_class: 1
bw_class_threshold: 0

--------------- Member Links ---------------
Serial0/2/1/0/1:0, HW state = Up, link state = Up
my_lid: Serial0/2/1/0/1:0
peer_lid: Serial0/2/1/0/1:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:06 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.002 (0 secs 2999991 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 2  Add Link Rx: 1
Add Link Ack Tx: 1  Add Link Ack Rx: 1
Add Link Rej Tx: 0  Add Link Rej Rx: 0
Remove Link Tx: 0  Remove Link Rx: 0
Remove Link Ack Tx: 0  Remove Link Ack Rx: 0
Hello Tx: 2  Hello Rx: 2
Hello Ack Tx: 2  Hello Ack Rx: 2
Loopback Detected: 0  Invalid Pkts Rx: 1
Bundle Mismatch: 0  Expired Ack Rx: 0
Hello Timer expiry: 2  Ack Timer expiry: 0

Serial0/2/1/0/1:1:0, HW state = Up, link state = Up
my_lid: Serial0/2/1/0/1:0
peer_lid: Serial0/2/1/0/1:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
show frame-relay multilink

Last Packet Tx: 00:00:06 ago
Round trip: 00:00:000 (0 secs 999997 nsecs)
Min Round trip: 00:00:000 (0 secs 999997 nsecs)
Max Round trip: 00:00:002 (0 secs 2999991 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 2 Add Link Rx: 1
Add Link Ack Tx: 1 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 2 Hello Rx: 2
Hello Ack Tx: 2 Hello Ack Rx: 2
Loopback Detected: 0 Invalid Pkts Rx: 1
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 2 Ack Timer expiry: 0

Bundle interface: Multilink0/2/1/0/2, ifhandle 0x04002880
Member Links: 2 active, 0 inactive
State = Up, BW Class = A
nodeid: 0x829
group: 2
my_bid: Multilink0/2/1/0/2
peer_bid: Multilink0/2/1/0/2
magic: 0x41f1f15a
flags: 0x0
im_state: 3 [Up]
fsm_req_state: 3 [Up]
is_owned_resource: Y
is_zombie: N
active_mbr_count: 2
cfg_bid:
bw_class: 1
bw_class_threshold: 0

------------------------ Member Links ------------------------
Serial0/2/1/0/1/4:0, HW state = Up, link state = Up
my_lid: Serial0/2/1/0/1/4:0
peer_lid: Serial0/2/1/0/1/4:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rowd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:06 ago
Round trip: 00:00:000 (0 secs 999997 nsecs)
Min Round trip: 00:00:000 (0 secs 999997 nsecs)
Max Round trip: 00:00:002 (0 secs 2999991 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
### Member Link Statistics

<table>
<thead>
<tr>
<th></th>
<th>Tx</th>
<th>Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Link</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Add Link Ack</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Add Link Rej</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Remove Link</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Remove Link Ack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hello</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Hello Ack</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Loopback Detected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Invalid Pkts Rx</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Bundle Mismatch</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Expired Ack Rx</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Hello Timer expiry</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

### Member Link Information

- **Serisl0/2/1/0/1/3:0**: HW state = Up, link state = Up
- **my_lid**: Serial0/2/1/0/1/3:0
- **peer_lid**: Serial0/2/1/0/1/3:0
- **flags**: 0x0
- **fsm_state**: 3 [Up]
- **im_state**: 3 [Up]
- **fsm_req_state**: 3 [Up]
- **cause**: 0 [None]
- **retry_count**: 0
- **in_loopback**: No
- **bc_init_rcvd**: Yes
- **bc_owned_res**: Yes
- **cc_owned_res**: Yes
- **is_parent_up**: Yes
- **Last Packet Tx**: 00:00:06 ago
- **Round trip**: 00:00.000 (0 secs 999997 nsecs)
- **Min Round trip**: 00:00.000 (0 secs 999997 nsecs)
- **Max Round trip**: 00:00.002 (0 secs 2999991 nsecs)

The following example shows how to display detailed multilink Frame Relay information for all interfaces, including IDB information and FSM statistics, on a Cisco 4-Port Channelized T3 SPA:

```
RP/0/RSP0/CPU0:router# show frame-relay multilink detail
```

Member interface: Serial0/0/0/0/1:0, ifhandle 0x00005180
HW state = Up, link state = Up
Member of bundle interface Multilink0/0/0/0/1 with ifhandle 0x00005280
Local bid: Multilink0/0/0/0/1  Peer bid: Multilink0/0/0/0/1
my_lid: Serial0/0/0/0/1:0
peer_lid: Serial0/0/0/0/1:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
show frame-relay multilink

```
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:06 ago
Round trip: 00:00:000 (0 secs 999997 nsecs)
Min Round trip: 00:00:000 (0 secs 999997 nsecs)
Max Round trip: 00:00:001 (0 secs 1999994 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

------------ Member Link Statistics ------------
Add Link Tx: 3 Add Link Rx: 1
Add Link Ack Tx: 1 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 21692 Hello Rx: 21690
Hello Ack Tx: 21690 Hello Ack Rx: 21692
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 21693 Ack Timer expiry: 1
```

Member interface: Serial0/0/0/0/2:0, ifhandle 0x000051c0
HW state = Up, link state = Up
Member of bundle interface Multilink0/0/0/0/1 with ifhandle 0x00005280
Local bid: Multilink0/0/0/0/1 Peer bid: Multilink0/0/0/0/1
my_lid: Serial0/0/0/0/2:0
peer_lid: Serial0/0/0/0/2:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:03 ago
Round trip: 00:00:000 (0 secs 999997 nsecs)
Min Round trip: 00:00:000 (0 secs 999997 nsecs)
Max Round trip: 00:00:001 (0 secs 1999994 nsecs)
cfg_lid:
mfr_t_hello: 10
mfr_t_ack: 4
mfr_retry_max: 2

------------ Member Link Statistics ------------
Add Link Tx: 3 Add Link Rx: 1
Add Link Ack Tx: 1 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 21688 Hello Rx: 21694
Hello Ack Tx: 21694 Hello Ack Rx: 21688
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 21689 Ack Timer expiry: 1
```
Member interface: Serial0/0/0/0/3:0, ifhandle 0x00005200
HW state = Up, link state = Up
Member of bundle interface Multilink0/0/0/0/2 with ifhandle 0x000052c0
Local bid: Multilink0/0/0/0/2 Peer bid: Multilink0/0/0/0/2
my_lid: Serial0/0/0/0/3:0
peer_lid: Serial0/0/0/0/3:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:03 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.001 (0 secs 1999994 nsecs)
cfg_lid:
  mfr_t_hello: 10
  mfr_t_ack: 4
  mfr_retry_max: 2

--------------- Member Link Statistics ---------------
Add Link Tx: 3 Add Link Rx: 1
Add Link Ack Tx: 1 Add Link Ack Rx: 1
Add Link Rej Tx: 0 Add Link Rej Rx: 0
Remove Link Tx: 0 Remove Link Rx: 0
Remove Link Ack Tx: 0 Remove Link Ack Rx: 0
Hello Tx: 21694 Hello Rx: 21689
Hello Ack Tx: 21689 Hello Ack Rx: 21694
Loopback Detected: 0 Invalid Pkts Rx: 0
Bundle Mismatch: 0 Expired Ack Rx: 0
Hello Timer expiry: 21695 Ack Timer expiry: 1

Member interface: Serial0/0/0/0/4:0, ifhandle 0x00005240
HW state = Up, link state = Up
Member of bundle interface Multilink0/0/0/0/2 with ifhandle 0x000052c0
Local bid: Multilink0/0/0/0/2 Peer bid: Multilink0/0/0/0/2
my_lid: Serial0/0/0/0/4:0
peer_lid: Serial0/0/0/0/4:0
flags: 0x0
fsm_state: 3 [Up]
im_state: 3 [Up]
fsm_req_state: 3 [Up]
cause: 0 [None]
retry_count: 0
in_loopback: No
bc_init_rcvd: Yes
bc_owned_res: Yes
cc_owned_res: Yes
is_parent_up: Yes
Last Packet Tx: 00:00:00 ago
Round trip: 00:00.000 (0 secs 999997 nsecs)
Min Round trip: 00:00.000 (0 secs 999997 nsecs)
Max Round trip: 00:00.001 (0 secs 1999994 nsecs)
cfg_lid:
  mfr_t_hello: 10
  mfr_t_ack: 4
mfr_retry_max: 2

--------------- Member Link Statistics -------------------
Add Link Tx: 3  Add Link Rx: 1
Add Link Ack Tx: 1  Add Link Ack Rx: 1
Add Link Rej Tx: 0  Add Link Rej Rx: 0
Remove Link Tx: 0  Remove Link Rx: 0
Remove Link Ack Tx: 0  Remove Link Ack Rx: 0
Hello Tx: 21691  Hello Rx: 21689
Hello Ack Tx: 21691  Hello Ack Rx: 21691
Loopback Detected: 0  Invalid Pkts Rx: 0
Bundle Mismatch: 0  Expired Ack Rx: 0
Hello Timer expiry: 21692  Ack Timer expiry: 1

Bundle interface: Multilink0/0/0/0/1, ifhandle 0x00005280
Member Links: 2 active, 0 inactive
  nodeid: 0x808
  group: 1
  my_bid: Multilink0/0/0/0/1
  peer_bid: Multilink0/0/0/0/1
  magic: 0x48bac00c
  flags: 0x0
  im_state: 3 [Up]
  fsm_req_state: 3 [Up]
  is_owned_resource: Y
  is_zombie: N
  active_mbr_count: 2
  cfg_bid: 1
  bw_class: A
  bw_class_threshold: 0

The following example shows how to display the multilink Frame-Relay information for the interface at location 0/3/0/0/1:

RP/0/RSP0/CPU0# show frame-relay multilink interface multilink 0/3/0/0/1

Bundle interface: Multilink0/3/0/0/1, ifhandle 0x060322c0
Member Links: 2 active, 0 inactive
  State = Up,  BW Class = A
  nodeid: 0x808
  group: 1
  my_bid: Multilink0/3/0/0/1
  peer_bid: Multilink0/3/0/0/1
  magic: 0x48bac00c
  flags: 0x0
  im_state: 3 [Up]
  fsm_req_state: 3 [Up]
  is_owned_resource: Y
  is_zombie: N
  active_mbr_count: 2
  cfg_bid: 1
  bw_class: A
  bw_class_threshold: 0

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface multilink, on page 591</td>
<td>Configures a multilink interface and enters multilink interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>frame-relay multilink bid, on page 382</td>
<td>Creates a name for a Frame Relay multilink bundle interface.</td>
<td></td>
</tr>
</tbody>
</table>
show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the `show frame-relay pvc` command in EXEC mode.

```
show frame-relay pvc [{interface type interface-path-id | location node-id}] [dlci-number]
```

**Syntax Description**

- **interface** (Optional) Interface for which information is to be displayed. Use the `type` and `interface-path-id` arguments to specify the interface.

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id** (Optional) Physical interface or virtual interface.

  **Note**: Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id** (Optional) Displays information about all interfaces on the specified node. The `node-id` argument is entered in the `rack/slot/module` notation.

- **dlci-number** (Optional) DLCI number used to identify the PVC. The range is from 16 to 1007.

**Command Default**

Information for all Frame Relay interfaces and PVCs is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show frame-relay pvc` command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

This command is used to check the status of PVCs on interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the output from the `show frame-relay pvc` command:

```
RP/0/RSP0/CPU0:router# show frame-relay pvc
```
PVC Statistics for interface POS0/3/2/0 (Frame Relay DCE)

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Inactive</th>
<th>Deleted</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switched</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dynamic</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

DLCI = 612, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT VE, INTERFACE = POS0/3/2/0.1

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN packets 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:00:00 last time pvc status changed 00:00:00

DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT VE, INTERFACE = POS0/3/2/0.2

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN packets 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:00:00 last time pvc status changed 00:00:00

DLCI = 614, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT VE, INTERFACE = POS0/3/2/0.3

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN packets 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:00:00 last time pvc status changed 00:00:00

DLCI = 615, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT VE, INTERFACE = POS0/3/2/0.4

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN packets 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:00:00 last time pvc status changed 00:00:00

The following example shows the output for a specific frame-relay PVC:

RP/0/RSP0/CPU0:router# show frame-relay pvc 613

DLCI = 613, DLCI USAGE = LOCAL, ENCAP = CISCO, INHERIT = TRUE, PVC STATUS = ACT VE, INTERFACE = POS0/3/2/0.2

input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN packets 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
pvc create time 00:00:00 last time pvc status changed 00:00:00

Table 25: show frame-relay pvc Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLCI</td>
<td>One of the DLCI numbers for the PVC.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
DLCI USAGE | Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.
ENCAP | Type of encapsulation.
INHERIT | Encapsulation type for the PVC is inherited from the main interface.
PVC STATUS | Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE | Specific subinterface associated with this DLCI.
input pkts | Number of packets received on this PVC.
output pkts | Number of packets sent on this PVC.
in bytes | Number of bytes received on this PVC.
out bytes | Number of bytes sent on this PVC.
dropped pkts | Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
in FECN pkts | Number of packets received with the FECN bit set.
in BECN pkts | Number of packets received with the BECN bit set.
out FECN pkts | Number of packets sent with the FECN bit set.
out BECN pkts | Number of packets sent with the BECN bit set.
in DE pkts | Number of DE packets received.
out DE pkts | Number of DE packets sent.
out bcast pkts | Number of output broadcast packets.
out bcast bytes | Number of output broadcast bytes.
pvc create time | Time at which the PVC was created.
last time pvc status changed | Time at which the PVC changed status.
shaping drops | Number of packets dropped by the traffic-shaping process.
Fragment Counters | Displays whether fragment counters are enabled or disabled on the PVC. Fragment counters are disabled by default. Use the `fragment-counter` command to enable collection of these statistics.
show frame-relay vcm-info interface

To display Virtual Circuit (VC) manager information for a given interface, use the `show frame-relay vcm-info interface` command in EXEC mode.

```
show frame-relay vcm-info interface type interface-path-id [vc dlci]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (<code>?</code> online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (```?``` online help function.

| vc | (Optional) Specifies a VC on the interface. |
| dlci | (Optional) Data-link Connection Identifier number. Range is from 0 to 1023. |

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to display Virtual Circuit (VC) manager information for the multilink interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router# show frame-relay vcm-info interface multilink 0/3/0/0/1
```

```
VCM IDB: Multilink0_3_0_0_1
-----------------------------------
IDB type: IFT_MAIN
<main specific>
  i/f term type: L3
  i/f handle: 0x06186240
  BW: 0x00000c00
  OIR insert: F
```
VC chkpt oid: 0x00000000
proto info: 500323c8 [ptr]
proto fn table: 500323d4 [ptr]
i/f type: 0x00000037 [IFT_MULTILINK]
i/f state: 0x00000003 [up]
i/f basecaps num: 0x0000004c [fr]
i/f basecaps state: 0x00000003 [up]
VCM states: 5002c708 [ptr]
in db: T
cchkpt: F
datapath info 0 [0 bytes]
partner info 50016d98 [16 bytes]
encaps type: IETF
intf type: DTE
non chkptd info 0 [0 bytes]

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface multilink, on page 591</td>
<td>Configures a multilink interface and enters multilink interface configuration mode.</td>
</tr>
<tr>
<td>frame-relay multilink bid, on page 382</td>
<td>Creates a name for a Frame Relay multilink bundle interface.</td>
</tr>
</tbody>
</table>
show interfaces (frame relay)

To display statistics about Frame Relay interfaces, use the `show interfaces` command in EXEC mode.

```
show interfaces [summary | [type interface-path-id] [ { brief | description | detail | accounting [rates] } ]] [location node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a summary of interface information by interface type.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>(Optional) Displays brief information about each interface (one line per interface).</td>
</tr>
<tr>
<td><code>description</code></td>
<td>(Optional) Displays an interface description.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed information about each interface. This is the default.</td>
</tr>
<tr>
<td><code>accounting</code></td>
<td>(Optional) Displays the number of packets of each protocol type that have been sent through the interface.</td>
</tr>
<tr>
<td><code>rates</code></td>
<td>(Optional) Displays interface accounting rates.</td>
</tr>
<tr>
<td><code>location node-id</code></td>
<td>(Optional) Displays information about all interfaces on the specified node. The <code>node-id</code> argument is entered in the rack/slot/module notation.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

Release 4.0.0  This command was introduced

**Usage Guidelines**

The `show interfaces` (Frame Relay) command is available on Packet-over-SONET/SDH (POS), serial, and multilink interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows the output from the `show interfaces` command when the interface is configured with Frame Relay encapsulation:

```
RP/0/RSP0/CPU0:router# show interfaces pos 0/1/0/0
POS0/1/0/0 is up, line protocol is up
  Hardware is Packet over SONET/SDH
  Internet address is Unknown
  MTU 4474 bytes, BW 622080 Kbit
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 32, controller loopback not set,
  LMI enq sent 0, LMI stat recv 0, LMI upd recv 0
  LMI enq recv 9463, LMI stat sent 9463, LMI upd sent 0, DCE LMI up
  LMI DLCI 0 LMI type is ANSI Annex D frame relay DCE
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    20934 packets input, 1508069 bytes, 1151 total input drops
    0 drops for unrecognized upper-level protocol
    Received 0 broadcast packets, 0 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
    1151 input errors, 1058 CRC, 0 frame, 0 overrun, 93 ignored, 0 abort
    19590 packets output, 990924 bytes, 0 total output drops
    Output 0 broadcast packets, 0 multicast packets
    0 output errors, 0 underruns, 0 applique, 0 resets
    0 output buffer failures, 0 output buffers swapped out
```

### Table 26: show interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Displays the name of the current interface. In the example, the interface name is POS0/1/0/0.</td>
</tr>
<tr>
<td>Interface state</td>
<td>Displays the state of the interface. In the example, the interface is in the administratively up state.</td>
</tr>
<tr>
<td>Line protocol state</td>
<td>Displays the state of the Layer 2 line protocol. This field may be different from the interface state if, for example, a keepalive failure has brought down the Layer 2.</td>
</tr>
<tr>
<td></td>
<td>Note The line protocol state is not the same as the protocol state displayed in the <code>show ip interfaces</code> command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).</td>
</tr>
<tr>
<td>Hardware</td>
<td>Displays the current hardware type.</td>
</tr>
<tr>
<td>Internet address is n.n.n.n/n</td>
<td>Displays the Layer 2 address (MAC address for Ethernet interfaces).</td>
</tr>
<tr>
<td></td>
<td>Note Enter the <code>mac-address</code> command to configure the hardware address.</td>
</tr>
<tr>
<td>MTU</td>
<td>Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface.</td>
</tr>
<tr>
<td></td>
<td>Note The MTU field indicates the interface MTU. Enter the <code>mtu</code> command to configure a lower MTU value at the layer 3 level.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BW</td>
<td>Displays the bandwidth of the interface in kbps.</td>
</tr>
<tr>
<td>reliability</td>
<td>Displays the proportion of packets that are not dropped and do not have errors.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The reliability is shown as a fraction of 255.</td>
</tr>
<tr>
<td>txload</td>
<td>Indicates the traffic flowing out of the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The txload is shown as a fraction of 255.</td>
</tr>
<tr>
<td>rxload</td>
<td>Indicates the traffic flowing into the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The rxload is shown as a fraction of 255.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Layer 2 encapsulation installed on the interface.</td>
</tr>
<tr>
<td>CRC</td>
<td>Indicates the length of the cyclic redundancy check (CRC), in bytes.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter the <code>pos crc</code> command to configure the CRC.</td>
</tr>
<tr>
<td>controller loopback</td>
<td>Indicates that the hardware was configured as controller loopback.</td>
</tr>
<tr>
<td>LMI enq sent</td>
<td>Number of LMI enquiry messages sent.</td>
</tr>
<tr>
<td>LMI stat recvd</td>
<td>Number of LMI status messages received.</td>
</tr>
<tr>
<td>LMI upd recvd</td>
<td>Number of LMI updated messages received.</td>
</tr>
<tr>
<td>LMI enq recvd</td>
<td>Number of LMI enquiry messages received.</td>
</tr>
<tr>
<td>LMI stat sent</td>
<td>Number of LMI status messages sent.</td>
</tr>
<tr>
<td>LMI upd sent</td>
<td>Number of LMI updated messages sent.</td>
</tr>
<tr>
<td>DCE LMI</td>
<td>Displays the state of the DCE LMI.</td>
</tr>
<tr>
<td>LMI DLCI</td>
<td>Displays the LMI DLCI identifier.</td>
</tr>
<tr>
<td>LMI type</td>
<td>Displays the LMI type.</td>
</tr>
<tr>
<td>Last clearing</td>
<td>Time at which the counters that measure cumulative statistics (such as number of bytes</td>
</tr>
<tr>
<td></td>
<td>transmitted and received) shown in this report were last reset to zero. Note that variables</td>
</tr>
<tr>
<td></td>
<td>that might affect routing for example, load and reliability) are not cleared when the</td>
</tr>
<tr>
<td></td>
<td>counters are cleared.</td>
</tr>
<tr>
<td>5 minute input rate</td>
<td>Average number of bits and packets transmitted per second in the last 5 minutes.</td>
</tr>
<tr>
<td>5 minute output rate</td>
<td>The 5-minute input and output rates should be used only as an approximation of traffic per</td>
</tr>
<tr>
<td></td>
<td>second during a given 5-minute period. These rates are exponentially weighted averages with</td>
</tr>
<tr>
<td></td>
<td>a time constant of 5 minutes. A period of four time constants must pass before the average is</td>
</tr>
<tr>
<td></td>
<td>within two percent of the instantaneous rate of a uniform stream of traffic over that period.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>packets input</td>
<td>Total number of error-free packets received by the system.</td>
</tr>
<tr>
<td>bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.</td>
</tr>
<tr>
<td>Received...broadcasts</td>
<td>Total number of broadcast or multicast packets received by the interface</td>
</tr>
<tr>
<td>runts</td>
<td>Number of packets that are discarded because they are smaller than the minimum packet size of the medium.</td>
</tr>
<tr>
<td>giants</td>
<td>Number of packets that are discarded because they exceed the maximum packet size of the medium.</td>
</tr>
<tr>
<td>input errors</td>
<td>Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.</td>
</tr>
<tr>
<td>frame</td>
<td>Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.</td>
</tr>
<tr>
<td>overrun</td>
<td>Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.</td>
</tr>
<tr>
<td>ignored</td>
<td>Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.</td>
</tr>
<tr>
<td>abort</td>
<td>Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.</td>
</tr>
<tr>
<td>carrier transitions</td>
<td>Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.</td>
</tr>
</tbody>
</table>
**snmp-server traps frame-relay pvc**

To enable Simple Network Management Protocol (SNMP) trap notifications for a Frame Relay permanent virtual circuit (PVC), use the `snmp-server traps frame-relay pvc` command in Global Configuration mode. To disable SNMP notifications for a FR PVC, use the `no` form of this command.

```
snmp-server traps frame-relay pvc [interval seconds]
```

**Syntax Description**

- **interval seconds** *(Optional) Minimum period between successive traps. The range is from 1 to 3600.*

**Command Default**

`seconds`: 30

**Command Modes**

Global Configuration mode

**Command History**

- **Release** 4.0.0  This command was introduced.

**Usage Guidelines**

Use the `snmp-server traps frame-relay pvc` command to enable trap requests for a Frame Relay PVC. This command is used with the `snmp-server host` command. Use the `snmp-server host` command to specify which host or hosts receive SNMP notifications.

See *Implementing SNMP on Cisco IOS XR Software* in *System Management Configuration Guide for Cisco ASR 9000 Series Routers* for detailed information about SNMP configuration tasks and commands.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>read, write</td>
</tr>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the router to send SNMP trap notifications for a Frame Relay PVC:

```
RP/0/RSP0/CPU0:router(config)# snmp-server host 12.25.61 traps public udp-port 5000
RP/0/RSP0/CPU0:router(config)# snmp-server community public RW
RP/0/RSP0/CPU0:router(config)# snmp-server traps frame-relay pvc interval 50
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server community</code></td>
<td>Configures the community access string to permit access to the SNMP.</td>
</tr>
</tbody>
</table>
### Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server host</code></td>
<td>Specifies the recipient of an SNMP notification operation.</td>
</tr>
</tbody>
</table>
snmp-server traps frame-relay pvc
Global Interface Commands

This module describes the global command line interface (CLI) commands for configuring interfaces on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- bandwidth (global), on page 422
- bundle wait-while, on page 423
- clear interface, on page 424
- dampening, on page 425
- interface (global), on page 427
- lacp system, on page 429
- mlacp reset priority, on page 430
- mlacp switchback, on page 431
- mlacp switchover maximize, on page 432
- mlacp switchover type, on page 433
- mtu, on page 434
- show im dampening, on page 437
- show interfaces, on page 440
- show mlacp inconsistencies, on page 454
- shutdown (global), on page 455
bandwidth (global)

To configure the bandwidth of an interface, use the `bandwidth` command in interface configuration mode.

```
banner bandwidth rate
```

**Syntax Description**

- `rate` Amount of bandwidth to be allocated on the interface, in Kilobits per second (kbps). Range is from 0 through 4294967295.

**Command Default**

The default bandwidth depends on the interface type.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To obtain the default bandwidth for a specific interface, use the `show interfaces` command after you first bring up the interface. The default interface bandwidth is displayed in the `show interfaces` command output.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>execute</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the bandwidth on a Ten Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# interface TenGigE 0/4/0
RP/0/RSP0/CPU0:router# bandwidth 4000000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown (global), on page 455</td>
<td>Disables an interface (forces an interface to be administratively down).</td>
</tr>
</tbody>
</table>
bundle wait-while

To specify the duration of the wait-while timer for a bundle, use the `bundle wait-while` command in the bundle interface configuration mode. To disable waiting, use the `no` form of the command.

```plaintext
bundle wait-while  time
```

**Syntax Description**

`time`  Wait-while time in milliseconds, range is 0-2000.

**Command Default**

2000 milliseconds

**Command Modes**

Bundle Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
<tr>
<td></td>
<td>interface</td>
</tr>
<tr>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

In the following example, the while-while time is configured for 20 seconds:

```plaintext
RP/0/RSP0/CPU0:router(config-if)bundle wait-while 20
```
clear interface

To clear interface statistics or packet counters, use the `clear interface` command in EXEC mode.

```
clear interface type interface-path-id
```

**Syntax Description**
- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.
  - **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.
  - For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- **Release 3.7.2** This command was introduced.

**Task ID**
- **Task ID** execute
- basic-services read, write

**Examples**
This example shows how to use the `clear interface` command to clear the loopback interface 2:

```
RP/0/RSP0/CPU0:router# clear interface loopback 2
```

**Related Commands**
- `shutdown (global), on page 455` Disables an interface (forces an interface to be administratively down).
dampening

To limit propagation of transient or frequently changing interface states on Interface Manager (IM) clients, turn on event dampening by using the `dampening` command in interface configuration mode. To turn dampening off, use the `no` form of this command.

```
dampening [half-life [reuse suppress max-suppress-time]]
```

**Syntax Description**

- **half-life** *(Optional)* Time (in minutes) after which a penalty is decreased. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 1 minute.

- **reuse** *(Optional)* Penalty value below which a stable interface is unsuppressed. Range is from 1 through 20000. Default value is 750.

- **suppress** *(Optional)* Limit at which an interface is suppressed when its penalty exceeds that limit. Range is from 1 through 20000, and must be greater than the reuse threshold. The default value is 2000.

- **max-suppress-time** *(Optional)* Maximum time (in minutes) that an interface can be suppressed. This value effectively acts as a ceiling that the penalty value cannot exceed. Default value is four times the half-life period.

**Command Default**

Dampening is turned off by default. When you use the `dampening` command, the following default values are enabled for any optional parameters that you do not enter:

- `half-life`: 1 minute
- `reuse`: 750
- `suppress`: 2000
- `max-suppress-time`: Four times the half-life

**Command Modes**

Interface configuration

**Command History**

- **Release 3.7.2** This command was introduced.

**Usage Guidelines**

Event dampening suppresses a constantly unstable interface until it remains stable for a period of time. Enabling dampening on an interface that already has dampening configured has the effect of resetting the penalty associated with that interface to zero. The reuse threshold must always be less than the suppress threshold.

Consider the following guidelines when configuring event dampening:

- Configuring dampening on both a subinterface and its parent is usually unnecessary because their states are almost always the same and dampening would be triggered at the same time on each interface.
- If all subinterfaces require dampening, then apply dampening to the main interface only. Applying configuration to large numbers of subinterfaces requires an abundance of memory and increases the time required to process the configuration during boot and failover.
- When dampening is enabled, an interface has a penalty value associated with it. The value starts at 0 and is increased by 1000 whenever the underlying state of the interface changes from up to down.
- The penalty value decreases exponentially while the interface state is stable. If the penalty value exceeds a configured suppress threshold, then the state of the interface is suppressed and IM will not notify upper layers of further state transitions. The suppressed state remains until the penalty value decreases past a configured reuse threshold.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable dampening with default values on an interface:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)# dampening
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show im dampening, on page 437</td>
<td>Displays the state of all interfaces on which dampening has been configured.</td>
</tr>
</tbody>
</table>
interface (global)

To configure an interface or to create or configure a virtual interface, use the `interface` command in Global Configuration mode. To delete the interface configuration, use the `no` form of this command.

```
interface type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No interfaces are configured

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `interface` command enters interface configuration mode to allow you to configure interfaces. If a virtual interface is configured, then the interface is created if it did not already exist.

The `no` form of this command applies only to virtual interfaces or to subinterfaces (that is, interfaces that have been created in global configuration mode).

Until Release 6.5.1, when you create an interface with some configurations, upon router or interface reload, interface configurations are lost. From Release 6.5.1, onwards, automatic shutdown config behavior is persistent and no shutdown configs are lost on interface or router reload.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the `interface` command is given for the card in location 0/2/0/1, and interface configuration mode is entered for that interface:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/2/0/1
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear interface, on page 424</td>
<td>Clears interface statistics or packet counters.</td>
</tr>
<tr>
<td></td>
<td>shutdown (global), on page 455</td>
<td>Disables an interface (forces an interface to be administratively down).</td>
</tr>
</tbody>
</table>
To set the default system parameters for the Link Aggregation Control Protocol (LACP) bundles, use the `lacp system` command in Global Configuration mode.

```plaintext
lacp system { mac | priority }
```

### Syntax Description
- **mac**: Unique MAC address used to identify the system in LACP negotiations.
- **priority**: Priority for this system. Lower value is higher priority. Range is from 1 to 65535.

### Command Default
- System priority is 32768. MAC address is automatically assigned from the backplane pool.

### Command Modes
- Global Configuration

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
- The parameters are the system MAC address and the priority of the system. The MAC address must be unique to the system (if it matches a partner system, LACP negotiations fail). The combination of the MAC address and the set system priority determine the priority of the LACP bundles.

### Task ID
- **Task ID**: bundle read, write

### Example
- The following example shows how to configure the MAC address on an LACP system:

  ```plaintext
  RP/0/RSP0/CPU0:router(config)#lacp system mac 000c.15c0.bd15
  ```
mlacp reset priority

To reset operational priorities of mlacp members to their configured mLACP priorities, use the `mlacp reset priority` command in EXEC mode.

```
mlacp reset priority  bundle-ether interface-path-id
```

### Syntax Description

- **bundle-ether interface-path-id**
  - Specifies a physical interface instance or a virtual interface instance.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is for aggregated ethernet interfaces only. The command cannot be used if brute-force switchover is employed.

### Task ID

- Task ID
  - bundle
  - execute

### Example

The following example shows how to use the `mlacp reset priority` command:

```
RP/0/RSP0/CPU0:router #mlacp reset priority bundle-ether 10
```
mlacp switchback

To force a switchback to the local mlacp device for a specified bundle, use the `mlacp switchback` command in the EXEC mode.

`mlacp switchback interface interface-path-id [ at | in | no prompt ]`

**Syntax Description**

- `interface interface-path-id`: Specifies a physical interface instance or a virtual interface instance.
- `at`: Schedules the operation for a future time and date.
- `in`: Schedules the operation for a specified delay.
- `no prompt`: Attempts to carry out the command without prompting.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
<tr>
<td>interface</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to schedule the operation at a specified time and date on a bundle-ether interface:

```
RP/0/RSP0/CPU0:router# mlacp switchback bundle-ether 20 at march 21 08:30:10
```
mlacp switchover maximize

To set the maximum number of links or bandwidth in the bundle, use the `mlacp switchover maximize` command in the bundle interface configuration mode.

```
mlacp switchover maximize { links | bandwidth } [threshold value]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>links</td>
<td>Compares the operational links, with respect to the total number of links.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Compares the available bandwidth, with respect to the total bandwidth.</td>
</tr>
<tr>
<td>threshold</td>
<td>Sets the threshold value to switch to the peer, if its has more links/bandwidth available.</td>
</tr>
</tbody>
</table>
| value      | -When used with the links keyword, sets the minimum number of links, below which the device switches to the peer if more links are available. Range is 1-64.  
            -When used with the bandwidth keyword, sets the minimum bandwidth (in kbps), below which the device switches to the peer if more bandwidth is available. Range is 1-4294967295. |

**Command Default**

No default behavior or value.

**Command Modes**

Bundle interface configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows switchovers to take place such that the active device is the one with most bandwidth or maximum links in the bundle.

**Example**

The following example shows how to maximize the links:

```bash
RP/0/RSP0/CPU0:router(config-if)#interface bundle-ether 10 mlacp switchover maximize links threshold 20
```
**mlacp switchover type**

To specify a non-default switchover method, use the `mlacp switchover type` command in the bundle interface configuration mode.

```
mlacp switchover type [ brute-force | revertive ]
```

**Syntax Description**

- **brute-force**  Force switchover by disabling all local member links.
- **revertive**  Revert based on configured priority values.

**Command Default**

The default switchover type is non-revertive.

**Command Modes**

Bundle interface configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **brute-force** and **revertive** options are mutually exclusive, and the value must match on the bundle on both POAs. They determine whether the dynamic priority management or brute force mechanism is used, and whether the behavior is revertive or non-revertive.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to force a switchover by disabling all local member links on an bundle-ether interface:

```
RP/0/RSP0/CPU0:router(config-if)#mlacp switchover type brute-force
```
To adjust the maximum transmission unit (MTU) value for packets on the interface, use the **mtu** command in interface configuration mode. To return the interface to the default MTU for the interface type, use the **no** form of this command.

```
mtu  bytes
```

**Syntax Description**

- **bytes**: Maximum number of bytes in a Layer 2 frame. Range is from 64 through 65535.

**Command Default**

The default MTU for each interface is as follows:

- Ethernet—1514 bytes
- POS—4474 bytes
- Tunnel—1500 bytes
- Loopback—1514 bytes
- ATM—4470 bytes

**Command Modes**

Interface configuration

**Command History**

- **Release 3.7.2**: This command was introduced.

**Usage Guidelines**

Use the **mtu** command to set a specific MTU value for an interface, or use the **no mtu** command to return the interface to the default MTU value for that interface type. The MTU value can be increased or decreased using the **mtu** command, subject to minimum and maximum MTU limits for the interface type.

If the MTU value is not configured, then each interface will have a default MTU value that is specific to the interface type. The default MTU value is generally the largest Layer 2 frame size possible for the interface type.

The default/configured MTU value on an atm interface includes the L2 header.

The MTU size consists of L2 header that includes either SNAP(8bytes)/MUX(0)/NLPID(2) header or the AAL5 SDU. The AAL5 SDU includes the L3 datagram and the optional Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) header.

The Ethernet interface is the Layer 3 datagram plus 14 bytes. For ATM main interface, the MTU is L3 datagram + 0 bytes.

For ATM L3 sub interface, mtu is as follows:

- SNAP - L3 datagram + 8 bytes
- NLPID - L3 datagram + 2 bytes
- MUX - L3 datagram + 0 bytes
- When no pvc is configured under sub interface - L3datagram + 0 bytes

You can use the **show interfaces** command to determine if the MTU value has been changed. The **show interfaces** command output displays the MTU size for each interface in the MTU (byte) field. Note that the MTU size that is displayed includes the Layer 2 header bytes used for each encapsulation type.
You can use the `show interfaces` command to determine if the MTU value has been changed. The `show interfaces` command output displays the MTU size for each interface in the MTU (byte) field. Note that the MTU size that is displayed includes the Layer 2 header bytes used for each encapsulation type.

Changing the MTU on an interface triggers a change on the protocols and encapsulations configured on that interface, although some protocol-specific configurations can override the interface MTU. For example, specifically changing the interface MTU configuration does not affect the IP MTU configuration, but may affect the resulting MTU on that node.

For the 10x10GigE CPAK (10 ports with only 8 profiles), it is not possible to support 10 different MTUs on 10 different 10GigE ports. One of the profiles needs to be reserved for the default MTU, in case you need to change the configured MTU back to the default MTU. Therefore on the 10x10g CPAK, you can configure different MTU sizes on 7 ports and the other 3 ports have the default MTU size. If you configure the 8th port, the configuration command succeeds but an error appears on the console.

### Examples

In this example, the MTU value for all interfaces is verified. The MTU value is shown in the next-to-last column:

```
RP/0/RSP0/CPU0:router# show interfaces all brief

<table>
<thead>
<tr>
<th>Intf Name</th>
<th>State</th>
<th>LineP State</th>
<th>Encap</th>
<th>MTU</th>
<th>BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nu0</td>
<td>up</td>
<td>up</td>
<td>Null</td>
<td>1500</td>
<td>Unknown</td>
</tr>
<tr>
<td>TenGigE6/0/0/0</td>
<td>up</td>
<td>up</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>TenGigE6/0/0/1</td>
<td>up</td>
<td>up</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>TenGigE6/0/0/2</td>
<td>admin-down</td>
<td>admin-down</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>TenGigE6/0/0/3</td>
<td>admin-down</td>
<td>admin-down</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/0</td>
<td>up</td>
<td>up</td>
<td>ARPA</td>
<td>1514</td>
<td>100000</td>
</tr>
</tbody>
</table>
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 6/0/0/0
RP/0/RSP0/CPU0:router(config-if)# mtu 1000
```

After the `mtu` command is used to decrease the MTU Layer 2 frame size for the POS interface on 6/0/0/0 to 1000 bytes, the `show interfaces all brief` command is used again to verify that the MTU Layer 2 frame size has been changed:

```
RP/0/RSP0/CPU0:router# show interfaces all brief
```
### Interfaces and Encapsulation

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>State</th>
<th>Encap Type</th>
<th>MTU</th>
<th>BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nu0</td>
<td>up</td>
<td>up</td>
<td>Null</td>
<td>1500</td>
<td>Unknown</td>
</tr>
<tr>
<td>PO6/0/0</td>
<td>up</td>
<td>up</td>
<td>HDLC</td>
<td>1000</td>
<td>2488320</td>
</tr>
<tr>
<td>PO6/0/1</td>
<td>up</td>
<td>up</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>PO6/0/2</td>
<td>admin-down</td>
<td>admin-down</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>PO6/0/3</td>
<td>admin-down</td>
<td>admin-down</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/0</td>
<td>up</td>
<td>up</td>
<td>ARPA</td>
<td>1514</td>
<td>100000</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown (global), on page 455</td>
<td>Disables an interface (forces an interface to be administratively down).</td>
</tr>
</tbody>
</table>
show im dampening

To display the state of all interfaces on which dampening has been configured, use the `show im dampening` command in EXEC mode.

```
show im dampening [{interface type | ifhandle handle}]
```

**Syntax Description**
- `interface type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `ifhandle handle` (Optional) Identifies the caps node whose Interface Manager (IM) dampening information you want to display.

**Command Default**
If you do not specify an interface, then the system displays brief details about all dampened interfaces.

**Command Modes**
EXEC

**Command History**
```
Release | Modification
---------|---------------------
Release 3.7.2 | This command was introduced.
```

**Usage Guidelines**
If you do not specify an interface, then the system displays brief details about all dampened interfaces.

The physical hardware (layer 1) is not the only part of an interface that can change state. L2 keepalive failure event is one of the many instances that can have a similar impact on routing protocols despite the underlying interface state staying UP. To take account of such events, when dampening is configured on an interface, it is applied independently to every layer. They all use the same parameters as the interface but they have their own penalty value which is incremented when that layer changes state.

Capsulations that may be dampened in this way include these:

- L2 basecaps, such as HDLC and PPP, which may flap if keepalives are not received due to events such as intermittent packet loss.
- L3 encapsulations (for example ipv4, ipv6). These may be brought down if another link has a conflicting IP address configured.
- Other locations where negotiation takes place with a peer router, as in the case of PPP control protocols such as IPCP. If the negotiation fails, then the caps is brought down.

**Task ID**
```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read</td>
</tr>
</tbody>
</table>
```

**Examples**
This example shows the output from the `show im dampening` command issued with default values:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/4/0/0
RP/0/RSP0/CPU0:router(config-if)# no shutdown
RP/0/RSP0/CPU0:router(config-if)# dampening
```
This sample output shows a POS interface with PPP basecaps and IPCP. The subsequent output for `show im dampening interface <ifname>` contains a table of any capsulations which have their own penalty as shown below:

```
RP/0/RSP0/CPU0:router# show im dampening

Interface            Protocol  Capsulation   Pen  Sup
------------------------------ -------------- ----- ---
GigabitEthernet0/0/0/0                      629  NO
GigabitEthernet0/0/0/1                      2389 YES
POS0/2/0/0                               <base>   ppp  0  NO
POS0/2/0/0                               ipv4     ipcp  0  NO

RP/0/RSP0/CPU0:router# show im dampening interface TenGigaE 0/1/0/0

TenGigaE 0/1/0/0 (0x01180020)
TenGigaE/0/1/0/0 is up, line protocol is down
Dampening enabled: penalty 0, not suppressed
half_life: 1    reuse:  750
suppress: 3000  max-suppress-time: 4
restart-penalty: 0
Hardware is Ten Gigabit Ethernet
Description: ensoft-gsr5 TenGigaE 4\2
Internet address is Unknown
MTU 4474 bytes, BW 155520 Kbit
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, controller loopback not set, keepalive set (10 sec)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 total input drops
  0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 0 multicast packets
  0 runs, 0 giants, 0 throttles, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 48 packets output, 1504 bytes, 0 total output drops
Output 0 broadcast packets, 0 multicast packets
  0 output errors, 0 underruns, 0 applique, 0 resets
  0 output buffer failures, 0 output buffers swapped out
```
Dampening enabled: Penalty 1625, SUPPRESSED (42 secs remaining)
Underlying state: Down
half-life: 1 reuse: 1000
suppress: 1500 max-suppress-time: 4
restart-penalty: 0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Capsulation</th>
<th>Pen</th>
<th>Suppression</th>
<th>U-L State</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>ipv6</td>
<td>1625</td>
<td>YES</td>
<td>42s remaining</td>
</tr>
</tbody>
</table>

When dampening is configured on an interface it is also applied independently to all capsulations on that interface. For example, the ppp or hdlc basecaps state can flap even while the interface stays up and if keepalives fail. The `show im dampening interface` command contains one line for each such capsulation as well as the interface itself.

### Table 27: `show im dampening` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dampening</td>
<td>Indicates the dampening state and penalty value: not suppressed, suppressed.</td>
</tr>
<tr>
<td>underlying state</td>
<td>Underlying state of the interface: up, down, administratively down (if an interface has been configured to be “shutdown”).</td>
</tr>
<tr>
<td>half_life</td>
<td>This is the time (in minutes) at which the penalty on the interface would be half that of the original penalty (of 1000) when the interface transitions from UP to DOWN. It ranges from 1 to 45 minutes and the default is 1 minute.</td>
</tr>
<tr>
<td>reuse</td>
<td>Penalty value below which a stable interface is unsuppressed. It ranges from 1 to 20000 and the default value is 750.</td>
</tr>
<tr>
<td>suppress</td>
<td>Limit at which an unstable interface is suppressed when the penalty value exceeds the suppress value. It ranges from 1 to 20000 and the default value is 2000.</td>
</tr>
<tr>
<td>max-suppress-time</td>
<td>Maximum time (in minutes) that an interface can be suppressed. The default is 4 minutes.</td>
</tr>
<tr>
<td>restart-penalty</td>
<td>Penalty assigned to the interface when it flaps.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dampening</code>, on page 425</td>
<td>Turns on event dampening.</td>
</tr>
<tr>
<td><code>shutdown (global)</code>, on page 455</td>
<td>Disables an interface (forces an interface to be administratively down).</td>
</tr>
</tbody>
</table>
**show interfaces**

To display statistics for all interfaces configured on the router or for a specific node, use the `show interfaces` command in EXEC mode.

```
show interfaces [{type interface-path-id | all | local | location node-id}] [{accounting | brief | description | detail | summary}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Specifies the type of interface for which you want to display statistics. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(Optional) Displays interface information for all interfaces. This is the default.</td>
</tr>
<tr>
<td><strong>local</strong></td>
<td>(Optional) Displays interface information for all interfaces in the local card.</td>
</tr>
<tr>
<td><strong>location node-id</strong></td>
<td>(Optional) Displays information about all interfaces on the specified node. The <code>node-id</code> argument is entered in the <code>rack/slot/module</code> notation.</td>
</tr>
<tr>
<td><strong>accounting</strong></td>
<td>(Optional) Displays the number of packets of each protocol type that have been sent through the interface.</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>(Optional) Displays brief information of each interface (one line per interface).</td>
</tr>
</tbody>
</table>
The `show interfaces` command displays statistics for the network interfaces. The resulting display shows the interface processors in slot order.

For example, if you type the `show interfaces` command without an interface type, you receive information for all the interfaces installed in the networking device. Only by specifying the interface `type`, `slot`, and `port` arguments can you display information for a particular interface.

If you enter a `show interfaces` command for an interface type that has been removed from the networking device, an error message is displayed: “Interface not found.”

The output displayed depends on the network for which an interface has been configured.

**Note**

Ten GigE interfaces will not show egress statistics when loopback line is configured, because the loopback is done at the physical interface. But in One GigE interfaces the line loopback is done at NP that happens after packets pass through MAC. The statistics from `show interface` command from MAC will not display updates with a loopback line on Ten GigE interface.

Beginning in Cisco IOS XR Release 3.9.0, when you shut down a bundle interface, the member links are put into err-disable link interface status and admin-down line protocol state.

Beginning in Cisco IOS XR Release 4.2.0, the Bundle-POS interface type is supported.
The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average is within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.

The following example shows the output from the `show interfaces` command. The output displayed depends on the type and number of interface cards in the networking device.

```
RP/0/RSP0/CPU0:router# show interfaces tenGigE 0/0/0/1
TenGigE0/0/0/1 is administratively down, line protocol is administratively down
Hardware is TenGigE, address is 0800.4539.d909 (bia 0800.4539.d909)
Description: user defined string
Internet address is Unknown
MTU 1514 bytes, BW 10000000 Kbit
    reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
    Full-duplex, 10000Mbit/s, LR
output flow control is off, input flow control is off
loopback not set
ARP type ARPA, ARP timeout 01:00:00
Last clearing of "show interface" counters never
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
    Received 0 broadcast packets, 0 multicast packets
    0 runs, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 total output drops
    Output 0 broadcast packets, 0 multicast packets
    0 output errors, 0 underruns, 0 applique, 0 resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

The following example shows bundle member links whose link interface status is “err-disable” and line protocol state is “admin-down” after the bundle interface has been administratively shut down using the `shutdown` command:

```
RP/0/RSP0/CPU0:router# show interfaces brief
Thu May 6 06:30:55.797 DST

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>Intf</td>
<td>LineP</td>
<td>Encap</td>
<td>MTU</td>
<td>BW</td>
</tr>
<tr>
<td>Name</td>
<td>State</td>
<td>State</td>
<td>Type (byte)</td>
<td>(Kbps)</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>-------</td>
<td>--------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>BE16</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA</td>
<td>9216</td>
<td>1000000</td>
</tr>
<tr>
<td>BE16.160</td>
<td>up</td>
<td>up</td>
<td>802.1Q VLAN</td>
<td>9220</td>
<td>1000000</td>
</tr>
<tr>
<td>BE16.161</td>
<td>up</td>
<td>up</td>
<td>802.1Q VLAN</td>
<td>9220</td>
<td>1000000</td>
</tr>
<tr>
<td>BE16.162</td>
<td>up</td>
<td>up</td>
<td>802.1Q VLAN</td>
<td>9220</td>
<td>1000000</td>
</tr>
</tbody>
</table>
```
### Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers

**show interfaces**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Description</th>
<th>MTU</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE16.163</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lo0</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nu0</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tt44190</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tt44192</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tt44194</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tt44196</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mg0/RSP0/CP00/0</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Mg0/RSP0/CP00/1</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/0</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/1</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/2</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3.160</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3.161</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3.165</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3.169</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/3.215</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/4</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/5</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/6</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/7</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.185</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.187</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.189</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.210</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.211</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/7.215</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/8</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/9</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/10</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/11</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/12</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/13</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/14</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/15</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/16</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/17</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/18</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/19</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/21</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/22</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/23</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/24</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/25</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/26</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/27</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/28</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/29</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/30</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/31</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/1/0/32</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/33</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/34</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/35</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/36</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/37</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/38</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
<tr>
<td>Gi0/1/0/39</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA 1514</td>
<td>100000</td>
</tr>
</tbody>
</table>

Global Interface Commands

**show interfaces**
Table 28: show interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Displays the name of the current interface. In the example, the interface name is TenGigE0/1/0/1.</td>
</tr>
<tr>
<td>Interface state</td>
<td>Displays the state of the interface. In the example, the interface is in the administratively down state.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface state transitions</td>
<td>Displays the number of times the interface has changed the state.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• Interface state transitions command counts only if the interface stays up.</td>
</tr>
<tr>
<td></td>
<td>• Interface state transitions counts the state when the line protocol state</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>clear state-transitions</code> command to clear the counter for the</td>
</tr>
<tr>
<td></td>
<td>state from up to down/admin-down or admin-down/down to up. If an</td>
</tr>
<tr>
<td></td>
<td>interface changes the state from down to admin-down or admin-down to</td>
</tr>
<tr>
<td></td>
<td>down, the counter is not incremented.</td>
</tr>
<tr>
<td>line protocol state</td>
<td>Displays the state of the Layer 2 line protocol. This field may be</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• The line protocol state is not the same as the protocol state displayed</td>
</tr>
<tr>
<td></td>
<td>in the <code>show ip interfaces</code> command, because it is the state of Layer 2</td>
</tr>
<tr>
<td></td>
<td>(media) rather than Layer 3 (IP protocol).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Hardware</td>
<td>Displays the current hardware type.</td>
</tr>
<tr>
<td>address is n.n.n/n</td>
<td>Displays the Layer 2 address (MAC address for Ethernet interfaces).</td>
</tr>
<tr>
<td>Note</td>
<td>Enter the mac-address command to configure the hardware address.</td>
</tr>
<tr>
<td>bia</td>
<td>Displays the burned-in address (BIA) for the interface. The BIA is the default L2 (MAC) address for the interface.</td>
</tr>
<tr>
<td>Note</td>
<td>The BIA is not configurable.</td>
</tr>
<tr>
<td>description</td>
<td>Displays the user-defined string that is associated with the interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Enter the description command to configure the description associated with the interface.</td>
</tr>
<tr>
<td>Internet address</td>
<td>Displays the Layer 3 (IP) address for the interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Enter the ipv4 address command to configure the internet address for the interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface.</td>
</tr>
<tr>
<td>Note</td>
<td>The MTU field indicates the interface MTU. Enter the mtu command to configure a lower MTU value at the Layer 3 level.</td>
</tr>
<tr>
<td>BW</td>
<td>Displays the bandwidth of the interface in kbps.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reliability</td>
<td>Displays the proportion of packets that are not dropped and do not have errors.</td>
</tr>
<tr>
<td>txload</td>
<td>Indicates the traffic flowing out of the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td>rxload</td>
<td>Indicates the traffic flowing into the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Layer 2 encapsulation installed on the interface.</td>
</tr>
<tr>
<td>CRC</td>
<td>Indicates the length of the cyclic redundancy check (CRC), in bytes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>loopback or controller loopback</td>
<td>Indicates whether the hardware has been configured to be looped back.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>keepalive</td>
<td>Displays the configured keepalive value, in seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Enter the <code>keepalive</code> command to configure the value of the keepalive field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <code>keepalive</code> field may not be present if it is not applicable to the interface type.</td>
</tr>
<tr>
<td>Duplexity</td>
<td>Displays the duplexity of the link.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field is present only for shared media.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For some interface types, you can configure the duplexity by entering the <code>full-duplex</code> and <code>half-duplex</code> commands.</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed and bandwidth of the link in Mbps. This field is present only when other parts of the media info line are also displayed (see duplexity and media type).</td>
</tr>
<tr>
<td>Media Type</td>
<td>Media type of the interface.</td>
</tr>
<tr>
<td>output flow control</td>
<td>Whether output flow control is enabled on the interface.</td>
</tr>
<tr>
<td>input flow control</td>
<td>See output flow control.</td>
</tr>
<tr>
<td>ARP type</td>
<td>Address Resolution Protocol (ARP) type used on the interface. This value is not displayed on interface types that do not use ARP.</td>
</tr>
<tr>
<td>ARP timeout</td>
<td>ARP timeout in <code>hours:mins:secs</code>. This value is configurable using the <code>arp timeout</code> command.</td>
</tr>
<tr>
<td>Last clearing of counters</td>
<td>Time since the following counters were last cleared using the <code>clear counters</code> exec command in <code>hours:mins:secs</code>.</td>
</tr>
</tbody>
</table>
### 5 minute input rate

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 minute input rate</td>
<td>Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic).</td>
</tr>
</tbody>
</table>

**Note**

The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes.

**Note**

The 5-minute input should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
### show interfaces

#### Field | Description
--- | ---
5 minute output rate | Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic).

**Note**  The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes.

**Note**  The 5-minute output should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

packets input | Number of packets received on the interface that were successfully delivered to higher layers.

bytes input | Total number of bytes successfully received on the interface.

total input drops | Total number of packets that were dropped after they were received. This includes packets that were dropped due to configured quality of service (QoS) or access control list (ACL) policies. This does not include drops due to unknown Layer 3 protocol.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drops for unrecognized upper-level protocol</td>
<td>Total number of packets that could not be delivered because the necessary protocol was not configured on the interface.</td>
</tr>
<tr>
<td>Received broadcast packets</td>
<td>Total number of Layer 2 broadcast packets received on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>Received multicast packets</td>
<td>Total number of Layer 2 multicast packets received on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>runts</td>
<td>Number of received packets that were too small to be handled. This is a subset of the input errors count.</td>
</tr>
<tr>
<td>giants</td>
<td>Number of received packets that were too large to be handled. This is a subset of the input errors count.</td>
</tr>
<tr>
<td>throttles</td>
<td>Number of packets dropped due to throttling (because the input queue was full).</td>
</tr>
<tr>
<td>parity</td>
<td>Number of packets dropped because the parity check failed.</td>
</tr>
<tr>
<td>input errors</td>
<td>Total number of received packets that contain errors and hence cannot be delivered. Compare this to total input drops, which counts packets that were not delivered despite containing no errors.</td>
</tr>
<tr>
<td>CRC</td>
<td>Number of packets that failed the CRC check.</td>
</tr>
<tr>
<td>frame</td>
<td>Number of packets with bad framing bytes.</td>
</tr>
<tr>
<td>overrun</td>
<td>Number of overrun errors experienced by the interface. Overruns represent the number of times that the receiver hardware is unable to send received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ignored</td>
<td>Total number of ignored packet errors. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets.</td>
</tr>
<tr>
<td>abort</td>
<td>Total number of abort errors on the interface.</td>
</tr>
<tr>
<td>packets output</td>
<td>Number of packets received on the interface that were successfully delivered to higher layers.</td>
</tr>
<tr>
<td>bytes output</td>
<td>Total number of bytes successfully received on the interface.</td>
</tr>
<tr>
<td>total output drops</td>
<td>Number of packets that were dropped before being transmitted</td>
</tr>
<tr>
<td>Received broadcast packets</td>
<td>Number of Layer 2 broadcast packets transmitted on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>Received multicast packets</td>
<td>Total number of Layer 2 multicast packets transmitted on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>output errors</td>
<td>Number of times that the receiver hardware was unable to handle received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.</td>
</tr>
<tr>
<td>underruns</td>
<td>Number of underrun errors experienced by the interface. Underruns represent the number of times that the hardware is unable to transmit data to a hardware buffer because the output rate exceeds the transmitter’s ability to handle the data.</td>
</tr>
<tr>
<td>applique</td>
<td>Number of applique errors.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resets</td>
<td>Number of times that the hardware has been reset. The triggers and effects of this event are hardware-specific.</td>
</tr>
<tr>
<td>output buffer failures</td>
<td>Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.</td>
</tr>
<tr>
<td>output buffers swapped out</td>
<td>Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.</td>
</tr>
<tr>
<td>carrier transitions</td>
<td>Number of times the carrier detect (CD) signal of a serial interface has changed state.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controller interface</td>
<td>Displays information that is specific to the interface hardware statistics for all interfaces configured on the networking device.</td>
</tr>
</tbody>
</table>
show mlacp inconsistencies

To check and highlight inconsistencies and misconfigurations in mlacp setup, use the `show mlacp inconsistencies` command in EXEC mode.

`show mlacp inconsistencies`

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Example**
The following example shows how to view mlacp inconsistencies:

```
RP/0/RSP0/CPU0:router # show mlacp inconsistencies
```
shutdown (global)

To disable an interface (to force an interface to be administratively down), use the `shutdown` command in interface configuration mode. To enable an interface that has been shut down, use the `no` form of this command.

```
shutdow
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
The interface is enabled by default and is disabled only when shutdown is configured.

**Note**
When you add an interface to the system, or when all the configuration for an interface is lost or deleted, the interface is put in the shutdown state by the system adding the interface.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `shutdown` command to move the state of an interface to administratively down, which stops traffic flowing through the interface. This state does not stop other action from happening on the interface such as changes in configuration, protocols, capsulations, and so forth.

The `shutdown` command also marks the interface as unavailable. To check whether the state of an interface is down, use the `show interfaces` command in EXEC mode, which displays the current state of the interface. An interface that has been shut down is shown as administratively down in the display from the `show interfaces` command.

**Task ID**
Task ID | Operations
-------|-------------
interface | read, write

**Examples**
In this example, TenGigE interface 0/4/0/2 is turned off:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/4/0/2
RP/0/RSP0/CPU0:router(config-if)# shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces, on page 440</code></td>
<td>Displays statistics for all interfaces configured on the router or on a specific node.</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Displays IPv4 interface status and configuration.</td>
</tr>
</tbody>
</table>
shutdown (global)
Internal Ethernet Control Network Commands

This module provides command line interface (CLI) commands for configuring internal ethernet control on your router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- clear controller backplane ethernet location statistics, on page 458
- show controllers backplane ethernet local brief, on page 459
- show controllers backplane ethernet local clients, on page 460
- show controllers backplane ethernet local detail, on page 462
- show controllers backplane ethernet local multicast groups, on page 464
- show controllers backplane ethernet location brief, on page 466
- show controllers backplane ethernet location clients, on page 468
- show controllers backplane ethernet location detail, on page 470
- show controllers backplane ethernet location multicast groups, on page 473
clear controller backplane ethernet location statistics

To delete the aggregate statistics of traffic sent and received over the control Ethernet, use the `clear controller backplane ethernet location statistics` command in EXEC mode.

```
clear controller backplane ethernet location node-id statistics
```

**Syntax Description**
- `node-id` Identifies the node whose controller information you want to delete. The `node-id` argument is entered in the `rack/slot/module` notation.

**Command Modes**
- EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to clear all client statistics on the node at 0/1/1:

```
RP/0/RSP0/CPU0:router# clear controller backplane ethernet location 0/1/1 clients all statistics
```
show controllers backplane ethernet local brief

To display brief information about the Ethernet interface that connects the node to the router control Ethernet, use the `show controllers backplane ethernet local brief` command in EXEC mode.

```
show controllers backplane ethernet local brief
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>The <code>local</code> keyword was deprecated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows the output from the `show controllers backplane ethernet local brief` command:

```
RP/0/RSP0/CP0:router# show controllers backplane ethernet local brief

FastEthernet0_RP1_0 (local) is up, MTU 1514 bytes
   561688 packets input, 53760372 bytes
   683424 packets output, 216565877 bytes
RP/0/RSP0/CP0:router#
```

**Table 29: show controllers backplane ethernet local brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Maximum packet size, in bytes, that a particular interface can handle.</td>
</tr>
<tr>
<td>packets input</td>
<td>Total number of packets received.</td>
</tr>
<tr>
<td>packets output</td>
<td>Total number of packets transmitted.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers backplane ethernet local clients</code>, on page 460</td>
<td>Displays all multicast addresses currently being used by active interfaces on the router.</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet local detail</code>, on page 462</td>
<td></td>
</tr>
<tr>
<td><code>show controllers backplane ethernet local multicast groups</code>, on page 464</td>
<td></td>
</tr>
</tbody>
</table>
show controllers backplane ethernet local clients

To display information about local client applications, use the show controllers backplane ethernet local clients command in EXEC mode.

`show controllers backplane ethernet local clients {client-id statistics | all}`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-id statistics</td>
<td>Displays a list of client statistics for the specified client ID. Range is from 1 to 22.</td>
</tr>
<tr>
<td>all</td>
<td>Displays a list of all client applications and their IDs.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC mode

**Command History**

Release 3.7.2  This command was introduced.
Release 5.3.0  The `local` keyword was deprecated.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows the output from the show controllers backplane ethernet local clients command, which displays a list of client statistics for client ID 1:

```
RP/0/RSP0/CPU0:router# show controllers backplane ethernet local clients 1 statistics

Client QNET, ES Client Id 1, PID 20498 running on FastEthernet0_33_1
490915 packets input, 41918238 bytes
0 packets discarded (0 bytes) in garbage collection
0 (0 bytes) unicast packets filtered
0 (0 bytes) multicast packets filtered
0 (0 bytes) buffer mgmt policy discards
555660 packets output, 134265364 bytes, 0 could not be transmitted
```

**Table 30: show controllers backplane ethernet local clients Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Client application name and ID, followed by backplane client application statistics.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers backplane ethernet local brief, on page 459</td>
<td>Displays brief information about the Ethernet interface that connects the node to the router control Ethernet.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show controllers backplane ethernet local detail, on page 462</td>
<td>Displays all multicast addresses currently being used by active interfaces on the router.</td>
</tr>
<tr>
<td>show controllers backplane ethernet local multicast groups, on page 464</td>
<td></td>
</tr>
</tbody>
</table>
show controllers backplane ethernet local detail

To display detailed information for the Ethernet interface that connects the node to the router control Ethernet, use the `show controllers backplane ethernet local detail` command in EXEC mode.

```
RP/0/RSP0/CPU0:router# show controllers backplane ethernet local detail
FastEthernet0_33_1 is up
Hardware is 10/100 Ethernet, H/W address is 5246.4800.0211
Internet address is 10.0.2.17
MTU 1514 bytes
Encapsulation HFRIES (HFR Internal Ethernet Server)
Mode : Full Duplex, Rate : 100Mb/s
787486 packets input, 64535218 bytes, 0 total input drops
0 packets discarded (0 bytes) in garbage collection
3 packets discarded (582 bytes) in recv processing
Received 8 broadcast packets, 285994 multicast packets
Input errors: 0 CRC, 0 overrun, 0 alignment, 0 length, 0 collision
682244 packets output, 157245225 bytes, 0 total output drops
Output 42649 broadcast packets, 42649 multicast packets
Output errors: 0 underruns, 0 aborts, 0 loss of carrier
```

**Table 31: show controllers backplane ethernet local detail Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Provides the hardware type, followed by the hardware address.</td>
</tr>
<tr>
<td>Internet address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum packet size, in bytes, that a particular interface can handle.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation method assigned to the interface.</td>
</tr>
</tbody>
</table>
### Field Description

**Mode** Indicates the operating mode of the interface, followed by transmission data.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers backplane ethernet local brief, on page 459</td>
<td>Displays brief information about the Ethernet interface that connects the node to the router control Ethernet.</td>
</tr>
<tr>
<td>show controllers backplane ethernet local clients, on page 460</td>
<td></td>
</tr>
<tr>
<td>show controllers backplane ethernet local multicast groups, on page 464</td>
<td>Displays all multicast addresses currently being used by active interfaces on the router.</td>
</tr>
</tbody>
</table>
show controllers backplane ethernet local multicast groups

To display all multicast addresses currently being used by active interfaces on the router, use the `show controllers backplane ethernet local multicast groups` command in EXEC mode.

### Syntax Description

This command has no keywords or arguments.

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>The <code>local</code> keyword was deprecated.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Examples

The following example shows the output from the `show controllers backplane ethernet local multicast groups` command:

```
RP/0/RSP0/CPU0# show controllers backplane ethernet local multicast groups

Intf Name                     Multicast address  Client registered for this address Name
-------------------------------- --------------------------------- ----------------------------- -----------
FastEthernet0_RP1_CPU0        0100.0000.0064  2                             GSP
                               0100.0000.0065  2                             GSP
                               0100.0000.0066  2                             GSP
                               0100.0000.0068  2                             GSP
                               0100.0000.006a  2                             GSP
                               0100.0000.006c  2                             GSP
                               0100.0000.006e  2                             GSP
                               0100.0000.0070  2                             GSP
                               0100.0000.0072  2                             GSP
                               0100.0000.2774  2                             GSP
                               0100.0000.2775  2                             GSP
                               0100.0000.2776  2                             GSP
                               0100.0000.2777  2                             GSP
                               0100.0000.2778  2                             GSP
                               0100.0000.277a  2                             GSP
                               0100.0000.277c  2                             GSP
                               0100.0000.277e  2                             GSP
                               0100.0000.2780  2                             GSP
                               0100.0000.2782  2                             GSP
                               0100.0000.2784  2                             GSP
                               0100.0000.2786  2                             GSP

--More--
```
### Table 32: show controllers backplane ethernet local multicast groups Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Name</td>
<td>Identifies the interface whose multicast addresses are displayed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A multicast address is a single address that refers to multiple network devices.</td>
</tr>
<tr>
<td>Multicast address</td>
<td>Multicast addresses associated with the specified interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A multicast address is a single address that refers to multiple network devices.</td>
</tr>
<tr>
<td>ID</td>
<td>Client identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>Client application name.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers backplane ethernet local brief, on page 459</code></td>
<td>Displays brief information about the Ethernet interface that connects the node to the router control Ethernet.</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet local clients, on page 460</code></td>
<td></td>
</tr>
<tr>
<td><code>show controllers backplane ethernet local detail, on page 462</code></td>
<td></td>
</tr>
</tbody>
</table>
show controllers backplane ethernet location brief

To display brief information about backplane Ethernet interfaces in a particular location, use the `show controllers backplane ethernet location brief` command in EXEC mode.

```
show controllers backplane ethernet location node-id brief
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows the output from the `show controllers backplane ethernet location brief` command:

```
RP/0/RSP0/CPU0:router# show controllers backplane ethernet location 0/1/0 brief

FastEthernet0_0_CPU0 (local) is up, MTU 1514 bytes
57569 packets input, 5999749 bytes
36963 packets output, 4105673 bytes
RP/0/RSP0/CPU0:router#
```

*Table 33: show controllers backplane ethernet location brief Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Maximum packet size, in bytes, that a particular interface can handle.</td>
</tr>
<tr>
<td>packets input</td>
<td>Total number of packets received.</td>
</tr>
<tr>
<td>packets output</td>
<td>Total number of packets transmitted.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Input errors</td>
<td>Displays the number of errors received by the interface. Input errors occur when incoming cells are dropped or corrupted. The possible input errors are as follows:</td>
</tr>
<tr>
<td></td>
<td>• CRC—Number of times that the checksum calculated from the data received did not match the checksum from the transmitted data.</td>
</tr>
<tr>
<td></td>
<td>• overrun—Number of times that the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data.</td>
</tr>
<tr>
<td></td>
<td>• alignment—Number of nonoctets received.</td>
</tr>
<tr>
<td></td>
<td>• length—Number of times the interface prevented the ASIC from overrunning a maximum transmission unit (MTU) size.</td>
</tr>
<tr>
<td></td>
<td>• collision—Number of messages retransmitted because of an Ethernet collision.</td>
</tr>
<tr>
<td>packets output</td>
<td>Total number of messages transmitted by the system.</td>
</tr>
<tr>
<td>bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.</td>
</tr>
<tr>
<td>total output drops</td>
<td>Total number of packets dropped from the output queue because the queue was full.</td>
</tr>
<tr>
<td>Output</td>
<td>Indicates the total number of broadcast and multicast packets transmitted by the interface.</td>
</tr>
<tr>
<td>Output errors</td>
<td>Displays the number of errors transmitted on the interface. Output errors occur when outgoing cells are dropped or corrupted. The possible types output errors are as follows:</td>
</tr>
<tr>
<td></td>
<td>• underruns—Number of times that the far-end transmitter has been running faster than the near-end receiver can handle.</td>
</tr>
<tr>
<td></td>
<td>• aborts—Number of illegal sequences of one bits on the interface.</td>
</tr>
<tr>
<td></td>
<td>• loss of carrier—Number of times the interface was reset because the carrier detect line of that interface was up, but the line protocol was down.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers backplane ethernet location clients, on page 468</code></td>
<td>Displays information about client applications in a particular location.</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet location detail, on page 470</code></td>
<td>Displays detailed information about the backplane interfaces in a particular location.</td>
</tr>
</tbody>
</table>
show controllers backplane ethernet location clients

To display information about client applications in a particular location, use the `show controllers backplane ethernet location clients` command in EXEC mode.

```
show controllers backplane ethernet location node-id clients client-id {statistics | all}
```

**Syntax Description**
- **node-id**: Identifies the node whose local client applications information you want to display. The `node-id` argument is entered in the rack/slot/module notation.
- **client-id statistics**: Displays a list of client statistics for the specified client ID. Range is from 1 through 22.
- **client-id all**: Displays a list of all client applications and their IDs.

**Command Modes**
- EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following guidelines show the output from the `show controllers backplane ethernet location clients` command, which displays detailed information about the backplane client application statistics:

```
RP/0/RSP1/CPU0:router# show controllers backplane ethernet location 0/0/CPU0 clients all

<table>
<thead>
<tr>
<th>Intf Name</th>
<th>Client ethernet server id</th>
<th>Client Process Id</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE0_0_CPU0</td>
<td>1</td>
<td>12307</td>
<td>QNX network manager</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>28726</td>
<td>Group services</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>Reserved for Attach</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0</td>
<td>Plugin controller</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0</td>
<td>Designated SC</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0</td>
<td>HFR H/W diags</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>0</td>
<td>IP packet handler</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>16415</td>
<td>Redundancy controller</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>0</td>
<td>HFR Virtual console</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>12312</td>
<td>HFR Virtual terminal</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>12305</td>
<td>Control ethernet echo</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>0</td>
<td>Control eth echo reply</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>0</td>
<td>Card Configuration Protocol</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>0</td>
<td>Reserved for Attach</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>0</td>
<td>Chassis controller</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>0</td>
<td>Forwarding driver</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>16414</td>
<td>MBI hello</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>0</td>
<td>MBI Boot Server Source</td>
</tr>
</tbody>
</table>
```
Table 34: show controllers backplane ethernet location clients Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Name</td>
<td>Identifies the Ethernet interface.</td>
</tr>
<tr>
<td>Client ethernet server id</td>
<td>Identifies the Ethernet server for the specified interface.</td>
</tr>
<tr>
<td>Client process id</td>
<td>Identifies the client process running on the specified interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the backplane client application.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers backplane ethernet location brief, on page 466</td>
<td>display brief information about backplane Ethernet interfaces in a particular location</td>
</tr>
<tr>
<td>show controllers backplane ethernet location detail, on page 470</td>
<td>Displays detailed information about the backplane interfaces in a particular location.</td>
</tr>
</tbody>
</table>
show controllers backplane ethernet location detail

To display detailed information about the backplane interfaces in a particular location, use the `show controllers backplane ethernet location detail` command in EXEC mode.

**show controllers backplane ethernet location node-id detail**

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows the output from the `show controllers backplane ethernet location detail` command:

```
RP/0/RSP0/CPU0:router# show controllers backplane ethernet location 0/1/0 detail

FastEthernet0_1_0 is up
  Hardware is 10/100 Ethernet, H/W address is 5246.4800.0010
  Internet address is 10.0.0.16
  MTU 1514 bytes
  Encapsulation HFRIES (HFR Internal Ethernet Server)
  Mode : Full Duplex, Rate : 100Mb/s
        426422 packets input, 0 bytes, 1 total input drops
        14170 packets discarded (935122 bytes) in garbage collection
        16 packets discarded (5344 bytes) in recv processing
        Received 0 broadcast packets, 0 multicast packets
        Input errors: 0 CRC, 0 overrun, 0 alignment, 0 length, 0 collision
        440272 packets output, 0 bytes, 0 total output drops
        Output 0 broadcast packets, 0 multicast packets
        Output errors: 0 underruns, 0 aborts, 0 loss of carrier

Table 35: show controllers backplane ethernet location detail Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Provides the hardware type, followed by the hardware address.</td>
</tr>
<tr>
<td>Internet address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum packet size, in bytes, that a particular interface can handle.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation method assigned to the interface.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates the operating mode of the interface, followed by transmission data.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>packets input</td>
<td>Total number of packets received.</td>
</tr>
<tr>
<td>bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.</td>
</tr>
<tr>
<td>total input drops</td>
<td>Total number of packets dropped from the input queue because the queue was full.</td>
</tr>
<tr>
<td>packets discarded in garbage collection</td>
<td>Number of packets and bytes discarded.</td>
</tr>
<tr>
<td>packets discarded in recv processing</td>
<td>Number of packets and bytes discarded.</td>
</tr>
<tr>
<td>Received broadcast packets and multicast packets</td>
<td>Indicates the total number of broadcast and multicast packets received by the interface.</td>
</tr>
<tr>
<td>Input errors</td>
<td>Displays the number of errors received by the interface. Input errors occur when incoming cells are dropped or corrupted. The possible input errors are as follows:</td>
</tr>
<tr>
<td></td>
<td>• CRC—Number of times that the checksum calculated from the data received did not match the checksum from the transmitted data.</td>
</tr>
<tr>
<td></td>
<td>• overrun—Number of times that the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data.</td>
</tr>
<tr>
<td></td>
<td>• alignment—Number of nonoctets received.</td>
</tr>
<tr>
<td></td>
<td>• length—Number of times the interface prevented the ASIC from overrunning a maximum transmission unit (MTU) size.</td>
</tr>
<tr>
<td></td>
<td>• collision—Number of messages retransmitted because of an Ethernet collision.</td>
</tr>
<tr>
<td>packets output</td>
<td>Total number of messages transmitted by the system.</td>
</tr>
<tr>
<td>bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, in the error-free packets transmitted by the system.</td>
</tr>
<tr>
<td>total output drops</td>
<td>Total number of packets dropped from the output queue because the queue was full.</td>
</tr>
<tr>
<td>Output</td>
<td>Indicates the total number of broadcast and multicast packets transmitted by the interface.</td>
</tr>
</tbody>
</table>
Output errors

Displays the number of errors transmitted on the interface. Output errors occur when outgoing cells are dropped or corrupted. The possible types of output errors are as follows:

- **underruns**—Number of times that the far-end transmitter has been running faster than the near-end receiver can handle.
- **aborts**—Number of illegal sequences of one bits on the interface.
- **loss of carrier**—Number of times the interface was reset because the carrier detect line of that interface was up, but the line protocol was down.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers backplane ethernet location brief</code> on page 466</td>
<td>Display brief information about backplane Ethernet interfaces in a particular location.</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet location clients</code> on page 468</td>
<td>Displays information about client applications in a particular location.</td>
</tr>
</tbody>
</table>
show controllers backplane ethernet location multicast groups

To display information about backplane interfaces that are in multicast groups in a particular location, use the `show controllers backplane ethernet location multicast groups` command in EXEC mode.

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

EXEC mode

**Command History**

**Release** Modification

Release 3.7.2 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows the output from the `show controllers backplane ethernet location multicast groups` command, which displays detailed information about the backplane interfaces.

```
RP/0/RSP0/CPU0# show controllers backplane ethernet location multicast groups

Intf Name Multicast address Client registered for this address
--------------------------------------------------------------------------------------------------
FastEthernet0_2_CPU0 0100.0000.0064 2 GSP
0100.0000.0065 2 GSP
0100.0000.0066 2 GSP
0100.0000.0068 2 GSP
0100.0000.006a 2 GSP
0100.0000.006c 2 GSP
0100.0000.006e 2 GSP
0100.0000.0071 2 GSP
0100.0000.2774 2 GSP
0100.0000.2775 2 GSP
0100.0000.2776 2 GSP
0100.0000.2778 2 GSP
0100.0000.277a 2 GSP
0100.0000.2782 2 GSP
0100.0000.278a 2 GSP
0100.0000.2796 2 GSP
0100.0000.2798 2 GSP
```

**Table 36: show controllers backplane ethernet location multicast groups Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Name</td>
<td>Identifies the interface whose multicast addresses are displayed.</td>
</tr>
</tbody>
</table>

**Note**

A multicast address is a single address that refers to multiple network devices.
### Multicast Addresses

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast address</td>
<td>Multicast addresses associated with the specified interface.</td>
</tr>
<tr>
<td>Note</td>
<td>A multicast address is a single address that refers to multiple network devices.</td>
</tr>
<tr>
<td>ID</td>
<td>Client identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>Client application name.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers backplane ethernet location brief</code>, on page 466</td>
<td>display brief information about backplane Ethernet interfaces in a particular location</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet location clients</code>, on page 468</td>
<td>Displays information about client applications in a particular location.</td>
</tr>
<tr>
<td><code>show controllers backplane ethernet location detail</code>, on page 470</td>
<td>Displays detailed information about the backplane interfaces in a particular location.</td>
</tr>
</tbody>
</table>
Integrated Routing and Bridging Commands

This module describes the commands to configure Integrated Routing and Bridging (IRB) on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

• interface bvi, on page 476
• routed interface bvi, on page 478
• show interfaces bvi, on page 479
interface bvi

To create a bridge-group virtual interface (BVI), use the `interface bvi` command in Global Configuration mode. To delete the BVI, use the `no` form of this command.

```
interface bvi  identifier
```

**Syntax Description**

| `identifier`        | Number for the BVI interface from 1 to 65535. |

**Command Default**

No BVI interface is configured.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BVI is a virtual interface within the router that acts like a normal routed interface. The BVI does not support bridging itself, but acts as a gateway for the corresponding bridge-domain to a routed interface within the router.

Aside from supporting a configurable MAC address, a BVI supports only Layer 3 attributes, and has the following characteristics:

- Uses a MAC address taken from the local chassis MAC address pool, unless overridden at the BVI interface.
- Is configured as an interface type using the `interface bvi` command and uses an IPv4 or IPv6 address that is in the same subnet as the hosts on the segments of the bridged domain. The BVI also supports secondary addresses.
- The BVI identifier is independent of the bridge-domain identifier. These identifiers do not need to correlate like they do in Cisco IOS software.
- Is associated to a bridge group using the `routed interface bvi` command.
- The following interface commands are supported on a BVI:
  - `arp purge-delay`
  - `arp timeout`
  - `bandwidth` (The default is 10 Gbps and is used as the cost metric for routing protocols for the BVI)
  - `ipv4`
  - `ipv6` (Supported on Gigabit Ethernet line cards only in Cisco IOS XR Release 4.1)
  - `mac-address`
  - `mtu` (The default is 1514 bytes.)
  - `shutdown`
• The BVI supports IP helper addressing and secondary IP addressing.

To display bridge group, bridge-domain, interface status, line protocol state, and packet counters for the specified BVI, use the `show l2vpn bridge domain interface bvi` form of the `show l2vpn bridge domain` (VPLS) command. To display the reason that a BVI is down, you can use the `detail` keyword option.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows how to create a BVI interface and configure its IPv4 address:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bvi 50
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.10.0.4 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routed interface bvi, on page 478</td>
<td>Associates the specified bridge group virtual interface (BVI) as the routed interface for the interfaces assigned to the bridge domain.</td>
</tr>
<tr>
<td>show interfaces bvi, on page 479</td>
<td>Displays interface status, line protocol state, and packet counters for the specified BVI.</td>
</tr>
</tbody>
</table>
routed interface bvi

To associate the specified bridge group virtual interface (BVI) as the routed interface for the interfaces assigned to the bridge domain, use the `routed interface bvi` command in L2VPN bridge group bridge domain configuration mode. To remove the BVI as the routed interface for the interfaces assigned to the bridge domain, use the `no` form of this command.

`routed interface bvi`  
*identifier*

**Syntax Description**

| identifier | Number for the BVI interface from 1 to 65535. |

**Command Default**

No routed interface is configured.

**Command Modes**

L2VPN bridge group bridge domain configuration mode (config-l2vpn-bg-bd)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Only one BVI can be configured in any bridge domain.
- The same BVI can not be configured in multiple bridge domains.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows association of a BVI interface numbered “50” on the bridge domain named “IRB”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group 10
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain IRB
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# routed interface bvi 50
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface bvi, on page 476</td>
<td>Creates a BVI interface.</td>
</tr>
<tr>
<td>show interfaces bvi, on page 479</td>
<td>Displays interface status, line protocol state, and packet counters for the specified BVI.</td>
</tr>
</tbody>
</table>
show interfaces bvi

To display interface status, line protocol state, and packet counters for the specified BVI, use the `show interfaces bvi` command in EXEC mode.

```
show interfaces bvi identifier [accounting | brief | description | detail | location location]
```

**Syntax Description**

- `identifier`: Number for the BVI interface from 1 to 65535.
- `accounting`: (Optional) Displays the number of packets of each protocol type that have been sent through the interface.
- `brief`: (Optional) Displays summary information about the interface.
- `description`: (Optional) Displays summary status information and the description for the interface.
- `detail`: (Optional) Displays detailed information about the interface. This is the default.
- `location location`: (Optional) Displays information the interface on the specified node. The `location` argument is entered in the `rack/slot/module` notation.

**Command Default**

Detailed information about the BVI interface is displayed.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID   Operation
interface read
```

The following example shows sample output for the `show interfaces bvi` command:

```
RP/0/RSP0/CPU0:router# show interfaces bvi 50
Wed Feb 16 16:05:11.508 PST
BVI50 is up, line protocol is up
   Interface state transitions: 3
   Hardware is Bridge-Group Virtual Interface, address is 0000.0000.0002
   Description: IRB Routed Example
   Internet address is 172.16.0.1/24
   MTU 9014 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
      reliability 255/255, txload 0/255, rxload 0/255
   Encapsulation ARPA, loopback not set,
   ARP type ARPA, ARP timeout 04:00:00
   Last input 00:00:37, output 00:00:00
   Last clearing of "show interface" counters never
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
```
Table 37: show interfaces bvi Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVIX is</td>
<td>Displays the state of the specified BVI interface, where x is the number of the interface. The possible values are: administratively down, down, or up.</td>
</tr>
<tr>
<td>line protocol is</td>
<td>Displays the state of the line protocol for the BVI interface. The possible values are: administratively down, down, or up.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The line protocol state is not the same as the protocol state displayed in the <code>show ip interfaces</code> command, because it is the state of Layer 2 (media) rather than Layer 3 (IP protocol).</td>
</tr>
<tr>
<td>Interface state transitions:</td>
<td>Displays the number of times the interface has changed states.</td>
</tr>
<tr>
<td>Hardware is</td>
<td>Displays Bridge-Group Virtual Interface for a BVI.</td>
</tr>
<tr>
<td>address is</td>
<td>Layer 2 MAC address of the BVI.</td>
</tr>
<tr>
<td>Description:</td>
<td>Displays the description of the interface when configured.</td>
</tr>
<tr>
<td>Internet address is <code>n.n.n.n/n</code></td>
<td>Layer 3 IP address of the BVI in dotted decimal format.</td>
</tr>
<tr>
<td>MTU</td>
<td>Displays the maximum transmission unit (MTU) for the interface. The MTU is the maximum packet size that can be transmitted over the interface. 1514 is the default.</td>
</tr>
<tr>
<td>BW x Kbit</td>
<td>Displays the current bandwidth of the interface in kilobits per second.</td>
</tr>
<tr>
<td>Max:</td>
<td>Displays the maximum bandwidth available on the interface in kilobits per second.</td>
</tr>
<tr>
<td>reliability</td>
<td>Displays the proportion of packets that are not dropped and do not have errors.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The reliability is shown as a fraction of 255.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>txload</td>
<td>Indicates the traffic flowing out of the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The txload is shown as a fraction of 255.</td>
</tr>
<tr>
<td>rxload</td>
<td>Indicates the traffic flowing into the interface as a proportion of the bandwidth.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The rxload is shown as a fraction of 255.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Layer 2 encapsulation on the interface.</td>
</tr>
<tr>
<td>loopback</td>
<td>Always displays “not set” for a BVI because loopbacks are not supported.</td>
</tr>
<tr>
<td>ARP type</td>
<td>Address Resolution Protocol (ARP) type used on the interface.</td>
</tr>
<tr>
<td>ARP timeout</td>
<td>ARP timeout in the format hours:mins:secs. This value is configurable using the <code>arp timeout</code> command.</td>
</tr>
<tr>
<td>Last input</td>
<td>Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed.</td>
</tr>
<tr>
<td>output</td>
<td>Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.</td>
</tr>
<tr>
<td>Last clearing of “show interface” counters</td>
<td>Time since the counters in this command were last cleared using the <code>clear counters</code> Exec command in hours:mins:secs.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5 minute input rate</td>
<td>Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). Note: The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. Note: The 5-minute input should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.</td>
</tr>
<tr>
<td>5 minute output rate</td>
<td>Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). Note: The 5-minute period referenced in the command output is a load interval that is configurable under the interface. The default value is 5 minutes. Note: The 5-minute output should be used only as an approximation of traffic per second during a given 5-minute period. This rate is exponentially weighted average with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.</td>
</tr>
<tr>
<td>packets input</td>
<td>Number of packets received on the interface that were successfully delivered to higher layers.</td>
</tr>
<tr>
<td>bytes</td>
<td>Number of bytes received on the interface.</td>
</tr>
<tr>
<td>total input drops</td>
<td>Total number of valid packets that were dropped after they were received. This includes packets that were dropped due to configured quality of service (QoS) or access control list (ACL) policies. This does not include drops due to unknown Layer 3 protocol.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>drops for unrecognized upper-level protocol</td>
<td>Total number of packets that could not be delivered because the necessary protocol was not configured on the interface.</td>
</tr>
<tr>
<td>Received x broadcast packets</td>
<td>Total number of Layer 2 broadcast packets received on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>multicast packets</td>
<td>Total number of Layer 2 multicast packets received on the interface. This is a subset of the total input packet count.</td>
</tr>
<tr>
<td>packets output</td>
<td>Number of packets sent from the interface.</td>
</tr>
<tr>
<td>bytes</td>
<td>Total number of bytes successfully sent from the interface.</td>
</tr>
<tr>
<td>total output drops</td>
<td>Number of packets that were dropped before being transmitted.</td>
</tr>
<tr>
<td>Output x broadcast packets</td>
<td>Number of Layer 2 broadcast packets transmitted on the interface. This is a subset of the total output packet count.</td>
</tr>
<tr>
<td>multicast packets</td>
<td>Total number of Layer 2 multicast packets received on the interface. This is a subset of the total output packet count.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface bvi, on page 476</td>
<td>Creates a BVI interface.</td>
</tr>
</tbody>
</table>
show interfaces bvi
Link Bundling Commands

This module provides command line interface (CLI) commands for configuring Link Bundle interfaces on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- backbone interface, on page 487
- bundle lacp delay, on page 488
- bundle-hash, on page 489
- bundle id, on page 495
- bundle load-balancing hash, on page 497
- bundle load-balancing hash (EFP), on page 499
- bundle maximum-active links, on page 501
- bundle minimum-active bandwidth, on page 503
- bundle minimum-active links, on page 504
- bundle port-priority, on page 505
- bundle wait-while, on page 507
- clear lacp counters, on page 508
- interface (bundle), on page 509
- isolation recovery-delay, on page 510
- lacp cisco enable, on page 511
- lacp churn logging, on page 513
- lacp collector-max-delay, on page 514
- lacp fast-switchover, on page 515
- lacp non-revertive, on page 516
- lacp packet-capture, on page 517
- lacp period short, on page 519
- lacp system priority, on page 522
- member neighbor, on page 524
- mlacp connect, on page 525
- mlacp iccp-group, on page 526
- mlacp node, on page 527
- mlacp port-priority, on page 528
- mlacp system mac, on page 529
• mlacp system priority, on page 530
• redundancy iccp group, on page 531
• redundancy one-way, on page 532
• show bundle, on page 533
• show bundle brief, on page 548
• show bundle load-balancing, on page 551
• show bundle replication bundle-ether, on page 555
• show iccp group, on page 556
• show lacp bundle, on page 558
• show lacp counters, on page 560
• show lacp io, on page 562
• show lacp packet-capture, on page 565
• show lacp port, on page 568
• show lacp system-id, on page 570
• show mlacp, on page 572
• show mlacp counters, on page 574
backbone interface

To configure interchassis group ICCP backbone interface, use the `backbone interface` command in the redundancy group ICCP configuration mode. To return to the default behavior, use the `no` form of this command.

```
backbone interface type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

None

**Command Modes**

Redundancy group ICCP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure interchassis group ICCP backbone interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# backbone interface GigabitEthernet 0/2/1/0
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy iccp group, on page 531</td>
<td>Configures Inter Chassis Communication Protocol (ICCP) parameters.</td>
</tr>
</tbody>
</table>
bundle lacp delay

To apply delay of a specified duration in adding a member to a specific bundle, use the `bundle lacp-delay` command in the interface configuration mode.

```
bundle lacp-delay
```

**Syntax Description**

`lacp-delay`  Duration of delay before a member is added to the bundle.

The range is from 1 sec to 15 sec.

**Command Default**

No default behavior or values. If not configured, there is no delay that is imposed on bundle members.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the delay for a newly added member on a bundle interface. In this example, the delay defined is for 6 secs:

```
RP/0/RSP0/CPU0:router(config)# int bundle-ether 1
RP/0/RSP0/CPU0:router(config-if)# bundle lacp-delay ?
<1000-15000> Lacp-delay timeout in milliseconds
RP/0/RSP0/CPU0:router(config-if)# bundle lacp-delay 6000
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bundle maximum-active links</code></td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td><code>show bundle</code></td>
<td></td>
</tr>
</tbody>
</table>
bundle-hash

To display the source and destination IP addresses for the member links, distributed by the load balancing feature, in a multilink interface bundle, use the `bundle-hash` command in EXEC mode.

```
bundle-hash {Bundle-Ether bundle-id | members {GigabitEthernet | TenGigabitEthernet} interface-path-id}
```

**Syntax Description**

- **Bundle-Ether bundle-id** Specifies an Ethernet bundle for which you want to calculate load balancing. Range is 1-65535.
- **members** Identifies specific bundle member links for which you want to calculate load balancing.
- **GigabitEthernet** Specifies the Gigabit Ethernet interface for which you want to calculate load balancing.
- **TenGigE** Specifies the 10 Gigabit Ethernet interface for which you want to calculate load balancing.
- **interface-path-id** Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **location** Location of source interface.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Bundle interface traffic is distributed over the various member links of a bundle according to a hash function. The `bundle-hash` command allows you to determine which bundle member link will carry a particular flow of traffic.

You can use the `bundle-hash` command to get these information:

- Which members are used for a specified source/destination address pair, such as 10.10.10.1 20.20.20.1
- The destination IP address for a specified source IP address on a specified member.
- The load balancing distribution—how many times the members of a bundle are used for a specified range of IP addresses.
The `bundle-hash` command does not display all possible IP addresses in an entire series. It stops displaying addresses after all the addresses for all the members of the bundle have been displayed once.

The `bundle-hash` command is not applicable to multicast traffic and only applicable to unicast traffic.

The `bundle-hash` command invokes a utility that initially prompts you to select some options. Based on the options you select, the utility prompts you more options to select. The initial options to select are as follows:

- L3/3-tuple or L4/7-tuple
- Single pair or Range
- IPv4 or IPv6

The `bundle-hash` command utility prompts you for these options as follows:

- Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4):
- Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]:
- Enter bundle type IP V4 (1) or IP V6 (2):
- Enter source IP V4 address:
- Enter destination IP V4 address:
- Compute destination address set for all members? [y/n]:
- Enter subnet prefix for destination address set:
- Enter bundle IP V4 address [10.10.10.10]:

You may also be prompted to make further option choices depending on your selections.

You can use the `show bundle` command to get IP address information.

Table 38: `bundle-hash` Command Options, on page 490 provides a general summary of the options and the information you need to provide for each selected option. The actual information that you need to provide depends on the selections you make and may vary from the information provided in Table 38: `bundle-hash` Command Options, on page 490.

**Table 38: `bundle-hash` Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Information You Need to Provide</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3/3-tuple</td>
<td>L3 information:</td>
</tr>
<tr>
<td></td>
<td>• Source IP address</td>
</tr>
<tr>
<td></td>
<td>• Destination IP address</td>
</tr>
<tr>
<td></td>
<td>• Destination subnet prefix</td>
</tr>
<tr>
<td></td>
<td>• Bundle IP address</td>
</tr>
</tbody>
</table>
Information You Need to Provide

<table>
<thead>
<tr>
<th>Option</th>
<th>Information You Need to Provide</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4/7-tuple</td>
<td>L3 information:</td>
</tr>
<tr>
<td></td>
<td>• Source IP address</td>
</tr>
<tr>
<td></td>
<td>• Destination IP address</td>
</tr>
<tr>
<td></td>
<td>• Protocol</td>
</tr>
<tr>
<td>L4 information:</td>
<td>..............................................................................................................................................</td>
</tr>
<tr>
<td></td>
<td>• Source port</td>
</tr>
<tr>
<td></td>
<td>• Destination port</td>
</tr>
<tr>
<td>Platform-related information:</td>
<td>..............................................................................................................................................</td>
</tr>
<tr>
<td></td>
<td>• Router ID</td>
</tr>
<tr>
<td></td>
<td>• Ingress interface</td>
</tr>
<tr>
<td>Single pair</td>
<td>Information for a single source port and destination port. The utility uses this information to</td>
</tr>
<tr>
<td></td>
<td>calculate the hash and display the bundle load-balance distribution among the user-provided</td>
</tr>
<tr>
<td></td>
<td>physical/bundle links.</td>
</tr>
<tr>
<td></td>
<td>The default is single mode.</td>
</tr>
<tr>
<td></td>
<td>While in single mode, you may receive the following prompt:</td>
</tr>
<tr>
<td>Range</td>
<td>Information for sets of source and destination addresses to generate a packet flow for each set.</td>
</tr>
<tr>
<td></td>
<td>The utility uses this information to calculate the hash for the generated packet flows and display</td>
</tr>
<tr>
<td></td>
<td>the user-provided egress member links/bundle interfaces and the number of packet flows on each</td>
</tr>
<tr>
<td></td>
<td>link.</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv4 addresses</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6 addresses</td>
</tr>
</tbody>
</table>

Compute destination address set for all members [y|n]:

If you enter y(es), several sample IPv4 addresses in the destination subnet are generated, and the link is calculated for each sample address. During this calculation, the destination network address is derived from the destination IPv4 address and the subnet prefix.

Task ID | Task ID | Operations
--------|---------|-------------
bundle   | read    |

Examples

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 28) using the 3-tuple hash algorithm, a single source and destination, and IPv4 addresses:
RP/0/RSP0/CPU0:router# bundle-hash bundle-ether 28

Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): 13
Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: s

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address: 10.12.28.2
Enter destination IP V4 address: 10.12.28.1
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 8
Enter bundle IP V4 address [10.12.28.2]: 10.12.28.2

Link hashed to is GigabitEthernet0/6/5/7
Destination address set for subnet 10.0.0.0:
  10.0.0.6 hashes to link GigabitEthernet0/1/5/6
  10.0.0.8 hashes to link GigabitEthernet0/6/5/5
  10.0.0.12 hashes to link GigabitEthernet0/6/5/6
  10.0.0.2 hashes to link GigabitEthernet0/6/5/7
  10.0.0.1 hashes to link GigabitEthernet0/1/5/7

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 28) using the 3-tuple hash algorithm, a range of source and destinations, and IPv4 addresses:

RP/0/RSP0/CPU0:router# bundle-hash bundle-ether 28

Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): 13
Single SA/DA pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: r

Maximum number of flows (num src addr * num dst addr): 65536
Enter first source IP address: 10.12.28.2
Enter subnet prefix for source address set: 8
Enter number of source addresses (1-245): 20
Enter source address modifier (1-12) [def:1]: 5

Enter destination IP address: 10.12.28.1
Enter subnet prefix for destination address set: 8
Enter number of destination addresses (1-245): 20
Enter destination address modifier (1-12) [1]: 5
Many to many (M) or simple pairs (S)? [M]: s

Calculating simple pairs...
Total number of hits 20
Member GigabitEthernet0/1/5/6 has 6 hits
Member GigabitEthernet0/6/5/5 has 2 hits
Member GigabitEthernet0/6/5/6 has 2 hits
Member GigabitEthernet0/6/5/7 has 9 hits
Member GigabitEthernet0/1/5/7 has 1 hits

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 202) using the 7-tuple hash algorithm, a single source and destination, and IPv4 addresses:

RP/0/RSP0/CPU0:router# bundle-hash bundle-ether 202
Specify load-balance configuration (L3/3-tuple or L4/7-tuple) (L3,L4): 14
Single SA:SP/DA:SP pair (IPv4,IPv6) or range (IPv4 only): S/R [S]: s

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address: 172.20.180.167
Enter destination IP V4 address: 172.30.15.42

Ingress interface --
- physical interface format: [ GigabitEthernet | TenGigE ]R/S/I/P
- bundle interface format: [ Bundle-Ether ]bundle-id
Enter ingress interface: GigabitEthernet0/2/0/3

Enter L4 protocol (TCP,UDP,SCTP,L2TPV3,NONE): UDP
Enter src port: 1000
Enter destination port: 2000
Compute destination address set for all members? [y/n]: n

S/D pair 172.20.180.167:1000/172.30.15.42:2000 -- Link hashed to is GigabitEthernet0/3/3/6

Another? [y]: y

Enter bundle type IP V4 (1) or IP V6 (2): 1
Enter source IP V4 address [172.20.180.167]: 172.20.180.167
Enter destination IP V4 address [172.30.15.42]: 172.30.15.42

Ingress interface --
- physical interface format: [ GigabitEthernet | TenGigE ]R/S/I/P
- bundle interface format: [ Bundle-Ether ]bundle-id
Enter ingress interface [GigabitEthernet0/2/0/3]: GigabitEthernet0/2/0/3

Enter L4 protocol (TCP,UDP,SCTP,L2TPV3,NONE) [udp]: UDP
Enter src port [1000]: 1000
Enter destination port [2000]: 2000
Compute destination address set for all members? [y/n]: y
Enter subnet prefix for destination address set: 24
Enter bundle IP V4 address [172.20.180.167]: 209.165.200.225

S/D pair 172.20.180.167:1000/172.30.15.42:2000 -- Link hashed to is GigabitEthernet0/3/3/6

Destination address set for subnet 172.30.15.0:
S/D pair 172.20.180.167:1000/172.30.15.6:2000 hashes to link GigabitEthernet0/2/0/1
S/D pair 172.20.180.167:1000/172.30.15.3:2000 hashes to link GigabitEthernet0/2/0/2
S/D pair 172.20.180.167:1000/172.30.15.5:2000 hashes to link GigabitEthernet0/0/3/0

Another? [y]: n

The following example shows how to calculate load balancing across the members of a link bundle (bundle-ether 5001) using entropy label, and ingress interface:

RP/0/RSP0/CPU0# bundle-hash bundle-ether 5001 location 0/0/CPU0
Calculate Bundle-Hash for L2 or L3 or sub-int based: 2/3/4 [3]: 3
Enter traffic type (1:IPv4-inbound, 2:MPLS-inbound, 3:IPv6-inbound, 4:IPv4-MGSCP, 5:IPv6-MGSCP): [1]: 2
Entropy label: y/n [n]: y
Enter Entropy Label (in decimal): 1997
Enter the source interface name (Enter to skip interface details): TenGigE0/0/0/0/0
Entropy Label 1997 -- Link hashed to is TenGigE0/1/0/29, (raw hash 0xb5703292, LAG hash 2, ICL (), LON 2, IFH 0x06001740)

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
bundle id

To add a port to an aggregated interface (or bundle), enter the `bundle id` command in interface configuration mode. To remove a port from the bundle, use the no form of the command.

```
bundle id  bundle-id  [mode  {active | on | passive}]
```

**Syntax Description**

`bundle-id`  Number of the bundle (from 1 to 65535) on which you want to add a port.

`mode`  (Optional) Specifies the mode of operation, as follows:

- **active**—Use the `mode active` keywords to run Link Aggregation Control Protocol (LACP) in active mode over the port. When you specify `active`, the port joins the bundle and is activated if LACP determines that it is compatible.
- **on**—Use the `mode on` keywords to configure an Etherchannel link over the port (no LACP running over the port).
- **passive**—Use the `mode passive` keywords to run LACP in passive mode over the port. When you specify `passive`, LACP packets are sent only if the other end of the link is using active LACP. The link joins the bundle and is activated if LACP packets are exchanged and the port is compatible.

**Command Default**

The default setting is `mode on`.

**Command Modes**

Interface configuration

**Command History**

```
Release  Modification
3.7.2     This command was introduced.
```

**Usage Guidelines**

If you enter the `bundle id` command and specify a port that is already bound to a bundle, the port unbinds from the original bundle and becomes attached to the new bundle. If the bundle numbers are the same, then the port does not unbind, but the mode changes to mode you specified with the `bundle id` command.

**Task ID**

```
Task ID Operations
bundle   read, write
```

**Examples**

This example shows how to add a port onto a bundle:

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/5/0
RP/0/RSP0/CPU0:router(config-if)# bundle id 1
```

This example shows how to add an active LACP port onto an aggregated interface (or bundle):
bundle id

RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/6/5/7
RP/0/RSP0/CPU0:router(config-if)# bundle id 5 mode active

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle id</td>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td></td>
<td>show interfaces, on page 440</td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
<tr>
<td></td>
<td>show lacp bundle, on page 558</td>
<td>Displays detailed information about LACP ports and their peers.</td>
</tr>
<tr>
<td></td>
<td>show lacp port, on page 568</td>
<td></td>
</tr>
</tbody>
</table>
bundle load-balancing hash

To specify the hash function to be used for traffic being forwarded over a bundle interface, use the bundle load-balancing hash command in interface configuration mode. To return to the default, use the no form of the command.

```
bundle load-balancing hash {dst-ip | src-ip}
```

**Syntax Description**
- `dst-ip` Specifies a load-balancing hash based on destination IP address.
- `src-ip` Specifies a load-balancing hash based on source IP address.

**Command Default**
The default platform hashes for the bundle are used. For IPv4 traffic, the default hash is based on router ID, source IP, destination IP, and if available, source and destination Layer 4 port.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Bundle load balancing hashes based on source IP address or destination IP address are used for MGSCP deployment models where traffic forwarded from the subscriber side of the network is based on source IP address, and traffic forwarded from the core side of the network is based on destination IP address.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example configures load balancing on bundle members based on source IP address:

```
RP/0/RSP0/CPU0:router(config)#interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# bundle load-balancing hash src-ip
```

The following example configures load balancing on bundle members based on source IP address under bundle subinterface:

```
RP/0/RSP0/CPU0:router(config)#interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# bundle load-balancing hash src-ip
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (bundle), on page 509</td>
<td>Specifies or creates a new bundle and enters interface configuration mode for that bundle.</td>
</tr>
<tr>
<td>lacp cisco enable, on page 511</td>
<td>Enables use of Cisco-specific TLVs in addition to standard TLVs for negotiating and exchanging LACP information on link bundles.</td>
</tr>
</tbody>
</table>
### Command and Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show bundle, on page 533</code></td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td><code>show bundle load-balancing, on page 551</code></td>
<td>Displays load balancing information, such as the ports, usage, weight, and</td>
</tr>
<tr>
<td></td>
<td>distribution of traffic on individual members of a link bundle interface.</td>
</tr>
</tbody>
</table>
bundle load-balancing hash (EFP)

To configure all egressing traffic on a particular subinterface of a bundle to flow through the same physical member link, use the bundle load-balancing hash (EFP) command in subinterface configuration mode. To disassociate the traffic from the physical member link, use the no form of the command.

bundle load-balancing hash hash-value [auto]

Syntax Description

<table>
<thead>
<tr>
<th>hash-value</th>
<th>Numeric value that specifies the physical member link through which all egressing traffic in this bundle will flow. The values are 1 through 64.</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>The physical member link through which all egressing traffic on this bundle will flow is automatically chosen.</td>
</tr>
</tbody>
</table>

Command Default

Ethernet flow point (EFP) load balancing is enabled.

Command Modes

Subinterface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The hash-value range was changed from an upper limit of 8 to 64.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is only available on an Ethernet Bundle subinterface with Layer 2 transport (l2transport) enabled.

This command allows the user to configure all egressing traffic on the fixed members of a bundle to flow through the same physical member link. If the active members of the bundle change, the traffic for the bundle may get mapped to a different physical link that has a hash value that matches the configured value.

Examples

The following example shows how to configure all egressing traffic on the fixed members of a bundle to flow through the same physical member link automatically.

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# bundle load-balancing hash auto
```

The following example shows how to configure all egressing traffic on the fixed members of a bundle to flow through a specified physical member link.

```
RP/0/RSP0/CPU0:router# config
```
RP/0/RSP0/CPU0:router(config)# **interface bundle-ether 1.1 l2transport**
RP/0/RSP0/CPU0:router(config-subif)# **bundle load-balancing hash 1**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle-hash, on page 489</td>
<td>Displays the source and destination IP addresses for the member links.</td>
</tr>
<tr>
<td>interface (bundle), on page 509</td>
<td>Specifies or creates a new bundle and enters interface configuration mode for that bundle.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td>show bundle load-balancing, on page 551</td>
<td>Displays load balancing information, such as the ports, usage, weight, and distribution of traffic on individual members of a link bundle interface.</td>
</tr>
</tbody>
</table>
bundle maximum-active links

To designate one active link and one link in standby mode that can take over immediately for a bundle if the active link fails, use the **bundle maximum-active links** command in interface configuration mode. To return to the default maximum active links value, use the **no** form of this command.

```plaintext
bundle maximum-active links links [hot-standby]
```

**Syntax Description**

- **links**: Number of active links you want to bring up in the specified bundle, up to the maximum supported on the platform. The range is 1 to 64.
- **hot-standby**: Modifies some default timeouts, such as wait-while timer and suppress-flaps, to avoid bundle-level flaps when the highest priority link fails or recovers.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Misconfiguration or inconsistent configuration with a remote side can be causing traffic loss even though the bundle is up. We recommend that you use LACP protocol to better protect against the misconfiguration.

If the **bundle maximum-active links** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

- Another Cisco IOS XR device using the same option.
- Another device using an IEEE standard-based switchover. (Cisco does not recommend using this option because unexpected behavior, such as the peer sending traffic on the standby link, can occur.)

When you configure the **hot-standby** keyword, if the partner device is not XR, you may have to further modify the timeouts. Use the commands that are used for refining the timeouts on the partner device as well. For best performance, do not configure with **bundle-maximum-active links** command on the partner device.

The **bundle maximum-active links hot-standby** command can be configured at both ends. However, this will impact the switchover times.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set default values for timeouts, to avoid bundle-level flaps when the highest priority link fails or recovers:
The following example shows how to set the number of active links required to bring up a specific bundle. In this example, the user sets the required number of active links required to bring up Ethernet bundle 5 to 2:

```
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 5
RP/0/RSP0/CPU0:router(config-if)# bundle maximum-active links 1 hot-standby
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle minimum-active links, on page 504</td>
<td>Sets the number of active links required to bring up a specific bundle.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
bundle minimum-active bandwidth

To set the minimum amount of bandwidth required before a user can bring up a specific bundle, use the `bundle minimum-active bandwidth` command in interface configuration mode.

```
bundle minimum-active bandwidth kbps
```

**Syntax Description**

`kbps` Minimum bandwidth required before you can bring up a bundle. Range is from 1 through a number that is equivalent to the combined bandwidths of 8 TenGigabitEthernet interfaces.

**Command Default**

The default setting is `kbps = 1`.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the minimum amount of bandwidth required before a user can bring up a specific bundle. In this example, the user sets the minimum amount of bandwidth required to bring up Ethernet bundle 1 to 620000:

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 1
RP/0/RSP0/CPU0:router(config-if)# bundle minimum-active bandwidth 620000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
bundle minimum-active links

To set the number of active links required to bring up a specific bundle, use the `bundle minimum-active links` command in interface configuration mode.

```
bundle minimum-active links links
```

**Syntax Description**

- `links` Minimum number of active links allowed in the specified bundle.
- The range is from 1 through 64.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

- **Release 3.7.2** This command was introduced.
- **Release 4.0.0** The command range maximum was changed from 8 to 64.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the number of active links required to bring up a specific bundle. In this example, the user configures Ethernet bundle 5 so that 2 links must be active before the bundle can be brought up:

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 5
RP/0/RSP0/CPU0:router(config-if)# bundle minimum-active links 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle maximum-active links, on page 501</td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td></td>
</tr>
</tbody>
</table>
bundle port-priority

To configure Link Aggregation Control Protocol (LACP) priority for a port, enter the `bundle port-priority` command in interface configuration mode. To return to the default LACP priority value, use the `no` form of this command.

```
bundle port-priority priority
```

**Syntax Description**
- `priority` Priority for this port, where a lower value equals a higher priority. Replace the `priority` argument with a number. Range is from 1 through 65535.

**Command Default**
- `priority`: 32768

**Command Modes**
- Interface configuration

**Command History**
- **Release** | **Modification**
  - Release 3.7.2 | This command was introduced.

**Usage Guidelines**
- The LACP priority value forms part of the port ID, which is transmitted within the LACP packets that are exchanged with the peer. The peer uses the LACP packets to determine whether a given port should carry traffic for the bundle.

For Multi-Gigabit Service Control Point (MGSCP), the `bundle port-priority` command applies to working links.

**Note**
- A lower LACP value is a higher LACP priority for the port.

**Task ID**
- **Task** | **Operations**
  - bundle | read, write

**Examples**
The following example shows how to configure LACP priority on a port:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# bundle port-priority 1
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle id, on page 495</td>
<td>Adds a port to an aggregated interface or bundle.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show lACP bundle, on page 558</td>
<td>Displays detailed information about LACP ports and their peers.</td>
</tr>
<tr>
<td>show lACP port, on page 568</td>
<td></td>
</tr>
<tr>
<td>show lACP system-id, on page 570</td>
<td>Displays the local system ID used by the LACP.</td>
</tr>
</tbody>
</table>
bundle wait-while

To specify the duration of the wait-while timer for a bundle, use the `bundle wait-while` command in the bundle interface configuration mode. To disable waiting, use the `no` form of the command.

```
bundle wait-while  wait-while-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>wait-while-time</code></th>
<th>Wait-while time, in milliseconds. The range is between 0 to 2000.</th>
</tr>
</thead>
</table>

**Command Default**
The default wait-while time is 2000 milliseconds.

**Command Modes**
Bundle interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to configure the wait-while time.

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# bundle wait-while 20
```
clear lacp counters

To clear Link Aggregation Control Protocol (LACP) counters for all members of all bundles, all members of a specific bundle, or for a specific port, enter the **clear lacp counters** command in EXEC mode.

```
clear lacp counters [{bundle Bundle-Ether bundle-id | port {GigabitEthernet interface-path-id | TenGigE interface-path-id}}]
```

**Syntax Description**

- **bundle**: (Optional) Clears LACP counters for all members of a bundle.
- **Bundle-Ether node-id**: (Optional) Ethernet bundle. Use the `node-id` argument to specify the node ID number of the LACP counters you want to clear. Range is 1 through 65535.
- **port**: (Optional) Clears all LACP counters on the specified bundle or interface.
- **GigabitEthernet**: (Optional) Gigabit Ethernet interface. Use the `interface-path-id` argument to specify the Gigabit Ethernet interface whose LACP counters you want to clear.
- **TenGigE**: (Optional) Ten Gigabit Ethernet interface. Use the `interface-path-id` argument to specify the Ten Gigabit Ethernet interface whose LACP counters you want to clear.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>execute</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear LACP counters:

```
RP/0/RSP0/CPU0:router# clear lacp counters
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp counters, on page 560</td>
<td>Displays LACP statistics.</td>
</tr>
</tbody>
</table>
interface (bundle)

To create a new bundle and enter interface configuration mode for that bundle, use the `interface (bundle)` command in Global Configuration mode. To delete a bundle, use the `no` form of this command.

```
interface Bundle-Ether bundle-id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
<th>Usage Guidelines</th>
<th>Task ID</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether</td>
<td>No bundle interface is configured.</td>
<td>Global Configuration mode</td>
<td>Release 3.7.2 This command was introduced.</td>
<td>No specific guidelines impact the use of this command.</td>
<td>bundle read, write</td>
<td>show bundle, on page 533 Displays information about configured bundles.</td>
</tr>
</tbody>
</table>

This example shows how to create an Ethernet bundle and enter interface configuration mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/RSP0/CPU0:router(config-if)#
```
**isolation recovery-delay**

To specify a delay before clearing the isolation condition after recovery from failure, use the `isolation recovery-delay` command in the redundancy group ICCP configuration mode. To return to the default value, use the `no` form of this command.

```
isolation recovery-delay seconds
```

**Syntax Description**

- `seconds`  Recovery delay in seconds.

**Command Default**

By default, the delay is set to 180 seconds.

**Command Modes**

Redundancy group ICCP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

This example shows how to configure ICCP parameters:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# isolation recovery-delay 35
```

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redundancy iccp group</code>, on page 531</td>
<td>Configures Inter Chassis Communication Protocol (ICCP) parameters.</td>
</tr>
</tbody>
</table>
To enable use of Cisco-specific TLVs in addition to standard TLVs for negotiating and exchanging LACP information on link bundles, use the `lacp cisco enable` command in interface configuration mode. To return to the default, use the `no` form of the command.

```
lacp cisco enable [link-order signaled]
```

**Syntax Description**

- **link-order signaled** (Optional) Includes link order numbering as part of the LACP processing.
- **Note** This keyword is required for MGSCP.

**Command Default**

Cisco type-length values (TLVs) are not used.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `lacp cisco enable link-order signaled` command is required on bundle interfaces supporting deployment of Multi-Gigabit Service Control Point (MGSCP), and must be configured symmetrically on both the access and core bundle. When link order signaling is enabled, then only one set of Link Ordering Numbers (LONs) are used for the bundle, and LACP processing of LONs is enabled for load balancing tables.

The LONs from the highest priority LACP system take precedence. Where both systems have the same LACP system ID (for example, with MGSCP where both ends of the bundle terminate on the same device), the LONs from the bundle interface with the numerically lowest bundle ID take precedence.

When `lacp cisco enable` command is configured without link order signaling, then links are assigned ordering numbers as they become active and keep them until the link goes inactive. The numbers are exchanged using LACP, but they are not used.

**Example**

The following example enables the use of Cisco TLVs to include link order numbering as part of the LACP processing on this bundle:
RP/0/RSP0/CPU0:router(config)# **interface** Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# **lacp cisco enable link-order signaled**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>interface (bundle), on page 509</strong></td>
<td>Specifies or creates a new bundle and enters interface configuration mode for that bundle.</td>
</tr>
</tbody>
</table>
**lscp churn logging**

To configure the parameters for LACP churn detection, enter the `lscp churn logging` command in interface configuration mode. To return to the default, use the `no` form of the command.

```
lscp churn logging {actor | both | partner}
```

**Syntax Description**
- **actor**: Logs the churn events of the actor, which is the router under consideration, only.
- **both**: Logs the churn events of both the actor and the partner.
- **partner**: Logs the churn events of the partner router only

**Command Default**
The parameters for churn detection are not configured.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.1.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to configure the LACP churn detection on a partner router:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# lscp churn logging partner
```

The following example shows how to configure the LACP churn detection on both actor and partner routers:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# lscp churn logging both
```
**IACP Collector-Max-Delay**

To configure the maximum period of wait time between sending of two subsequent Ethernet frames on a link, enter the `IACP Collector-Max-Delay` command in interface configuration mode. To return to the default, use the `no` form of this command.

```
IACP Collector-Max-Delay  delay-in-tens-of-microseconds
```

**Syntax Description**

| delay-in-tens-of-microseconds | Length of wait time, in tens of microseconds. The range is from 0 to 65535. The default is 0xFFFF. |

**Command Default**

The collector-max-delay time is not configured.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to configure the maximum period of wait time between sending of two subsequent Ethernet frames on a link:

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 100
RP/0/RSP0/CPU0:router(config-if)# IACP Collector-Max-Delay 500
```
**lACP fast-switchover**

To disable the wait-while timer in the LACP state machine, use the `lACP fast-switchover` command in interface configuration mode. To re-enable the wait-while timer, use the `no` form of this command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

The wait-while timer in the LACP state machine is enabled.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you have 1:1 link protection enabled (you set the value of the `bundle maximum-active links` command to 1) on a bundle with member links running LACP, you can optionally disable the wait-while timer in the LACP state machine. Disabling this timer causes a bundle member link in standby mode to expedite its normal state negotiations, thereby enabling a faster switchover from a failed active link to the standby link.

Regardless of the type of switchover you are using, the default IEEE standard-based or the faster proprietary optimized switchover, the state negotiations of the standby link is expedited. (For more information about the switchover types, refer to the `bundle maximum-active links`, on page 501 command.) However, enabling the `lACP fast-switchover` command provides a greater benefit if used with the IEEE standard-based switchover.

### Examples

The following example shows how to disable the wait-while timer for LACP-enabled member links of Bundle-Ether 28:

```bash
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 28
RP/0/RSP0/CPU0:router(config-if)# lACP fast-switchover
```

The following example shows how to re-enable the wait-while timer for LACP-enabled member links of Bundle-Ether 28:

```bash
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 28
RP/0/RSP0/CPU0:router(config-if)# no lACP fast-switchover
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bundle maximum-active links</code>, on page 501</td>
<td></td>
</tr>
</tbody>
</table>
**lACP non-revertive**

To configure the currently active but lower priority port to remain active port even after a higher priority port is capable of being operational, use the `lACP non-revertive` command in the bundle interface configuration mode. To revert to the default configuration, use the `no` form of this command.

**lACP non-revertive**

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>A higher priority port would become the active port after it becomes operational again.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Bundle interface configuration mode

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.2</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Example**

The following example shows how to configure the non-revertive behaviour on an LACP bundle interface.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 1
RP/0/RSP0/CPU0:router(config-if)# lACP non-revertive
```
lacp packet-capture

To capture LACP packets so that their information can be displayed by the show lacp packet-capture command, use the `lacp packet-capture` command in EXEC mode.

```
lacp packet-capture gigabitethernet interface-path-id | tengige interface-path-id number-of-packets
```

To stop capturing LACP packets or to clear captured LACP packets, use the `lacp packet-capture stop` or `lacp packet-capture clear` command in EXEC mode.

```
lacp packet-capture [bundle-ether bundle-id] [gigabitethernet interface-path-id] [tengige interface-path-id] clear | stop
```

**Syntax Description**

- `bundle-ether` Ethernet bundle interface specified by `bundle-id`.
- `GigabitEthernet` Gigabit Ethernet interface specified by `interface-path-id`.
- `TenGigE` Ten Gigabit Ethernet interface specified by `interface-path-id`.
- `interface-path-id` Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- `bundle-id` Number specifying the bundle interface. The range is 1 to 65535.
- `number-of-packets` Number of packets to capture.
- `clear` Clears all currently captured packets.
- `stop` Stops capturing packets.

**Command Default**
The default (no parameters) executes globally for all interfaces on the line card.

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `lacp packet-capture` command captures transmitted and received LACP packets on a single bundle member interface. The contents of these packets can then be displayed by the `show lacp packet-capture` command. If the `lacp packet-capture` command is not issued, the `show lacp packet-capture` command does not display any information.

The `lacp packet-capture` command continues capturing LACP packets until the `stop` keyword is issued for that port or that bundle. Captured packets are stored and continue to be displayed until the `clear` keyword is issued for that port or that bundle.
LACP packets can only be captured for one port on a line card at a time. Starting a packet capture on a port implicitly stops and clears all packet-captures on all other ports on that line card.

To stop capturing LACP packets before the specified number of packets have been captured, issue the stop keyword.

If stop is specified for a single interface, packet capturing is stopped only on that interface.

If stop is specified for a bundle interface, packet capturing is stopped on all members of that bundle.

If stop is specified globally (the default - no parameters), packet capturing is stopped on all bundle interfaces on the router.

To clear all captured LACP packets that are stored for an interface, issue the clear keyword.

If clear is specified for a single interface, packets are cleared only on that interface.

If clear is specified for a bundle interface, packets are cleared on all members of that bundle.

If clear is specified globally (the default - no parameters), packets are cleared on all bundle interfaces on the router.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

RP/0/RSP0/CPU0:router# lACP packet-capture pos 0/1/0/0 100

RP/0/RSP0/CPU0:router# lACP packet-capture pos 0/1/0/0 stop

RP/0/RSP0/CPU0:router# lACP packet-capture pos 0/1/0/0 clear

The following example shows how to capture LACP packets on a Gigabit Ethernet interface:

RP/0/RSP0/CPU0:router# lACP packet-capture gigabitethernet 0/2/0/0 100

The following example shows how to stop capturing LACP packets on a Gigabit Ethernet interface:

RP/0/RSP0/CPU0:router# lACP packet-capture gigabitethernet 0/2/0/0 stop

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lACP io, on page 562</td>
<td>Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.</td>
</tr>
<tr>
<td>show lACP packet-capture, on page 565</td>
<td>Displays the contents of LACP packets that are sent and received on an interface.</td>
</tr>
<tr>
<td>lACP period short, on page 519</td>
<td>Enables a short period time interval for the transmission and reception of LACP packets.</td>
</tr>
</tbody>
</table>
**lACP period short**

To enable a short period time interval for the transmission and reception of Link Aggregation Control Protocol (LACP) packets, use the `lACP period short` command in interface configuration mode. To return to the default short period, use the `no` form of this command.

```
lACP period short [receive interval] [transmit interval]
```

**Syntax Description**

- `receive interval`: Time interval (in milliseconds) for receiving LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.

- `transmit interval`: Time interval (in milliseconds) for transmitting LACP packets when LACP short period is enabled. The range is 100 to 1000 and must be multiples of 100, such as 100, 200, 300, and so on.

**Command Default**

The default is 1000.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure a custom LACP short period `transmit interval` at one end of a link, you must configure the same time period for the `receive interval` at the other end of the link.

**Note**

You must always configure the `transmit interval` at both ends of the connection before you configure the `receive interval` at either end of the connection. Failure to configure the `transmit interval` at both ends first results in route flapping (a route going up and down continuously). When you remove a custom LACP short period, you must do it in reverse order. You must remove the `receive` intervals first and then the `transmit` intervals.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable a default Link Aggregation Control Protocol (LACP) short period on a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lACP period short
```
The following example shows how to configure custom Link Aggregation Control Protocol (LACP) short period transmit and receive intervals at both ends of a connection:

**Router A**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Router B**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Router A**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Router B**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short transmit 500
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Router A**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short receive 500
RP/0/RSP0/CPU0:router(config-if)# commit
```

**Router B**

```
RP/0/RSP0/CPU0:router(config-if)# config
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# lacp period short receive 500
RP/0/RSP0/CPU0:router(config-if)# commit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp io, on page 562</td>
<td>Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show lACP packet-capture</code>, on page 565</td>
<td>Displays the contents of LACP packets that are sent and received on an interface.</td>
</tr>
<tr>
<td><code>lACP packet-capture</code>, on page 517</td>
<td>Captures LACP packets so that their information can be displayed.</td>
</tr>
</tbody>
</table>
**Iacp system priority**

To configure the priority for the current system, enter the `Iacp system priority` command in Global Configuration mode mode. To return to the default LACP system priority value, use the `no` form of this command.

```
lacp system priority priority
```

**Syntax Description**

- Priority for this system. Replace `priority` with a number. Range is from 1 through 65535. A lower value is higher priority.

**Command Default**

The default setting is `priority = 32768`.

**Command Modes**

Global Configuration mode

**Command History**

Release | Modification
---------|-------------
3.7.2    | This command was introduced.

**Usage Guidelines**

The system priority value forms part of the LACP system ID, which is transmitted within each LACP packet. The system ID, port ID and key combine to uniquely define a port within a LACP system.

**Examples**

The following example shows how to configure an LACP priority of 100 on a router:

```
RP/0/RSP0/CPU0:router (config)# lacp system priority 100
```

The following example shows how to configure an LACP priority of 10 and MAC address on the Bundle-Ether interface:

```
RP/0/RSP0/CPU0:router (config)# do configure
RP/0/RSP0/CPU0:router (config)# interface Bundle-Ether 1
RP/0/RSP0/CPU0:router (config-if)# lacp system priority 10
RP/0/RSP0/CPU0:router (config-if)# lacp system mac 00c1.4c00.bd15
RP/0/RSP0/CPU0:router (config-if)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lacp system-id</code>, on page 570</td>
<td>Displays the local system ID used by the LACP.</td>
</tr>
</tbody>
</table>
### Command and Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp bundle, on page 558</td>
<td>Displays detailed information about LACP ports and their peers.</td>
</tr>
<tr>
<td>show lacp port, on page 568</td>
<td></td>
</tr>
</tbody>
</table>
member neighbor

To configure interchassis group ICCP members, use the `member neighbor` command in redundancy ICCP group configuration mode. To return to the default behavior, use the `no` form of this command.

```
member neighbor neighbor-ip-address
no member neighbor neighbor-ip-address
```

**Syntax Description**

- `neighbor-ip-address`: Specifies the ICCP member neighbor IP address.

**Command Default**

None

**Command Modes**

Redundancy ICCP group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure interchassis group ICCP members:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# member neighbor 10.1.1.1
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy iccp group, on page 531</td>
<td>Configures Inter Chassis Communication Protocol (ICCP) parameters.</td>
</tr>
</tbody>
</table>
**mlacp connect**

To specify configuration options for connecting to mLACP peers, use the `mlacp connect` command in the redundancy ICCP group configuration mode. To disable this feature, use the `no` form of this command.

```mlacp connect timeout seconds```

**Syntax Description**

- `timeout` Specifies the time to wait before assuming mLACP peer is down.
- `seconds` Number of seconds to wait before assuming the mLACP peer is down.

**Command Default**

No default behavior or values

**Command Modes**

Redundancy ICCP group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task**: read, write

**Examples**

This example shows how to specify configuration options for connecting to mLACP peers:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlacp connect timeout 100
```

**Related Commands**

- `redundancy iccp group` Configures ICCP parameters.
mlacp iccp-group

To configure ICCP redundancy group for a bundle, use the **mlacp iccp-group** command in bundle interface configuration mode. To return to the default value, use the **no** form of this command.

```
mlacp iccp-group  group-id
```

**Syntax Description**

- **group-id** Specifies the ICCP redundancy group in which the bundle should operate. The group-id value ranges between 1-4294967295.

**Command Default**

The bundle behaves as a single chassis LAG.

**Command Modes**

Bundle interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**
  - **Bundle**
    - read, write

**Examples**

The following example shows how to configure an ICCP redundancy group for a bundle:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 30
RP/0/RSP0/CPU0:router(config-if)# mlacp iccp-group 200
RP/0/RSP0/CPU0:router(config-if)#
```
mlacp node

To configure the mLACP node ID to be used in the ICCP group, use the `mlacp node` command in the redundancy ICCP group configuration mode. To return to the default value, use the `no` form of this command.

```
mlacp node node-id
```

**Syntax Description**

`node-id` Specifies the unique node ID in the ICCP group for this system. The `node-id` value ranges between 0 to 7.

**Command Default**

No default behavior or values

**Command Modes**

Redundancy ICCP group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the mLACP node ID to be used in the ICCP group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlacp node 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>redundancy iccp group</th>
<th>Configures ICCP parameters.</th>
</tr>
</thead>
</table>
mlacp port-priority

To set the priority for all member links, use the `mlacp port-priority` command in bundle interface configuration mode. To return to the default value, use the `no` form of this command.

```
mlacp port-priority  priority
```

**Syntax Description**

- `priority` Specifies the priority for member ports. The priority value ranges between 1-65535. A lower value indicates higher priority.

**Command Default**

No default behavior or values

**Command Modes**

Bundle interface configuration

**Command History**

- **Release 4.0.0** This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Bundle read, write**

**Examples**

This example shows how to set the priority for all member links:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 30
RP/0/RSP0/CPU0:router(config-if)# mlacp port-priority 20
```
mlacp system mac

To configure the LACP system ID to be used in an ICCP group, use the `mlacp system mac` command in the redundancy ICCP group configuration mode. To return to the default value, use the `no` form of this command.

```
mlacp system mac mac-id
```

**Syntax Description**

`mac-id` Specifies the unique ID for the system.

**Note**  A non-zero value is permitted.

**Command Default**

No default behavior or values

**Command Modes**

Redundancy ICCP group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 4.0.0 | This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**: ID
- **Operations**: bundle read, write

**Examples**

The following example shows how to configure the LACP system ID to be used in an ICCP group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlacp system mac 1.1.1
```

**Related Commands**

- redundancy iccp group: Configures ICCP parameters.
**mlacp system priority**

To configure the LACP system priority to be used in the ICCP group, use the `mlacp system priority` command in the redundancy ICCP group configuration mode. To return to the default value, use the `no` form of this command.

```
mlacp system priority priority
```

**Syntax Description**

- `priority` Specifies the priority for the system.
  
  **Note** Lower value indicates higher priority.

**Command Default**

No default behavior or values

**Command Modes**

Redundancy ICCP group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **read**
- **write**

**Examples**

This example shows how to configure the LACP system priority to be used in the ICCP Group:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlacp system priority 10
```

**Related Commands**

- `redundancy iccp group` Configures ICCP parameters.
redundancy iccp group

To configure Inter Chassis Communication Protocol (ICCP) parameters, use the `redundancy iccp group` command in the Global Configuration mode. To return to the default, use the `no` form of this command.

```
redundancy iccp group group-id
```

**Syntax Description**
- `group-id` Specifies ICCP group ID.

**Command Default**
ICCP redundancy is disabled.

**Command Modes**
Global Configuration mode

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure ICCP parameters:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)#
```
redundancy one-way

To enforce one-way pseudowire redundancy behavior when the redundancy group is configured, use the `redundancy one-way` command in the L2VPN pseudowire class configuration mode. To return to the default, use the `no` form of this command.

**redundancy one-way**

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
<th>Usage Guidelines</th>
<th>Task ID</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-way redundancy is disabled.</td>
<td>L2VPN pseudowire class configuration</td>
<td>Release 4.0.0 This command was introduced.</td>
<td>No specific guidelines impact the use of this command.</td>
<td>l2vpn</td>
<td>RP/0/RSP0/CP00:router# configure RP/0/RSP0/CP00:router (config)# l2vpn RP/0/RSP0/CP00:router (config-l2vpn)# pw-class class_mpls RP/0/RSP0/CP00:router (config-l2vpn-pwc)# encapsulation mpls RP/0/RSP0/CP00:router (config-l2vpn-pwc-mpls)# redundancy one-way RP/0/RSP0/CP00:router (config-l2vpn-pwc-mpls)#</td>
</tr>
</tbody>
</table>
show bundle

To display information about all bundles or a specific bundle of a particular type, use the **show bundle** command in EXEC mode.

**show bundle [Bundle-Ether|Bundle-POS bundle-id]**

### Syntax Description
- **Bundle-Ether**: Displays information for the specified Ethernet bundle.
- **Bundle-POS**: Displays information for the specified POS bundle.
- **bundle-id**: Number from 1 to 65535 that identifies a particular bundle.

### Command Default
Information is displayed for all configured bundles.

### Command Modes
EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.8.0</td>
<td>The <em>reasons</em> keyword was removed.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The output for this command was replaced with a new format.</td>
</tr>
<tr>
<td>Release 4.1.0</td>
<td>The following output fields were added:</td>
</tr>
<tr>
<td></td>
<td>• Load-balancing</td>
</tr>
<tr>
<td></td>
<td>• Link order signaling</td>
</tr>
<tr>
<td></td>
<td>• Hash type</td>
</tr>
<tr>
<td></td>
<td>• Cisco extensions</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>Support for Bundle-POS was added.</td>
</tr>
<tr>
<td>Release 5.3.2</td>
<td>The &quot;Non-revertive&quot; output field was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
To see information for all bundles configured on the router, use the **show bundle** form of the command.

To see information for a specific bundle, use the **show bundle Bundle-Ether bundle-id** form of the command with the number of the configured bundle.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows output for all bundle interfaces that are configured on the router:
show bundle

Bundle-Ether 2
Status: Up
Local links (active/standby/configured): 1 / 0 / 1
Local bandwidth (effective/available): 100000 (100000) kbps
MAC address (source): 1234.4321.1111 (Gi0/0/0/1)
Minimum active links / bandwidth: 1 / 500 kbps
Maximum active links: 32
Wait-while timer: 2000 ms
Load-balancing: Default
LACP: Operational
Flap suppression timer: 2500 ms
Cisco extensions: Disabled
Non-revertive: Disabled
mLACP: Operational
Interchassis group: 3
Foreign links (active/configured): 1 / 1
Switchover type: Revertive
Recovery delay: 300 s
Maximize threshold: 2 links
IPv4 BFD: Not operational
State: Off
Fast detect: Enabled
Start timer: Off
Neighbor-unconfigured timer: Off
Preferred min interval: 150 ms
Preferred multiple: 3
Destination address: Not Configured

<table>
<thead>
<tr>
<th>Port</th>
<th>Device</th>
<th>State</th>
<th>Port ID</th>
<th>B/W, kbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/1</td>
<td>Local</td>
<td>Active</td>
<td>0x8000, 0x0001</td>
<td>100000</td>
</tr>
<tr>
<td>MyFirstInterface</td>
<td></td>
<td>Negotiating</td>
<td>0x8000, 0x0032</td>
<td>100000</td>
</tr>
</tbody>
</table>

Bundle-Ether 3
Status: Up
Local links (active/standby/configured): 1 / 0 / 1
Local bandwidth (effective/available): 100000 / 100000 kbps
MAC address (source): 1234.4321.2222 (chassis pool)
Minimum active links / bandwidth: 1 / 500 kbps
Maximum active links: 32 (from partner)
Wait-while timer: 100 ms
Load-balancing:
  Link order signaling: Operational
  Hash type: Src-IP
LACP: Operational
Flap suppression timer: 120 s
Cisco extensions: Enabled
Non-revertive: Disabled
mLACP: Not configured
IPv4 BFD: Not operational

<table>
<thead>
<tr>
<th>Port</th>
<th>Device</th>
<th>State</th>
<th>Port ID</th>
<th>B/W, kbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/2</td>
<td>Local</td>
<td>Active</td>
<td>0x8000, 0x0002</td>
<td>100000</td>
</tr>
</tbody>
</table>
Table 39: show bundle Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-typenumber</td>
<td>Full name of the bundle interface, where type is Ether (Ethernet), followed by the configured number of the bundle.</td>
</tr>
<tr>
<td>Status:</td>
<td>State of the bundle on the local device, with one of the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• Admin down—The bundle has been configured to be shut down.</td>
</tr>
<tr>
<td></td>
<td>• Bundle shut—The bundle is holding all links in Standby state and will not support any traffic.</td>
</tr>
<tr>
<td></td>
<td>• Down—The bundle is operationally down. It has no Active members on the local device.</td>
</tr>
<tr>
<td></td>
<td>• mLACP cold standby—The bundle is acting as a multichassis LACP Standby device, but the higher layers are not synchronized.</td>
</tr>
<tr>
<td></td>
<td>• mLACP hot standby—The bundle is Up on the mLACP peer device, and the local device is ready to take over if that bundle goes down on the peer.</td>
</tr>
<tr>
<td></td>
<td>• Nak—The local and peer devices cannot resolve a configuration error.</td>
</tr>
<tr>
<td></td>
<td>• Partner down—The partner system indicates that the bundle is unable to forward traffic at its end.</td>
</tr>
<tr>
<td></td>
<td>• PE isolated—The bundle is isolated from the core.</td>
</tr>
<tr>
<td></td>
<td>• Up—The bundle has Active members on this device.</td>
</tr>
<tr>
<td>Local links &lt;active/standby/configured&gt;:</td>
<td>The number of links on the device (from 0 to the maximum number of supported links for the bundle) in the format x / y / z, with the following values:</td>
</tr>
<tr>
<td></td>
<td>• x—Number of links in Active state on the bundle.</td>
</tr>
<tr>
<td></td>
<td>• y—Number of links in Standby state on the bundle.</td>
</tr>
<tr>
<td></td>
<td>• z—Total number of links configured on the bundle.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Local bandwidth &lt;effective/available&gt;:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Bandwidth characteristics on the bundle in kilobits per second (kbps) in the format ( x/y ), with the following values:</td>
</tr>
<tr>
<td>• ( x )—Current bandwidth of the bundle (this effective bandwidth might be limited by configuration).</td>
</tr>
<tr>
<td>• ( y )—Available bandwidth of the bundle that is the sum of the bandwidths of all of the locally active links.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC address (source):</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Layer 2 MAC address on the bundle interface in the format ( xxxx.xxxx.xxxx ). The ( (source) ) of the address is shown in parentheses with the following possible values:</td>
</tr>
<tr>
<td>• Interface name—The MAC address is from the displayed member interface type and path.</td>
</tr>
<tr>
<td>• Configured—The MAC address is explicitly configured.</td>
</tr>
<tr>
<td>• Chassis pool—The MAC address is from the available pool of addresses for the chassis.</td>
</tr>
<tr>
<td>• [unknown MAC source 0]—No MAC address could be assigned to the bundle. (You might see this display if you have not completed your bundle configuration.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minimum active links / bandwidth:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Displays the following information in the format ( x/y ) kbps, with the following values:</td>
</tr>
<tr>
<td>• ( x )—Minimum number of active links (from 1 to the maximum number of links supported on the bundle) that are required for the bundle to be operative.</td>
</tr>
<tr>
<td>• ( y )—Minimum total bandwidth on active links (in kbps) that is required for the bundle to be operative.</td>
</tr>
<tr>
<td>• (partner)—Shows that the peer system's value is in use.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maximum active links:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Maximum number of links (from 1 to the maximum supported on a bundle) that can be active on the bundle.</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Wait-while timer:</td>
</tr>
<tr>
<td>Load balancing:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Link order signaling:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Hash type:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>LACP:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Flap suppression timer:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cisco extensions:</td>
</tr>
<tr>
<td>Non-revertive:</td>
</tr>
<tr>
<td>mLACP:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td>ICCP group:</td>
</tr>
</tbody>
</table>
| Role                         | ICCP redundancy role of the local device for this mLACP bundle, with the following possible values:  
  • Active—Bundle is currently active locally.  
  • Standby—Bundle is a backup locally. |
| Foreign links <active/configured>: | The number of links on the remote device in the format $x / y$, with the following values:  
  • $x$—Number of links in Active state on the remote bundle.  
  • $y$—Total number of links configured on the remote bundle. |
| Switchover type:             | Method of performing an mLACP switchover on the bundle with the following possible values:  
  • Bruteforce—Trigger the failover by marking member(s) as Not Aggregatable instead of using dynamic priority management. This is the only possible method of control when the dual-homed device (DHD) is the higher-priority system. Only applies to mLACP bundles.  
  • Non-revertive—This is the default. Dynamic priority management is used, where the bundle does not fail back to the originally active point of attachment (PoA) except when a subsequent failure occurs.  
  • Revertive—Dynamic priority management is used, but the higher-priority device (based on the configured port priorities for the bundle) is always Active unless it has encountered a failure. This means that if a failure is encountered triggering a switchover, once the failure condition is cleared the initially-active links become active again. |

The switchover type can be changed from the default behavior using the `mlacp switchover type` command,
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery delay:</td>
<td>Number of seconds (s) to delay becoming the active mLACP device after recovering from a failure, using the <code>mlacp switchover recovery delay</code> command. “None” is displayed when the <code>mlacp switchover recovery delay</code> command is not configured.</td>
</tr>
</tbody>
</table>
| Maximize threshold:       | Threshold value below which mLACP switovers are triggered to allow the bundle to reach the configured maximum number of active links or bandwidth (using the `mlacp switchover maximize` command), with the following possible values:  
  - `x` links—Number of active links used as the maximum threshold target to be maintained as a trigger for an mLACP switchover on a bundle.  
  - `y` kbps—Bandwidth in kilobits per second used as the target threshold to be maintained as a trigger for an mLACP switchover on a bundle.  
  - Not configured—The `mlacp switchover maximize` command is not configured. mLACP switovers are based on the minimum active links or bandwidth for the bundle. |
| IPv4 BFD:                 | Displays whether or not IPv4-based bidirectional forwarding (BFD) is operating on the bundle interface, with the following possible values:  
  - Operational—All required configuration has been committed for IPv4 BFD, and it is in use on the bundle.  
  - Not operational—IPv4 BFD is not working because some mandatory configuration is missing on the bundle or on the active members of the bundle.  
  - Not configured—None of the mandatory configuration for IPv4 BFD has been committed on the bundle, and the BFD sub-fields are not displayed. |
### State:

When BFD is enabled, displays the state of BFD sessions on the bundle from the sessions running on bundle members that is communicated to interested protocols, with the following possible values:

- **Down**—The configured minimum threshold for active links or bandwidth for BFD bundle members is not available so BFD sessions are down.
- **Off**—BFD is not configured on bundle members.
- **Up**—BFD sessions on bundle members are up because the minimum threshold for the number of active links or bandwidth is met.

### Fast detect:

Displays whether or not BFD fast detection is configured on the bundle, with the following possible values:

- **Enabled**—The `bfd fast-detect` command is configured on the bundle.
- **Disabled**—The `bfd fast-detect` command is not configured on the bundle.

### Start timer:

Displays status of the BFD start timer that is configured using the `bfd address-family ipv4 timers start` command, with the following possible values:

- **x s**—Number of seconds (from 60 to 3600) after startup of a BFD member link session to wait for the expected notification from the BFD peer to be received, so that the session can be declared up. If the SCN is not received after that period of time, the BFD session is declared down.
- **Off**—The start timer is not configured, and a BFD session is only declared Down upon notification from the BFD server.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor-unconfigured timer:</td>
<td>Displays status of the BFD start timer that is configured using the <code>bfd address-family ipv4 timers nbr-unconfig</code> command, with the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• <code>x s</code>—Number of seconds (from 60 to 3600) to wait after receipt of notification that the BFD configuration has been removed by a BFD neighbor, so that any configuration inconsistency between the BFD peers can be fixed. If the BFD configuration issue is not resolved before the specified timer is reached, the BFD session is declared down.</td>
</tr>
<tr>
<td></td>
<td>• Off—The neighbor-unconfigured timer is not configured, and a BFD session is only declared Down upon notification from the BFD server.</td>
</tr>
<tr>
<td>Preferred min interval:</td>
<td>Number of milliseconds (in the format <code>x ms</code>) as the minimum control packet interval for BFD sessions. The range is 15 to 30000.</td>
</tr>
<tr>
<td>Preferred multiple:</td>
<td>Value of the multiplier (from 2 to 50) that is used for echo failure detection, which specifies the maximum number of echo packets that can be missed before a BFD session is declared Down.</td>
</tr>
<tr>
<td>Destination address:</td>
<td>Destination IP address for BFD sessions on bundle member links that is configured using the <code>bfd address-family ipv4 destination</code> command. “Not configured” is displayed when no destination IP address is configured.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the local interface port that is configured to be a bundle member, or a foreign interface received by an mLACP peer device. The possible values are the shortened interface name or a text string.</td>
</tr>
<tr>
<td>Device</td>
<td>Label Distribution Protocol (LDP) address of the device where the interface port is located, with the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• <code>address</code>—IP address of the device.</td>
</tr>
<tr>
<td></td>
<td>• Local—Interface port is on the local device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>State</td>
<td>Status of the port, with one of the following possible values</td>
</tr>
<tr>
<td></td>
<td>• Active—Link can send and receive traffic.</td>
</tr>
<tr>
<td></td>
<td>• BFD Running—Link is inactive because BFD is down or has not been fully negotiated.</td>
</tr>
<tr>
<td></td>
<td>• Configured—Link is not operational or remains down due to a configuration mismatch. The link is not available for switchover from failure of an active link.</td>
</tr>
<tr>
<td></td>
<td>• Hot Standby—Link is ready to take over if an active link fails and can immediately transition to Active state without further exchange of LACP protocol data units (PDUs).</td>
</tr>
<tr>
<td></td>
<td>• Negotiating—Link is in the process of LACP negotiation and is being held in a lower LACP state by the peer (for example, because the link is Standby on the peer.)</td>
</tr>
<tr>
<td></td>
<td>• Standby—Link is not sending or receiving traffic, but is available for switchover from failure of an active link.</td>
</tr>
<tr>
<td>Port ID</td>
<td>ID of the interface port in the format x/y, with the following values:</td>
</tr>
<tr>
<td></td>
<td>• x—Port priority as a 2-byte hexadecimal value.</td>
</tr>
<tr>
<td></td>
<td>• y—Link ID as a 2-byte hexadecimal value.</td>
</tr>
<tr>
<td>B/W, kbps</td>
<td>Bandwidth of the interface port in kilobits per second.</td>
</tr>
<tr>
<td>State reason</td>
<td>Text string that is displayed beneath the bundle member listing explaining why a link has not reached Active state.</td>
</tr>
</tbody>
</table>

**Table 40: State Reasons**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD session is unconfigured on the remote end</td>
<td>The link is in BFD Running state because LACP is negotiated but the BFD session from the remote device has been unconfigured.</td>
</tr>
<tr>
<td>BFD state of this link is Down</td>
<td>The link is in BFD Running state because LACP is negotiated but the BFD session between the local system and the remote device is Down.</td>
</tr>
<tr>
<td>Reason</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Bundle has been shut down</td>
<td></td>
</tr>
<tr>
<td>Bundle interface is not present in configuration</td>
<td></td>
</tr>
<tr>
<td>Bundle is in the process of being created</td>
<td></td>
</tr>
<tr>
<td>Bundle is in the process of being deleted</td>
<td></td>
</tr>
<tr>
<td>Bundle is in the process of being replicated to this location</td>
<td></td>
</tr>
<tr>
<td>Forced switchover to the mLACP peer</td>
<td></td>
</tr>
<tr>
<td>ICCP group is isolated from the core network</td>
<td></td>
</tr>
<tr>
<td>Incompatible with other links in the bundle (bandwidth out of range)</td>
<td></td>
</tr>
<tr>
<td>LACP shutdown is configured for the bundle</td>
<td></td>
</tr>
<tr>
<td>Incompatible with other links in the bundle (LACP vs non-LACP)</td>
<td></td>
</tr>
<tr>
<td>Link is Attached and has not gone Collecting (reason unknown)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The link is in Configured state because the bundle it is configured as a member of is administratively down.</td>
</tr>
<tr>
<td>The link is in Configured state because the bundle it is configured as a member of has not itself been configured.</td>
</tr>
<tr>
<td>The link is in Configured state because the bundle it is configured as a member of is still being created.</td>
</tr>
<tr>
<td>The link is in Configured state because the bundle it is configured as a member of is being deleted.</td>
</tr>
<tr>
<td>The link is in Configured state because the bundle it is configured as a member of is still being replicated to the linecard where the link is located.</td>
</tr>
<tr>
<td>The link is in Configured state because it has been brought down as part of a forced switchover to the mLACP peer PoA. This happens only when brute force switchovers are configured.</td>
</tr>
<tr>
<td>The link is in Configured state because there is no connectivity through the network core for the ICCP group that the link and its bundle are part of. Therefore, the link has been brought down to prevent any traffic being sent by the LACP partner device.</td>
</tr>
<tr>
<td>The link is in Configured state because its bandwidth is incompatible with other links configured to be in the same bundle. The bandwidth may be too high or too low.</td>
</tr>
<tr>
<td>The link is in Configured state because the bundle is configured with LACP shutdown.</td>
</tr>
<tr>
<td>The link is in Configured state because its use of LACP is incompatible with other links configured in the same bundle. Some links might be running LACP while others are not.</td>
</tr>
<tr>
<td>The link is in Negotiating state because the mLACP peer PoA has not indicated that the link has gone Collecting in the Mux machine. This could be because of an issue between the mLACP peer and its LACP partner or because this state has not been communicated to the local system.</td>
</tr>
<tr>
<td>Reason</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Link is Collecting and has not gone Distributing (reason unknown)</td>
</tr>
<tr>
<td>Link is being removed from the bundle</td>
</tr>
<tr>
<td>Link is Defaulted; LACPDUs are not being received from the partner</td>
</tr>
<tr>
<td>Link is down</td>
</tr>
<tr>
<td>Link is Expired; LACPDUs are not being received from the partner</td>
</tr>
<tr>
<td>Link is in the process of being created</td>
</tr>
<tr>
<td>Link is marked as Standby by mLACP peer</td>
</tr>
<tr>
<td>Link is Not Aggregatable (reason unknown)</td>
</tr>
<tr>
<td>Link is not operational as a result of mLACP negotiations</td>
</tr>
<tr>
<td>Link is Standby; bundle has more links than are supported</td>
</tr>
<tr>
<td>Link is Standby due to maximum-active links configuration</td>
</tr>
<tr>
<td>Link is waiting for BFD session to start</td>
</tr>
<tr>
<td>Reason</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Loopback: Actor and Partner have the same System ID and Key</td>
</tr>
<tr>
<td>Not enough links available to meet minimum-active threshold</td>
</tr>
<tr>
<td>Partner has marked the link as Not Aggregatable</td>
</tr>
<tr>
<td>Partner has not advertised that it is Collecting</td>
</tr>
<tr>
<td>Partner has not echoed the correct parameters for this link</td>
</tr>
<tr>
<td>Partner is not Synchronized (Waiting, not Selected, or out-of-date)</td>
</tr>
<tr>
<td>Partner is not Synchronized (Waiting, Standby, or LAG ID mismatch)</td>
</tr>
<tr>
<td>Partner System ID/Key do not match that of the Selected links</td>
</tr>
<tr>
<td>Reason</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Wait-while timer is running</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (bundle), on page 509</td>
<td>Specifies or creates a new bundle and enters interface configuration mode for that bundle.</td>
</tr>
</tbody>
</table>
show bundle brief

To display summary information about all configured bundles, use the `show bundle brief` command in EXEC mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Information for all configured bundles is displayed.

**Command Modes**
EXEC mode

**Command History**
- **Release 4.0.0** This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- *Task ID*
- *Operation*
  - bundle
  - read

These examples show the status of two bundles, BE16 and BE100, that are configured on the router. Both are Ethernet bundles and only bundle 16 is Up:

```
RP/0/RSP0/CPU0:router# show bundle brief
Thu Mar 3 14:40:35.167 PST

Name  | IG  | State | LACP | BFD | Links | Local b/w, |
      |     |       |      |     |       | kbps      |
-------|------|-------|------|-----|-------|------------|
BE16   | - Up | On    | Off  | Off | 1 / 1 / 2 | 1000000    |
BE100  | - Down| Off   | Off  | Off | 0 / 0 / 0 | 0          |

Table 41: show bundle brief Field Descriptions, on page 548 describes the fields shown in the display.

**Table 41: show bundle brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name  | Abbreviated name of the bundle interface, with the following possible formats:  
  - BEx—Ethernet bundle with ID number x. |
<p>| IG    | Interchassis group ID (if configured) of which the bundle is a member. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| State | State of the bundle on the local device, with the following possible values:  
  • Admin down—The bundle has been configured to be shut down.  
  • Bundle shut—The bundle is holding all links in Standby state and will not support any traffic.  
  • Down—The bundle is operationally down. It has no Active members on the local device.  
  • mLACP cold standby—The bundle is acting as a multichassis LACP Standby device, but the higher layers are not synchronized.  
  • mLACP hot standby—The bundle is Up on the mLACP peer device, and the local device is ready to take over if that bundle goes down on the peer.  
  • Nak—The local and peer devices cannot resolve a configuration error.  
  • Partner down—The partner system indicates that the bundle is unable to forward traffic at its end.  
  • PE isolated—The bundle is isolated from the core.  
  • Up—The bundle has Active members on this device. |
| LACP  | Status of the Link Aggregation Control Protocol (LACP) on the bundle, with the following possible values:  
  • On—LACP is in use on the bundle.  
  • Off—LACP is not active. |
When BFD is enabled, displays the state of BFD sessions on the bundle from the sessions running on bundle members that is communicated to interested protocols, with the following possible values:

- **Down**—The configured minimum threshold for active links or bandwidth for BFD bundle members is not available so BFD sessions are down.
- **Off**—BFD is not configured on bundle members.
- **Up**—BFD sessions on bundle members are up because the minimum threshold for the number of active links or bandwidth is met.

### Links act/stby/cfgd

Number of links on the bundle with a particular status in the format `x/y/z`, with the following values:

- **x**—Number of links in Active state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle).
- **y**—Number of links in Standby state on the bundle for the local device (from 1 to the maximum number of links supported on the bundle).
- **z**—Total number of links configured on the bundle for the local device (from 1 to the maximum number of links supported on the bundle).

### Local b/w, kbps

Current bandwidth of the bundle on the local device (this effective bandwidth might be limited by configuration).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD</td>
<td>When BFD is enabled, displays the state of BFD sessions on the bundle from</td>
</tr>
<tr>
<td></td>
<td>the sessions running on bundle members that is communicated to interested</td>
</tr>
<tr>
<td></td>
<td>protocols, with the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• Down—The configured minimum threshold for active links or bandwidth</td>
</tr>
<tr>
<td></td>
<td>for BFD bundle members is not available so BFD sessions are down.</td>
</tr>
<tr>
<td></td>
<td>• Off—BFD is not configured on bundle members.</td>
</tr>
<tr>
<td></td>
<td>• Up—BFD sessions on bundle members are up because the minimum threshold</td>
</tr>
<tr>
<td></td>
<td>for the number of active links or bandwidth is met.</td>
</tr>
<tr>
<td>Links act/stby/cfgd</td>
<td>Number of links on the bundle with a particular status in the format <code>x/y/z</code></td>
</tr>
<tr>
<td></td>
<td>• x—Number of links in Active state on the bundle for the local device</td>
</tr>
<tr>
<td></td>
<td>(from 1 to the maximum number of links supported on the bundle).</td>
</tr>
<tr>
<td></td>
<td>• y—Number of links in Standby state on the bundle for the local device</td>
</tr>
<tr>
<td></td>
<td>(from 1 to the maximum number of links supported on the bundle).</td>
</tr>
<tr>
<td></td>
<td>• z—Total number of links configured on the bundle for the local device</td>
</tr>
<tr>
<td></td>
<td>(from 1 to the maximum number of links supported on the bundle).</td>
</tr>
<tr>
<td>Local b/w, kbps</td>
<td>Current bandwidth of the bundle on the local device (this effective</td>
</tr>
<tr>
<td></td>
<td>bandwidth might be limited by configuration).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
show bundle load-balancing

To display load balancing information, such as the ports, usage, weight, and distribution of traffic on individual members of a link bundle interface, use the `show bundle load-balancing` command in EXEC mode.

```
show bundle load-balancing [Bundle-Ether bundle-id] [Bundle-POS bundle-id] [brief] [detail] [location]
```

**Syntax Description**

- **Bundle-Ether bundle-id** (Optional) Specifies the number of the Ethernet bundle whose information you want to display. Range is 1 through 65535.
- **Bundle-POS bundle-id** (Optional) Specifies the number of the POS bundle whose information you want to display. Range is 1 through 65535.
- **brief** (Optional) Displays summary information for all nodes or for a specified location.
- **detail** (Optional) Displays detailed information for all nodes or for a specified location.
- **location** (Optional) Specifies the location of the node.
  
  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

When the **brief** or **detail** keywords are used and no **location** is specified, information is displayed for all nodes on the router.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>The <strong>Bundle-POS</strong> keyword was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to use the **show bundle load-balancing** command and its various keywords:

```
RP/0/RSP0/CPU0:router# show bundle load-balancing brief

Node: 0/0/CPU0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Sub-Intf</th>
<th>Member</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Count</td>
<td>Count</td>
<td>Wgt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers**

551
Bundle-Ether12345 10 63 134

show bundle load-balancing brief location 0/0/CPU0

Node: 0/0/CPU0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Count</th>
<th>Total Count</th>
<th>Wgt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether12345</td>
<td>10</td>
<td>63</td>
<td>134</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router# show bundle load-balancing location 0/0/CPU0

------------------------------------------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Bundle-Ether12345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: Ether (L2)</td>
</tr>
<tr>
<td>Members: 63</td>
</tr>
<tr>
<td>Total Weighting: 134</td>
</tr>
<tr>
<td>Sub-interfaces: 10</td>
</tr>
</tbody>
</table>

Member Information:

<table>
<thead>
<tr>
<th>Port ID</th>
<th>BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/1</td>
<td>0 10</td>
</tr>
<tr>
<td>Gi0/0/0/3</td>
<td>1 1</td>
</tr>
</tbody>
</table>
...

Platform Information:

Bundle Summary Information:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Ifhandle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether100</td>
<td>0xa0000a0</td>
</tr>
</tbody>
</table>

Virtual Port: 20
Local to LC: 1

Member Information:

<table>
<thead>
<tr>
<th>ul_id</th>
<th>Interface</th>
<th>ifhandle</th>
<th>SFP</th>
<th>port</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Gi0/0/0/3</td>
<td>0x8000100</td>
<td>16</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>Gi0/0/0/10</td>
<td>0x80002c0</td>
<td>17</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Gi0/0/0/17</td>
<td>0x8000480</td>
<td>17</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Gi0/0/0/24</td>
<td>0x8000640</td>
<td>18</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Bundle Table Information:

[NP 0]:

<table>
<thead>
<tr>
<th>idx</th>
<th>local</th>
<th>ul_id</th>
<th>SFP</th>
<th>port</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Show bundle load-balancing

Bundle-POS3
Type: POS (L3)
Members: 2
Total Weighting: 2
Sub-interfaces: 0

Member Information:
Port ID BW
------------ -- --
POS0/2/0/1 3 1
POS0/4/0/0 4 1

Bundle-Ether12345
Type: Ether (L2)
Members: 63
Total Weighting: 134
Sub-interfaces: 10

Member Information:
Port ID BW
------------ -- --
Gi0/0/0/1 0 10
Gi0/0/0/3 1 1

Sub-interface Information:
Sub-interface Type Load Balance
----------------------------- ---------
Bundle-Ether12345.4294967295 L2 Default
Bundle-Ether12345.2 L2 Hash: XID
Bundle-Ether12345.3 L2 Fixed: 2

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
show bundle load-balancing

Bundle-Ether12345
Type: Ether (L2)  
Members: 63  
Total Weighting: 134  
Sub-interfaces: 10

Sub-interface Information:
<table>
<thead>
<tr>
<th>Sub-interface</th>
<th>Type</th>
<th>Load Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether12345.2</td>
<td>L2</td>
<td>Hash: XID</td>
</tr>
</tbody>
</table>

Platform Information:

Bundle Summary Information:
<table>
<thead>
<tr>
<th>Interface</th>
<th>Ifhandle</th>
<th>Lag ID</th>
<th>Virtual Port</th>
<th>Number of Members</th>
<th>Local to LC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether100</td>
<td>0xa0000a0</td>
<td>1</td>
<td>20</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Member Information:
<table>
<thead>
<tr>
<th>ul_id</th>
<th>Interface</th>
<th>ifhandle</th>
<th>SFP</th>
<th>port</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Gi0/4/0/3</td>
<td>0x8000100</td>
<td>16</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>Gi0/4/0/10</td>
<td>0x80002c0</td>
<td>17</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Gi0/4/0/17</td>
<td>0x8000480</td>
<td>17</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Gi0/4/0/24</td>
<td>0x8000640</td>
<td>18</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Bundle Table Information:

[NP 0]:

<table>
<thead>
<tr>
<th>idx</th>
<th>local</th>
<th>ul_id</th>
<th>SFP</th>
<th>port</th>
<th>idx</th>
<th>local</th>
<th>ul_id</th>
<th>SFP</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>10</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>17</td>
<td>17</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>3</td>
<td>18</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>10</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>2</td>
<td>17</td>
<td>17</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>3</td>
<td>18</td>
<td>4</td>
<td>8</td>
<td>0</td>
<td>3</td>
<td>18</td>
<td>4</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle-hash, on page 489</td>
<td>Displays the source and destination IP addresses for the member links.</td>
</tr>
<tr>
<td>bundle load-balancing hash (EFP), on page 499</td>
<td>Configures all egress traffic on a particular subinterface of a bundle to flow through the same physical member link.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
show bundle replication bundle-ether

To display the replication status of a link bundle interface, use the show bundle replication bundle-ether command in EXEC mode.

```
show bundle replication bundle-ether bundle_id [all] [in-progress] [pending]
```

**Syntax Description**

- `all` Shows replication status for all nodes.
- `in-progress` Shows only nodes with replication in progress.
- `pending` Shows only nodes pending replication.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

Release 3.9.0 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

```
RP/0/RSP0/CPU0:router# show bundle replication bundle-ether 1 all
```
show iccp group

To display information for the ICCP parameters, use the `show iccp` command in EXEC mode.

`show iccp group {group-id | location node-id}`

**Syntax Description**

- **group-id**: ICCP group ID.
- **location**: Specifies the location.
- **node-id**: Node ID. The `node-id` argument is entered in the `rack/slot/module` notation.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **mpls-ip**: read

**Examples**

The following example shows the output of the `show iccp group` command:

```
RP/0/RSP0/CPU0:router#show iccp group

Redundancy Group 1
  member ip:2.2.2.2 (router2), up (connected)
  monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
  enabled applications: mLACP
  isolation recovery delay timer: 180 s, not running

Redundancy Group 2
  member ip:2.2.2.2 (router2), up (disconnected)
  monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
  enabled applications: mLACP
  isolation recovery delay timer: 180 s, not running

RP/0/RSP0/CPU0:router#show iccp group 1

Redundancy Group 1
  member ip:2.2.2.2 (router2), up (connected)
  monitor: route-watch (up)
  backbone interface Gi0/2/0/3: up
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
enabled applications: mLACP
isolation recovery delay timer: 180 s, not running
show lacp bundle

To display detailed information about Link Aggregation Control Protocol (LACP) ports and their peers, enter the **show lacp bundle** command in EXEC mode.

**show lacp bundle** {Bundle-Ether} bundle-id

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC mode</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>No specific guidelines impact the use of this command.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display LACP information for a specific Ethernet Bundle:

RP/0/RSP0/CPU0:router# **show lacp bundle Bundle-Ether 1**

Flags: A - Device is in Active mode. P - Device is in Passive mode.  
S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.  
D - Port is using default values for partner information  
E - Information about partner has expired

State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.  
2 - Port is In Sync with peer. 3 - Port is Collecting.  
4 - Port is Collecting and Distributing.

**Bundle-Ether1**

<table>
<thead>
<tr>
<th>Minimum active</th>
<th>Maximum active</th>
</tr>
</thead>
<tbody>
<tr>
<td>B/W (Kbps)</td>
<td>B/W (Kbps)</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>0</td>
<td>620000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Flags</th>
<th>Port ID</th>
<th>Key</th>
<th>System-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/2/0</td>
<td>1</td>
<td>ASDE</td>
<td>0x8000, 0x0001</td>
<td>0x8000, 08-00-45-3a-65-01</td>
<td></td>
</tr>
<tr>
<td>PEER</td>
<td>0</td>
<td>PSD</td>
<td>0xffff, 0x0000</td>
<td>0xffff, 00-00-00-00-00-00-00</td>
<td></td>
</tr>
</tbody>
</table>

**Table 42: show lacp bundle Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Flags | Describes the possible flags that may apply to a device or port, under the “Flags” field.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Describes the possible flags that may apply the port state, under the “State” field.</td>
</tr>
<tr>
<td>Port</td>
<td>Port identifier, in the rack/slot/module/port notation.</td>
</tr>
<tr>
<td>State</td>
<td>Provides information about the state of the specified port. Possible flags are:</td>
</tr>
<tr>
<td></td>
<td>• 0—Port is not aggregatable.</td>
</tr>
<tr>
<td></td>
<td>• 1—Port is out of sync with peer.</td>
</tr>
<tr>
<td></td>
<td>• 2—Port is in sync with peer.</td>
</tr>
<tr>
<td></td>
<td>• 3—Port is collecting.</td>
</tr>
<tr>
<td></td>
<td>• 4—Port is collecting and distributing.</td>
</tr>
<tr>
<td>Flags</td>
<td>Provides information about the state of the specified device or port. Possible flags are:</td>
</tr>
<tr>
<td></td>
<td>• A—Device is in Active mode.</td>
</tr>
<tr>
<td></td>
<td>• P—Device is in Passive mode.</td>
</tr>
<tr>
<td></td>
<td>• S—Device requests peer to send PDUs at a slow rate.</td>
</tr>
<tr>
<td></td>
<td>• F—Device requests peer to send PDUs at a fast rate.</td>
</tr>
<tr>
<td></td>
<td>• D—Port is using default values for partner information.</td>
</tr>
<tr>
<td></td>
<td>• E—Information about partner has expired.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port identifier, expressed in the format N_x_n_n. N is the port priority, and n_n_n is the port number assigned by the sending router.</td>
</tr>
<tr>
<td>Key</td>
<td>Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.</td>
</tr>
<tr>
<td>System-ID</td>
<td>System identifier. The system ID is a LACP property of the system which is transmitted within each LACP packet together with the details of the link.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle id, on page 495</td>
<td>Adds a port to an aggregated interface or bundle.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
**show lacp counters**

To display Link Aggregation Control Protocol (LACP) statistics, enter the `show lacp counters` command in EXEC mode.

```
show lacp counters  {Bundle-Ether}  bundle-id
```

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

- `bundle` read

**Examples**

The following example shows how to display LACP counters on an Ethernet bundle:

```
RP/0/RSP0/CPU0:router# show lacp counters bundle-ether 1
Bundle-Ether1
LACPDUs Marker
Port Sent Received Received Resp. Sent Last Cleared
Gi0/0/2/0 12 0 0 0 never

Port Excess Excess Pkt Errors
Gi0/0/2/0 0 0 0
```

**Table 43: show lacp counters Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACPDUs</td>
<td>Provides the following statistics for Link Aggregation Control Protocol data units (LACPDUs):</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Sent</td>
</tr>
<tr>
<td></td>
<td>• Received</td>
</tr>
<tr>
<td></td>
<td>• Last Cleared</td>
</tr>
<tr>
<td></td>
<td>• Excess</td>
</tr>
<tr>
<td></td>
<td>• Pkt Errors</td>
</tr>
</tbody>
</table>
The Marker Protocol is used by IEEE 802.3ad bundles to ensure that data no longer is transmitted on a link when a flow is redistributed away from that link.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lACP counters, on page 508</td>
<td>Clears LACP counters for all members of all bundles, all members of a specific bundle, or for a specific port.</td>
</tr>
</tbody>
</table>
show lacp io

To display the Link Aggregation Control Protocol (LACP) transmission information that used by the transmitting device for sending packets on an interface, use the `show lacp io` command in EXEC mode.

```
show lacp io {Bundle-Ether} bundle-id {GigabitEthernet | TenGigE} interface-path-id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Bundle-Ether bundle-id</th>
<th>GigabitEthernet</th>
<th>TenGigE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional) Displays information for the Ethernet bundle interface with the specified bundle-id. The range is 1 through 65535.</td>
<td>(Optional) Displays information for the Gigabit Ethernet interface with the specified interface-path-id.</td>
<td>(Optional) Displays information for the Ten Gigabit Ethernet interface with the specified interface-path-id.</td>
<td></td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
The default takes no parameters and displays information for all actively transmitting interfaces.

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command displays information only for interfaces that are actively transmitting packets.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to display Link Aggregation Control Protocol (LACP) information for the Ethernet bundle interface with bundle ID 28.

```
RP/0/RSP0/CPU0:router# show lacp io bundle-ether 28
Thu Jun 18 16:28:54:068 PST
Bundle-Ether28
Interface GigabitEthernet0/1/5/6
```
The following example shows how to display Link Aggregation Control Protocol (LACP) information for all actively transmitting interfaces:

RP/0/RSP0/CPU0# show lacp io

Thu Jun 18 16:33:57.330 PST

Bundle-Ether28

Interface GigabitEthernet0/1/5/6

Interface handle: 0x01180100
Interface media type: Ethernet
Fast periodic interval: 1000ms
Source MAC address: 0015.63c0.b3b8
Actor system: 0x8000, 00-15-63-c0-b0-04
Actor key: 0x001c
Actor port: 0x8000, 0x0001
Actor state:   Act (T/o) Agg Sync Coll Dist (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key: 0x001c
Partner port: 0x0001, 0x0003
Partner state: Act (T/o) Agg Sync Coll Dist (Def) (Exp)

Interface GigabitEthernet0/1/5/7

Interface handle: 0x01180120
Interface media type: Ethernet
Fast periodic interval: 1000ms
Source MAC address: 0015.63c0.b3b9
Actor system: 0x8000, 00-15-63-c0-b0-04
Actor key: 0x001c
Actor port: 0x8000, 0x0002
Actor state:   Act (T/o) Agg Sync (Coll) (Dist) (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key: 0x001c
Partner port: 0x0002, 0x0004
Partner state: Act (T/o) Agg (Sync) (Coll) (Dist) (Def) (Exp)
Actor state: Act (T/o) Agg Sync (Coll) (Dist) (Def) (Exp)
Partner system: 0x8000, 00-15-63-58-b9-04
Partner key: 0x001c
Partner port: 0x0002, 0x0004
Partner state: Act (T/o) Agg (Sync) (Coll) (Dist) (Def) (Exp)

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lACP packet-capture, on page 565</td>
<td>Displays the contents of LACP packets that are sent and received on an interface.</td>
</tr>
<tr>
<td>lACP period short, on page 519</td>
<td>Enables a short period time interval for the transmission and reception of LACP packets.</td>
</tr>
<tr>
<td>lACP packet-capture, on page 517</td>
<td>Captures LACP packets so that their information can be displayed.</td>
</tr>
</tbody>
</table>
show lacp packet-capture

To display the contents of Link Aggregation Control Protocol (LACP) packets that are sent and received on an interface, use the **show lacp packet-capture** command in EXEC mode.

```
show lacp packet-capture [decoded] [in | out] {GigabitEthernet | TenGigE} interface-path-id
```

**Syntax Description**

- **decoded** (Optional) Displays packet information in decoded form for the specified interface.
- **in** (Optional) Displays packet information for ingress packets only.
- **out** (Optional) Displays packet information for egress packets only.
- **GigabitEthernet** Displays packet information for the Gigabit Ethernet interface specified by `interface-path-id`.
- **TenGigE** Displays packet information for the Ten Gigabit Ethernet interface specified by `interface-path-id`.

**interface-path-id** Physical interface or virtual interface.

**Note**

- Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

The default displays both in and out information.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **lacp packet-capture** command captures transmit and receive packets on a single interface. The contents of these packets can then be displayed by the **show lacp packet-capture** command. If the **lacp packet-capture** command is not issued, the **show lacp packet-capture** command does not display any information.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to display the contents of an LACP packet, in hexadecimal, for a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/RSP0/CPU0# show lacp packet-capture gigabitethernet 0/1/0/0
```

```
Wed Apr 29 16:27:40.996 GMT
OUT Apr 29 17:05:50.123
------------------------
01 01 01 14 80 00 02 a7 4c 81 95 04 00 01 80 00 00 01 45 00
00 00 02 14 ff ff 00 00 00 00 00 00 ff ff 00 00 40 00
00 00 03 10 ff ff 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
OUT Apr 29 17:35:50.124
------------------------
...
```

The following example shows how to display the LACP parameters, decoded from individual packets, transmitted and received on a Gigabit Ethernet interface:

```
RP/0/RSP0/CPU0# lacp packet-capture gigabitethernet 0/1/0/0 100
RP/0/RSP0/CPU0# show lacp packet-capture decoded gigabitethernet 0/1/0/0
```

```
Subtype: 0x01 - LACP
Version: 1
TLV: 0x01 - Actor Information  Length: 20
System: Priority: 32768, ID: 02-a7-4c-81-95-04
Key: 0x0001, Port priority: 32768, Port ID: 1
State: Act (T/o) Agg (Sync) (Coll) (Dist) Def (Exp)

TLV: 0x02 - Partner Information  Length: 20
System: Priority: 65535, ID: 00-00-00-00-00-00
Key: 0x0000, Port priority: 65535, Port ID: 0
State: (Act) (T/o) (Agg) (Sync) (Coll) (Dist) Def (Exp)

TLV: 0x03 - Collector Information  Length: 16
```

Note

In the following example, after you issue the `lacp packet-capture` command, you must wait for a reasonable amount of time for the system to capture packets that are sent and received on the interface before you issue the `show lacp packet-capture` command. Otherwise, there is no information to display.
Max delay: 65535

TLV: 0x00 - TerminatorLength: 0

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lACP io</code>, on page 562</td>
<td>Displays the LACP transmission information that used by the transmitting device for sending packets on an interface.</td>
</tr>
<tr>
<td><code>lacp period short</code>, on page 519</td>
<td>Enables a short period time interval for the transmission and reception of LACP packets.</td>
</tr>
<tr>
<td><code>lacp packet-capture</code>, on page 517</td>
<td>Captures LACP packets so that their information can be displayed.</td>
</tr>
</tbody>
</table>
show lacp port

To display detailed information about Link Aggregation Control Protocol (LACP) ports, enter the `show lacp port` command in EXEC mode.

```
show lacp port [[[[GigabitEthernet | TenGigE]]] interface_instance]
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC mode</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 3.7.2 This command was introduced.</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>No specific guidelines impact the use of this command.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display LACP port information for all link bundles on a router:

```
RP/0/RSP0/CPU0:router# show lacp port
```

Flags: A - Device is in Active mode. P - Device is in Passive mode.
S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
D - Port is using default values for partner information
E - Information about partner has expired
State: 0 - Port is Not Aggregatable. 1 - Port is Out Of Sync with peer.
2 - Port is In Sync with peer. 3 - Port is Collecting.
4 - Port is Collecting and Distributing.

<table>
<thead>
<tr>
<th>Bundle-Ether1</th>
<th>Minimum active</th>
<th>Maximum active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B/W (Kbps)</td>
<td>MAC address</td>
</tr>
<tr>
<td></td>
<td>MAC address</td>
<td>B/W (Kbps)</td>
</tr>
<tr>
<td>0 0800.453a.651d</td>
<td>1 620000 32</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Flags</th>
<th>Port ID</th>
<th>Key</th>
<th>System-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>G10/0/2/0</td>
<td>1</td>
<td>ASDE</td>
<td>0x8000, 0x0001</td>
<td>0x0000</td>
<td>0x8000, 0x00-00-45-3a-65-01</td>
</tr>
<tr>
<td>PEER</td>
<td>0</td>
<td>PSD</td>
<td>0xffff, 0x0000</td>
<td>0x0000</td>
<td>0xffff, 0x00-00-00-00-00</td>
</tr>
</tbody>
</table>

### Table 44: show lacp port Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Identifies the LACP port whose information is displayed. The port number is expressed in the <code>rack/slot/module/port</code> notation.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
State | Provides information about the state of the specified device or port. Possible flags are:
  • 0—Port is not aggregatable.
  • 1—Port is out of sync with peer.
  • 2—Port is in sync with peer.
  • 3—Port is collecting.
  • 4—Port is collecting and distributing.
Flags | Provides information about the state of the specified port. Possible flags are:
  • A—Device is in Active mode.
  • P—Device is in Passive mode.
  • S—Device requests peer to send PDUs at a slow rate.
  • F—Device requests peer to send PDUs at a fast rate.
  • D—Port is using default values for partner information.
  • E—Information about partner has expired.
Port ID | Port identifier, expressed in the following format: $Nxnnn$. $N$ is the port priority, and $nnn$ is the port number assigned by the sending router.
Key | Two-byte number associated with the specified link and aggregator. Each port is assigned an operational key. The ability of one port to aggregate with another is summarized by this key. Ports which have the same key select the same bundled interface. The system ID, port ID and key combine to uniquely define a port within a LACP system.
System-ID | System identifier. The System ID is an LACP property of the system which is transmitted within each LACP packet together with the details of the link.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle id, on page 495</td>
<td>Adds a port to an aggregated interface or bundle.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
<tr>
<td>show lacp bundle, on page 558</td>
<td>Displays detailed information about LACP ports and their peers.</td>
</tr>
</tbody>
</table>
**show lacp system-id**

To display the local system ID used by the Link Aggregation Control Protocol (LACP), enter the `show lacp system-id` command in EXEC mode.

```
show lacp system-id
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The System ID and details about the specific link are transmitted within each LACP packet.

**Examples**

The following example shows how to display the system ID used by the LACP:

```
RP/0/RSP0/CPU0:router# show lacp system-id
Priority  MAC Address
---------  ---------------
0x8000     08-00-45-3a-65-01
```

**Table 45: show lacp system-id Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority for this system. A lower value is higher priority.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address associated with the LACP system ID.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle id, on page 495</td>
<td>Adds a port to an aggregated interface or bundle.</td>
</tr>
<tr>
<td>show bundle, on page 533</td>
<td>Displays information about configured bundles.</td>
</tr>
</tbody>
</table>
## Link Bundling Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lACP bundle, on page 558</td>
<td>Displays detailed information about LACP ports and their peers.</td>
</tr>
<tr>
<td>show lACP port, on page 568</td>
<td></td>
</tr>
</tbody>
</table>

*show lACP system-id*
# show mlacp

To display the MC-LAG information configured locally and for any connected mLACP peer devices, use the `show mlacp` command in the EXEC mode.

```
show mlacp [{Bundle-Ether interface-path-id | iccp-group group-id}] [{brief | verbose}]
```

## Syntax Description

- **Bundle-Ether interface-path-id**: Displays the information for the ICCP group of the bundle and only the specified bundle.
- **iccp-group group-id**: Displays information related to the ICCP group.
- **brief**: Displays only the ICCP group information without any bundle information.
- **verbose**: Displays the ICCP group, the bundle and member information.

## Command Default

No default behavior or values

## Command Modes

Exec

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>Read</td>
</tr>
</tbody>
</table>

## Examples

These examples display the MC-LAG information:

```
RP/0/RSP0/CPU0:router# show mlacp brief

ICCP Group 1
Connect timer: Off

<table>
<thead>
<tr>
<th>Node</th>
<th>LDP ID</th>
<th>State</th>
<th>System ID</th>
<th>Sync</th>
<th>Vers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.4.3.1</td>
<td>Up</td>
<td>0x0001,00-0d-00-0e-00-0f</td>
<td>Done 1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Local</td>
<td>Up</td>
<td>0x0001,00-0d-00-0e-00-0f</td>
<td>Done</td>
<td>-</td>
</tr>
</tbody>
</table>

RP/0/RP0/CPU0:poa2# show mlacp

ICCP Group 1
Connect timer: Off

<table>
<thead>
<tr>
<th>Node</th>
<th>LDP ID</th>
<th>State</th>
<th>System ID</th>
<th>Sync</th>
<th>Vers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Bundle-Ether1 (ROID: 0000.0001.0000.0000)

<table>
<thead>
<tr>
<th>Node</th>
<th>Aggregator Name</th>
<th>State</th>
<th>Agg ID</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BE1</td>
<td>Up</td>
<td>0x0001</td>
<td>00-0d-00-0e-00-0f</td>
</tr>
<tr>
<td>2</td>
<td>Bundle-Ether1</td>
<td>Up</td>
<td>0x0001</td>
<td>00-0d-00-0e-00-0f</td>
</tr>
</tbody>
</table>

RP/0/RP0/CPU0:router#show mlacp verbose

ICCP Group 1

Connect timer: Off

<table>
<thead>
<tr>
<th>Node</th>
<th>LDP ID</th>
<th>State</th>
<th>System ID</th>
<th>Sync</th>
<th>Vers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.4.3.1</td>
<td>Up</td>
<td>0x0001,00-0d-00-0e-00-0f</td>
<td>Done</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Local</td>
<td>Up</td>
<td>0x0001,00-0d-00-0e-00-0f</td>
<td>Done</td>
<td>-</td>
</tr>
</tbody>
</table>

Bundle-Ether1 (ROID: 0000.0001.0000.0000)

<table>
<thead>
<tr>
<th>Node</th>
<th>Aggregator Name</th>
<th>State</th>
<th>Agg ID</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BE1</td>
<td>Up</td>
<td>0x0001</td>
<td>00-0d-00-0e-00-0f</td>
</tr>
<tr>
<td>2</td>
<td>Bundle-Ether1</td>
<td>Up</td>
<td>0x0001</td>
<td>00-0d-00-0e-00-0f</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Node</th>
<th>Port Name</th>
<th>State</th>
<th>Port</th>
<th>Oper (Cfgd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gi0/1/0/3</td>
<td>Up</td>
<td>0x9001</td>
<td>0x03e8 (0x03e8)</td>
</tr>
<tr>
<td>2</td>
<td>Gi0/0/0/1</td>
<td>Up</td>
<td>0xa001</td>
<td>0x07d0 (0x07d0)</td>
</tr>
</tbody>
</table>
show mlacp counters

To display counters relating to mLACP information transferred to and from the local device, use the `show mlacp counters` command in the EXEC mode.

```
show mlacp counters [{bdl-info | ig-info | mbr-info [{bundle interface | member interface | iccp-group group-id | mlacp-device device-id | mlacp-interface foreign-member-interface}]}]
```

### Syntax Description

- **Bundle-Ether**
  - Displays the requested information associated with the bundle interface.
- **member interface**
  - Displays the requested information associated with the member interface.
- **counters**
  - Displays information on the mLACP counters.
- **bdl-info**
  - Displays the bundles counters.
- **ig-info**
  - Displays the ICCP group counters.
- **mbr-info**
  - Displays the member counters.
- **mlacp-device**
  - Displays the requested information associated with the mLACP device.

**Note**
The `mlacp-device` and `mlacp-interface` keywords are available only when mLACP devices and mLACP interfaces are configured.

- **mlacp-interface**
  - Displays the requested information associated with the mLACP interface.

### Command Default

No default behavior or values

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle</td>
<td>Read</td>
</tr>
</tbody>
</table>

### Examples

These examples display MC-LAG counter information:
The GigabitEthernet 0/0/0/1 is configured to Bundle-Ether 1 which is within ICCP Group1. Hence, the `show mlacp counters bdl-info GigabitEthernet 0/0/0/1` command displays the counters of the bundle that GigabitEthernet 0/0/0/1 is associated with (i.e. Bundle-Ether1). The `show mlacp counters mbr-info Bundle-Ether 1` displays the counters of the members that Bundle-Ether1 is associated with (locally: GigabitEthernet 0/0/0/1, and on the foreign device: GigabitEthernet 0/1/0/3).

---

**Note**

```
RP/0/RSP0/CPU0:router# show mlacp counters bdl-info GigabitEthernet 0/0/0/1
```

### ICCP Group 1

<table>
<thead>
<tr>
<th>Bundle</th>
<th>Config</th>
<th>TLVs Sent</th>
<th>TLVs Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle-Ether1</td>
<td>???????</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>mLACP Peer 5.4.3.1</td>
<td>???????</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

### Sync Requests

<table>
<thead>
<tr>
<th>Bundle</th>
<th>Sync Requests</th>
<th>Last Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle-Ether1</td>
<td>0</td>
<td>18m12s</td>
</tr>
<tr>
<td>mLACP Peer 5.4.3.1</td>
<td>0</td>
<td>17m57s</td>
</tr>
</tbody>
</table>

---

```
RP/0/0/CPU0:router#show mlacp counters mbr-info Bundle-Ether 1
```

### Bundle-Ether1 (ICCP Group 1)

<table>
<thead>
<tr>
<th>Port</th>
<th>Config</th>
<th>TLVs Sent</th>
<th>TLVs Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/1</td>
<td>???????</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mLACP Peer 5.4.3.1</td>
<td>???????</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

### Sync Requests

<table>
<thead>
<tr>
<th>Port</th>
<th>Sync Requests</th>
<th>Last Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All ports</td>
<td>0</td>
<td>19m3s</td>
</tr>
<tr>
<td>Gi0/0/0/1</td>
<td>0</td>
<td>19m3s</td>
</tr>
<tr>
<td>mLACP Peer 5.4.3.1</td>
<td>1</td>
<td>18m49s</td>
</tr>
</tbody>
</table>

---

---
show mlacp counters
Management Ethernet Interface Commands

This module provides command line interface (CLI) commands for configuring Management Ethernet interfaces on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- duplex (Management Ethernet), on page 578
- interface MgmtEth, on page 580
- ipv6 address autoconfig, on page 581
- mac-address (Management Ethernet), on page 583
- speed (Management Ethernet), on page 584
**duplex (Management Ethernet)**

To configure duplex mode operation on a Management Ethernet interface, use the `duplex` command in interface configuration mode. To return the interface to autonegotiated duplex mode, use the `no` form of the `duplex` command.

```
duplex {full}
```

**Syntax Description**

- `full` Configures the Management Ethernet interface to operate in full duplex mode.

  **Note** The system does not support half duplex on Management Ethernet interface.

**Command Default**

Autonegotiates duplex operation

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `interface` read, write

**Examples**

The following example shows how to configure the Management Ethernet interface to operate in full duplex mode:

```
RP/0/RSP0/CP00:router (config)# interface MgmtEth 0/RSP0/CP00/0
RP/0/RSP0/CP00:router (config-if)# duplex full
```

The following example shows how to configure the Management Ethernet interface to operate in half duplex mode:

```
RP/0/RSP0/CP00:router (config)# interface MgmtEth 0/RSP0/CP00/0
RP/0/RSP0/CP00:router (config-if)# duplex half
```

The following example shows how to return a Management Ethernet interface to autonegotiated duplex mode:

```
RP/0/RSP0/CP00:router (config)# interface MgmtEth 0/RSP0/CP00/0
RP/0/RSP0/CP00:router (config-if)# no duplex
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface MgmtEth, on page 580</td>
<td>Enters interface configuration mode for the Management Ethernet interface.</td>
</tr>
</tbody>
</table>
interface MgmtEth

To enter interface configuration mode for the Management Ethernet interface, use the `interface MgmtEth` command in Global Configuration mode. To delete a Management Ethernet interface configuration, use the `no` form of this command.

```
interface MgmtEth interface-path-id
```

**Syntax Description**

- `interface-path-id`: Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode

**Command History**

- **Release**
  - Release 3.7.2  This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

This example shows how to enter interface configuration mode for a Management Ethernet interface:

```
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-if)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>duplex (Management Ethernet), on page 578</code></td>
<td>Configures duplex mode operation on a Management Ethernet interface.</td>
</tr>
<tr>
<td><code>mac-address (Management Ethernet), on page 583</code></td>
<td>Sets the MAC layer address of a Management Ethernet interface.</td>
</tr>
<tr>
<td><code>speed (Management Ethernet), on page 584</code></td>
<td>Configures the speed for a Management Ethernet interface.</td>
</tr>
</tbody>
</table>
ipv6 address autoconfig

The `ipv6 address` command is used to configure IPv6 addresses or prefix on the interface. This command enables IPv6 processing on the interface. To remove all manually configured IPv6 addresses from an interface, use the `no ipv6 address` command without arguments.

```
ipv6 address { [ipv6addr] | [ipv6-prefix/prefix length] | [autoconfig] }
```

**Syntax Description**
- `ipv6addr` (Optional) Specify the IPv6 address.
- `ipv6-prefix/prefix length` (Optional) Specify the IPv6 prefix and the prefix length preceded by a slash `/`.
- `autoconfig` (Optional) Enable IPv6 Stateless Address Auto Configuration (SLAAC) on Management interface.

**Note** The `autoconfig` option is only available for Management Interfaces.

**Command Default**
No default behavior or values

**Command Modes**
Management Interface Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
In the `ipv6 address` interface configuration command, you can enter the `ipv6addr` or `ipv6-prefix/prefix length` variables with the address specified in hexadecimal using 16-bit values between colons. The `prefix length` variable (preceded by a slash `/`) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

The IPv6 Stateless Address Auto Configuration (SLAAC) is used to automatically assign IPv6 addresses to the host interfaces. This functionality can be used when the exact addresses used by the host need not be specific, as long as they are unique and can be properly routed. SLAAC helps in automating provisioning of the router. IPv6 auto configuration is disabled by default. To enable IPv6 SLAAC on Management interface, use the `ipv6 address autoconfig` command on the Management interface configuration mode.

**Task ID**
```
task id | operations
--------|----------------|
interface | read,
write
```

**Examples**
The following example shows how to configure the IPv6 address based on the IPv6 prefix 2001:0DB8:c18:1::/64:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/2/0/0
```
The following examples show how to enable IPv6 auto configuration on router:

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface mgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 address autoconfig

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface MgmtEth, on page 580</td>
<td>Enters interface configuration mode for the Management Ethernet interface.</td>
</tr>
</tbody>
</table>
mac-address (Management Ethernet)

To set the MAC layer address of a Management Ethernet interface, use the `mac-address` command in interface configuration mode. To return the interface to its default MAC address, use the `no` form of the `mac-address` command.

```
mac-address value1.value2.value3
```

**Syntax Description**

- `value1` High 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
- `value2` Middle 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.
- `value3` Low 2 bytes of the MAC address in hexadecimal. Range is from 0 to ffff.

**Command Default**
The default MAC address is read from the hardware burned-in address (BIA).

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The MAC address must be in the form of three 4-digit values (12 digits in dotted decimal notation).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the MAC address of the Management Ethernet interface located at 0/RSP0/CPU0/0:

```
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# mac-address 0001.2468.ABCD
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface MgmtEth, on page 580</td>
<td>Enters interface configuration mode for the Management Ethernet interface.</td>
</tr>
</tbody>
</table>
speed (Management Ethernet)

To configure the speed for a Management Ethernet interface, enter the speed command in interface configuration mode. To return the system to autonegotiate speed, use the no form of the speed command.

```
speed {10 | 100 | 1000}
```

**Syntax Description**

- `10` Configures the interface to transmit at 10 Mbps.
- `100` Configures the interface to transmit at 100 Mbps.
- `1000` Configures the interface to transmit at 1000 Mbps (1 Gbps).

**Command Default**

Interface speed is autonegotiated.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Keep in mind that both ends of a link must have the same interface speed. A manually configured interface speed overrides any autonegotiated speed, which can prevent a link from coming up if the configured interface speed at one end of a link is different from the interface speed on the other end.

Table 46: Relationship Between duplex and speed Commands, on page 584 describes the performance of the system for different combinations of the duplex and speed modes. The specified duplex command configured with the specified speed command produces the resulting system action.

**Table 46: Relationship Between duplex and speed Commands**

<table>
<thead>
<tr>
<th>duplex Command</th>
<th>speed Command</th>
<th>Resulting System Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>no duplex</td>
<td>no speed</td>
<td>Autonegotiates both speed and duplex modes.</td>
</tr>
<tr>
<td>no duplex</td>
<td>speed 1000</td>
<td>Forces 1000 Mbps (1 Gbps) and full duplex.</td>
</tr>
<tr>
<td>no duplex</td>
<td>speed 100</td>
<td>Autonegotiates for duplex mode and forces 100 Mbps.</td>
</tr>
<tr>
<td>no duplex</td>
<td>speed 10</td>
<td>Autonegotiates for duplex mode and forces 10 Mbps.</td>
</tr>
<tr>
<td>duplex full</td>
<td>no speed</td>
<td>Forces full duplex and autonegotiates for speed.</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 1000</td>
<td>Forces 1000 Mbps (1 Gbps) and full duplex.</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 100</td>
<td>Forces 100 Mbps and full duplex.</td>
</tr>
</tbody>
</table>
### Resulting System Action

<table>
<thead>
<tr>
<th>duplex Command</th>
<th>speed Command</th>
<th>Resulting System Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplex full</td>
<td>speed 10</td>
<td>Forces 10 Mbps and full duplex.</td>
</tr>
<tr>
<td>duplex half</td>
<td>no speed</td>
<td>Forces half duplex and autonegotiates for speed (10 or 100 Mbps.)</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 100</td>
<td>Forces 100 Mbps and half duplex.</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 10</td>
<td>Forces 10 Mbps and half duplex.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure the Management Ethernet interface to transmit at one gigabit:

```
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# speed 1000
```
speed (Management Ethernet)
Multilink Commands

This module provides command line interface (CLI) commands for configuring multilink interfaces on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- bundle, on page 588
- controller MgmtMultilink, on page 589
- interface multilink, on page 591
- multilink, on page 593
- multilink fragment, on page 594
- multilink group, on page 595
- show controllers mgmtmultilink, on page 596
- show interfaces multilink, on page 599
**bundle**

To create a multilink interface bundle, use the `bundle` command in the interface configuration mode. To remove a multilink interface bundle, use the `no` form of this command.

```
bundle bundleID
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bundleID</code></td>
<td>ID number of the multilink interface bundle. The bundle ID can be a 9-digit number.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `bundle` command is used in mgmtmultilink controller mode to dynamically create a multilink interface. This command is similar to the `channel-group` command on the T1 controller, which dynamically creates a serial interface.

**Examples**

The following example shows how to create a multilink interface with a bundle ID of 1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0
RP/0/RSP0/CPU0:router(config-mgmtmultilink)# bundle 1
RP/0/RSP0/CPU0:router(config-mgmtmultilink)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>multilink, on page 593</code></td>
<td>Enters the config-if-multilink submode.</td>
</tr>
<tr>
<td><code>multilink group, on page 595</code></td>
<td>Attaches a serial interface to a multilink interface bundle.</td>
</tr>
</tbody>
</table>
controller MgmtMultilink

To configure a controller for a generic multilink bundle and enter MgmtMultilink configuration mode, use the `controller MgmtMultilink` command in Global Configuration mode. To return to the default state, use the `no` form of this command.

```plaintext
controller MgmtMultilink interface-path-id
```

**Syntax Description**

- `interface-path-id`  Virtual interface.

  **Note**  Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (```?```), online help function.

**Command Default**  
No default behavior or values

**Command Modes**  
Global Configuration mode

**Command History**  

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module-instance`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number.
  - `instance`: Number of the controller instance. The instance is always 0.

- If specifying a virtual interface, the number range varies, depending on interface type.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the MgmtMultilink configuration mode:
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# controller MgmtMultilink 0/1/0/0
RP/0/RSP0/CPU0:router(config-mgmtmultilink)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controllers mgmtmultilink, on page 596</td>
<td>Displays information about the state and the number of bundles of a multi-link controller.</td>
</tr>
</tbody>
</table>
interface multilink

To configure a multilink interface and enter multilink interface configuration mode, use the `interface multilink` command in Global Configuration mode. To delete the interface configuration, use the `no` form of this command. To return to the default state, use the `no` form of this command.

```
interface multilink interface-path-id[.subinterface{12transport | point-to-point}]
```

**Syntax Description**

```
interface-path-id [.subinterface]  Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is interface-path-id.subinterface. The period in front of the subinterface value is required as part of the notation.

For more information about the syntax for the router, use the question mark (?) online help function.

12transport  Configures interface to function as one endpoint on a Layer 2 link.

point-to-point  Configures interface to function as one endpoint on a point-to-point link.
```

**Command Default**

No interfaces are configured.

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The <code>subinterface</code> argument and the keywords <code>12transport</code> and <code>point-to-point</code> were introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `subinterface` argument and keywords `12transport` and `point-to-point` are only applicable if frame relay encapsulation is enabled using the `encapsulation frame-relay` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable frame relay encapsulation for a multilink bundle, and enter subinterface configuration mode.

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# interface multilink 0/3/0/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation frame-relay
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# interface multilink 0/3/0/0/1.1 point-to-point
RP/0/RSP0/CPU0:router(config-subif)# ipv4 address 10.86.10.48/24
```
The following example shows how to enter interface configuration mode for a multilink bundle with ppp encapsulation. ppp encapsulation is the default encapsulation type:

RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# interface multilink 0/3/0/0/1
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.86.10.48/24

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show interfaces multilink, on page 599</td>
<td>Displays information about a multilink interface.</td>
</tr>
</tbody>
</table>
multilink

To enter the config-if-multilink submode, use the **multilink** command in the interface configuration mode.

```
multilink
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For multilink interfaces, the **multilink** command provides access to the config-if-multilink submode to use the **multilink fragment-size** command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the config-if-multilink submode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1/1:0
RP/0/RSP0/CPU0:router(config-if)# multilink
RP/0/RSP0/CPU0:router(config-if-multilink)# group 1
RP/0/RSP0/CPU0:router(config-if-multilink)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multilink group, on page 595</td>
<td>Attaches a serial interface to a multilink interface bundle.</td>
</tr>
</tbody>
</table>
multilink fragment

To set the fragmentation size or the fragmentation delay on a multilink interface, use the `multilink fragment` command in interface configuration mode. To remove the fragment size or fragment delay, use the `no` form of this command.

```
multilink fragment {size size | delay delay-ms}
```

**Syntax Description**

- **size**
  - Specifies the fragment size (in bytes) on a multilink interface. The range is 64 to 9216.

- **delay**
  - Specifies the fragment delay (in milliseconds) on a multilink interface. The range is 1 to 1000.

**Command Default**

No multilink fragment size or fragment delay is set.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Multilink fragmentation is only supported for ppp encapsulation, not for frame-relay encapsulation.

**Task ID**

- **hdlc**
  - read, write

**Examples**

The following example shows how to set the multilink fragment size:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# multilink fragment size 128
```

The following example shows how to set the multilink fragment delay:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# multilink fragment delay 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface multilink</code>, on page 591</td>
<td>Configures a multilink interface and enters multilink interface configuration mode.</td>
</tr>
</tbody>
</table>
multilink group

To attach a serial interface to a multilink interface bundle, use the `multilink group` command in interface configuration mode. To remove a serial interface from a multilink interface bundle, use the `no` form of this command.

```
multilink group bundleID
```

**Syntax Description**

- `bundleID`: Bundle ID number of the multilink interface, in the format `rack/slot/bay/controllerID/bundleID`.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following examples show how to attach a serial interface to a multilink interface bundle:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1/1:0
RP/0/RSP0/CPU0:router(config-if)# multilink group 1
RP/0/RSP0/CPU0:router(config-if)# commit
```

or

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1/1:0
RP/0/RSP0/CPU0:router(config-if)# multilink
RP/0/RSP0/CPU0:router(config-if-multilink)# group 1
(config-if-multilink)# commit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multilink, on page 593</td>
<td>Enters the config-if-multilink submode.</td>
</tr>
</tbody>
</table>
show controllers mgmtmultilink

To display information about the state and the number of bundles of a multilink controller, use the show controller mgmtmultilink command in EXEC mode.

```
show controllers mgmtmultilink interface-path-id [all | brief | internal-state | tabular]
```

Syntax Description

interface-path-id Virtual interface.

Note Use the show interfaces command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**all** Displays all multilink management information.

**brief** Displays brief multilink management information.

**internal-state** Displays internal multilink management state.

**tabular** Displays multilink management information in tabular format.

Command Default

No default behavior or values

Command Modes

EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For the interface-path-id argument, use the following guidelines:

- If specifying a physical interface, the naming notation is rack/slot/module.instance. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number. A physical layer interface module (PLIM) is always 0.
  - **instance**: Number of the controller instance. The instance is always 0.

- If specifying a virtual interface, the number range varies, depending on interface type.
The following example shows how to display information for a management multilink controller:

```
RP/0/RSP0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 all

Controller MgmtMultilink0/3/0/0
State is up
Number of bundles: 2
  Bundle 1 - Multilink0/3/0/0/1 (0x06186240)
    Type: Full Framed T1s
    Bandwidth: 3072 kbps
    Encapsulation: Frame Relay
    Fragment size: 0
    Number of members: 2
    Ancestor name: SONET0/3/0/0
    Member(s):
      Serial0/3/0/0/1:0 (0x0619b640) Active
      Serial0/3/0/0/1:2:0 (0x06176980) Active

  Bundle 2 - Multilink0/3/0/0/2 (0x06176840)
    Type: Full Framed T1s
    Bandwidth: 3072 kbps
    Encapsulation: Frame Relay
    Fragment size: 0
    Number of members: 2
    Ancestor name: SONET0/3/0/0
    Member(s):
      Serial0/3/0/0/1:3:0 (0x0619b3c0) Active
      Serial0/3/0/0/1:4:0 (0x0618b9c0) Active

RP/0/RSP0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 brief

MgmtMultilink0/3/0/0 is up

RP/0/RSP0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 tabular

MgmtMultilink0/3/0/0 is up

RP/0/RSP0/CPU0:router# show controllers mgmtmultilink 0/3/0/0 internal-state

Interface(layer) admin_up if_state
--------------------- -------- --------
MgmtMultilink0/3/0/0 up up

RP/0/RSP0/CPU0:router# show controllers mgmtmultilink 0/2/0/0

Controller MgmtMultilink0/2/0/0
State is up
Number of bundles: 1
  Bundle 1 - Multilink0/2/0/0/1 (0x0802e400)
    Type: Full Framed T1s
    Bandwidth: 1536 kbps
    Encapsulation: PPP
    Fragment size: 0
    Number of members: 1
    Ancestor name: SONET0/2/0/0
```
Member(s):
Serial0/2/0/0/1/1:0 (0x08023c00) Active

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show interfaces multilink, on page 599</td>
<td>Displays information about a multilink interface.</td>
</tr>
</tbody>
</table>
show interfaces multilink

To display information about a multilink interface, use the show interfaces multilink command in EXEC mode mode.

```
show interfaces multilink interface-path-id
```

### Syntax Description
- **interface-path-id**
  - Physical interface or virtual interface.

  **Note**
  - Use the show interfaces command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

### Command Default
- No default behavior or values

### Command Modes
- EXEC mode

### Command History
- **Release**
  - 3.9.0

  **Modification**
  - This command was introduced.

### Usage Guidelines
For the **interface-path-id** argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number. A physical layer interface module (PLIM) is always 0.
  - **port**: Physical port number of the interface.
  - If specifying a virtual interface, the number range varies, depending on interface type.

### Task ID
- **Task ID**
  - read

### Examples
The following example shows how to display information about a multilink interface:

```
RP/0/RSP0/CPU0:router# show interfaces multilink 0/1/0/0/1
Multilink0/1/0/0/1 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Multilink network interface(s)
```
Internet address is 10.1.1.1/24
MTU 1504 bytes, BW 1536 Kbit
   reliability 255/255, txload 3/255, rxload 3/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 02:06:24
5 minute input rate 19000 bits/sec, 5 packets/sec
5 minute output rate 19000 bits/sec, 5 packets/sec
   48769 packets input, 12425740 bytes, 0 total input drops
   0 drops for unrecognized upper-level protocol
   Received 0 runts, 0 giants, 0 throttles, 0 parity
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   67905 packets output, 17400050 bytes, 0 total output drops
   0 output errors, 0 underruns, 0 applique, 0 resets
   0 output buffer failures, 0 output buffers swapped out
Fragmentation Statistics
   Input Fragmented packets 0       Input Fragmented bytes 0
   Output Fragmented packets 0      Output Fragmented bytes 0
   Input Unfragmented packets 0     Input Unfragmented bytes 0
   Output Unfragmented packets 0    Output Unfragmented bytes 0
   Input Reassembled packets 0     Input Reassembled bytes 0
Packet-over-SONET Interface Commands

This module provides command line interface (CLI) commands for configuring Packet-over-SONET/SDH (POS) on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

This module describes the Cisco IOS XR commands used to configure, monitor, and troubleshoot Packet-over-SONET/SDH (POS).

POS provides a method for efficiently carrying data packets in SONET or Synchronous Digital Hierarchy (SDH) frames. High-bandwidth capacity and efficient link utilization are characteristics that make POS largely preferred for building the core of data networks. POS uses PPP in High-Level Data Link Control (HDLC)-like framing for data encapsulation at Layer 2 (data link) of the Open System Interconnection (OSI) stack. This method provides efficient packet delineation and error control.

In addition to high-bandwidth efficiency, POS offers secure and reliable transmission for data. Reliable data transfer depends on timing integrity.

The real-time POS functionality is performed in hardware, according to the hardware configuration setup. Configured hardware events are detected by the framer application-specific integrated circuits (ASICs) and the control is passed to the software. The generic POS driver is responsible for providing a mechanism to configure the hardware on a per-interface basis, to handle interface state transitions, and to collect POS-related statistics.

- crc (POS), on page 602
- encapsulation (POS), on page 603
- interface pos, on page 604
- keepalive (POS), on page 606
- pos, on page 608
- show interfaces pos, on page 610
- transmit-delay, on page 613
To set the length of the cyclic redundancy check (CRC) on a Packet-over-SONET/SDH (POS) interface, use the `crc` command in POS configuration mode. To return the CRC setting on a POS interface to the 32-bit default setting, use the `no` form of this command.

```
crc {16 | 32}
```

**Syntax Description**

- `16` Sets 16-bit CRC mode.
- `32` Sets 32-bit CRC mode. The default is 32 bits.

**Command Default**

The default CRC mode is 32 bits.

**Command Modes**

POS configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>pos-dpt</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In this example, the 32-bit CRC on POS interface 0/1/0/2 is enabled:

```
rack/slot/module(config)# interface POS 0/1/0/2
rack/slot/module(config-if)# POS
rack/slot/module(config-if-pos)# crc 32
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit-delay, on page 613</td>
<td>Specifies a number of flag sequences to be inserted between the packets.</td>
</tr>
</tbody>
</table>
encapsulation (POS)

To set the Layer 2 encapsulation of an interface, use the `encapsulation` command in interface configuration mode. To restore the system to the default encapsulation, use the `no` form of this command.

```
encapsulation {hdlc | ppp | frame-relay [ietf] }
```

**Syntax Description**
- `hdlc`: Enables Cisco High-Level Data Link Control (cHDLC) encapsulation on the interface. This is the default encapsulation type.
- `ppp`: Enables Point-to-Point Protocol (PPP) encapsulation on the interface.
- `frame-relay` (Optional): Enables Frame Relay encapsulation on the interface.
- `ietf` (Optional): Enables RFC1490/RFC2427 encapsulation.

**Command Default**
For Packet-over-SONET/SDH (POS) interfaces, the default encapsulation is HDLC.

**Command Modes**
Interface configuration

**Command History**
```
Release   Modification
---------  ------------
Release 4.0.0  This command was introduced.
```

**Usage Guidelines**
The task ID `hdlc` (r,w) is required for use of the keyword `hdlc`. The task ID `ppp(r,w)` is required for use of the keyword `ppp`. The task ID `fr(r,w)` is required for use of the keyword `frame-relay`.

**Task ID**
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc OR ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>fr</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
In this example, PPP encapsulation is set on POS interface 0/3/0/1:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces pos</code>, on page 610</td>
<td>Displays information about a POS interface.</td>
</tr>
<tr>
<td><code>show ppp interfaces (BNG)</code>, on page 655</td>
<td>Displays PPP state information for an interface.</td>
</tr>
</tbody>
</table>
interface pos

To enter interface or subinterface configuration mode for a POS interface or subinterface, use the `interface pos` command in Global Configuration mode. To delete a POS configuration, use the `no` form of this command.

```
interface pos  interface-path-id[.subinterface] {l2 transport | point-to-point}
```

**Syntax Description**

- `interface-path-id`: Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is `interface-path-id.subinterface`. The period in front of the subinterface value is required as part of the notation.

  For more information about the syntax for the router, use the question mark (?) online help function.

- `l2transport`: (Optional) Configures the interface to function as an attachment circuit (AC) on one endpoint of a Layer 2 link.

- `point-to-point`: (Optional) Configures interface to function as one endpoint of a point-to-point link.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Subinterfaces of a POS interface can only be configured using the `l2transport` keyword, if Frame Relay encapsulation is configured on the POS interface, using the `encapsulation frame-relay` command. Interfaces configured to use HDLC or PPP encapsulation cannot be configured using the `l2transport` keyword.

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to enter interface configuration mode for a POS interface:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)#
```

The following example shows how to create a subinterface on a POS interface in slot 1, subslot 1, port 2 and enter subinterface configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/2.1
RP/0/RSP0/CPU0:router(config-subif)#
```

The following example shows how to configure frame-relay encapsulation on the main POS interface before being able to configure an AC subinterface:

```
RP/0/RSP0/CPU0:router# interface pos 0/1/0
RP/0/RSP0/CPU0:router(config-if)# encapsulation frame-relay
RP/0/RSP0/CPU0:router(config-if)# commit
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/0.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# commit
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces pos, on page 610</td>
<td>Displays information about a POS interface.</td>
</tr>
</tbody>
</table>
keepalive (POS)

To set the keepalive timer for a specific interface, use the `keepalive` command in interface configuration mode. To reset the keepalive timer to the default of 10 seconds, use the `no` form of this command.

```
keepalive {interval [retry] | disable}
```

**Syntax Description**

- **interval** Number of seconds (from 1 to 30) between keepalive messages. The default is 10.
- **retry** (Optional) Number of keepalive messages (from 1 to 255) that can be sent to a peer without a response before transitioning the link to the down state. The default is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation.
- **disable** Turns off the keepalive timer.

**Command Default**
The default interval is 10 seconds between keepalive messages. The default number of retry keepalive messages that can be sent without a response is 5 for interfaces with PPP encapsulation, and 3 for interfaces with HDLC encapsulation. However, when more than 5 (or 3) keepalive messages are sent to a peer without a response, the link transitions to the down state.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

HDLC keepalives require that the `keepalive` command is configured the same way on both routers. The two connected routers have no way of negotiating the keepalive value, because there is no way for the routers to tell each other what their configured values are. The keepalive value configured on each router (local and partner) sets the rate at which the Cisco IOS XR software sends packets. It also sets the rate at which the local end expects to receive incoming packets.

To set the keepalive value to the default value, use the `keepalive` command without specifying a value for the `seconds` argument.

If three keepalives are sent to the peer and no response is received from the peer, then the link makes the transition to the down state.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure keepalives for 3 seconds on POS interface 0/7/0/1:
RP/0/RSP0/CPU0:router(config)# interface POS 0/7/0/1
RP/0/RSP0/CPU0:router(config-if)# keepalive 3
To access the POS configuration submode, use the `pos` command in interface configuration mode.

**pos**

**Command Default**
No default behavior or values

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 4.0.0</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you issue the `pos` command in interface configuration mode for a POS interface, the CLI prompt changes to “config-if-pos” indicating that you have entered POS configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under POS configuration submode:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RSP0/CPU0:router(config-if)# POS
RP/0/RSP0/CPU0:router(config-if-pos)# ?
```

- **commit**: Commit the configuration changes to running
- **crc**: Set the CRC on a POS interface
- **describe**: Describe a command without taking real actions
- **do**: Run an exec command
- **exit**: Exit from this submode
- **no**: Negate a command or set its defaults
- **show**: Show contents of configuration
- **transmit-delay**: Set POS transmit delay on an interface

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>pos-dpt</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to access the POS configuration submode from the POS configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RSP0/CPU0:router(config-if)# POS
RP/0/RSP0/CPU0:router(config-if-pos)#
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crc (POS), on page 602</td>
<td>Sets the length of the CRC on a Packet-over-SONET/SDH (POS) interface.</td>
</tr>
<tr>
<td></td>
<td>transmit-delay, on page 613</td>
<td>Specifies a number of flag sequences to be inserted between the packets.</td>
</tr>
</tbody>
</table>
show interfaces pos

To display information about a POS interface, use the show interfaces pos command in EXEC mode.

```
show interfaces pos interface-path-id  [{accounting [rates] | brief | description | detail}] [location node-id]
```

**Syntax Description**

- `interface-path-id` (Optional) Physical interface or virtual interface.

  **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- `accounting` (Optional) Displays accounting information for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.

- `rates` (Optional) Displays interface accounting rates for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.

- `brief` (Optional) Displays brief output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.

- `description` Displays descriptive output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.

- `detail` (Optional) Displays detailed output for all POS interfaces on the router, for a specific POS interface instance, or for all POS interfaces on a specific node.

- `location node-id` (Optional) Displays detailed POS information for the designated node. The `node-id` argument is entered in the rack/slot/module notation.

**Command Default**

Enter the show interfaces pos command without including any of the optional keywords or arguments to display detailed information about all POS interfaces configured on the router.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
• **port**: Physical port number of the interface.

• If specifying a virtual interface, the number range varies, depending on interface type.

### Task ID Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display summarized information for a POS interface on a specific node:

```
RP/0/RSP0/CPU0:router# show interfaces pos summary location 0/1/CPU0
```

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Total</th>
<th>UP</th>
<th>Down</th>
<th>Admin Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------------</td>
<td>-------</td>
<td>----</td>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>ALL TYPES</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>IFT_POS</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Table 47: show interfaces pos summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Type</td>
<td>Type of interface described in the display.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of configured interfaces of the specified type.</td>
</tr>
<tr>
<td>Up</td>
<td>Number of interfaces of the specified type that are in the “Up” state.</td>
</tr>
<tr>
<td>Down</td>
<td>Number of interfaces of the specified type that are in the “Down” state.</td>
</tr>
<tr>
<td>Admin Down</td>
<td>Number of interfaces of the specified type that are in the “Admin Down” state.</td>
</tr>
</tbody>
</table>

The following example shows how to display brief information for a specific POS interface:

```
RP/0/RSP0/CPU0:router# show interfaces pos 0/2/0/0 brief
```

<table>
<thead>
<tr>
<th>Intf Name</th>
<th>Intf State</th>
<th>LineP State</th>
<th>Encap</th>
<th>MTU</th>
<th>BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO0/2/0/0</td>
<td>admin-down</td>
<td>admin-down</td>
<td>HDLC</td>
<td>4474</td>
<td>2488320</td>
</tr>
</tbody>
</table>

**Table 48: show interfaces pos Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf Name</td>
<td>Interface identifier, in the type*rack/slot/module/port notation.</td>
</tr>
<tr>
<td>Intf State</td>
<td>Indicates whether the interface is in the admin-up or admin down state.</td>
</tr>
<tr>
<td>LineP State</td>
<td>Line protocol state.</td>
</tr>
</tbody>
</table>
### Field and Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encap Type</td>
<td>Encapsulation type for the specified interface. Can be HDLC or PPP.</td>
</tr>
<tr>
<td>MTU (byte)</td>
<td>Maximum transmission unit (MTU) value configured for the specified interface, in bytes.</td>
</tr>
<tr>
<td>BW (Kbps)</td>
<td>Bandwidth of the interface, in kbps.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers pos, on page 769</td>
<td>Displays information on the POS controllers.</td>
</tr>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
transmit-delay

To specify a number of flag sequences to be inserted between the packets, use the **transmit-delay** command in POS configuration mode. To restore the default, use the no form of this command.

**transmit-delay  microseconds**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>microseconds</strong> Number of microseconds of minimum delay after sending a packet. Range is from 0 to 1023. Default is 0 (disabled).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>microseconds</strong> = 0 (disabled)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Releases</strong>  <strong>Modifications</strong></td>
</tr>
<tr>
<td>Release 4.0.0  This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>No specific guidelines impact the use of this command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task ID</strong></td>
</tr>
<tr>
<td>pos-dpt</td>
</tr>
<tr>
<td>read, write</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
</table>

In the following example, a delay of 2 microseconds is specified on POS interface 0/1/0/2:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RSP0/CPU0:router(config-if)# pos
RP/0/RSP0/CPU0:router(config-if-pos)# transmit-delay 2
```

In the following example, the transmit delay on POS interface 0/1/0/2 is disabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RSP0/CPU0:router(config-if)# pos
RP/0/RSP0/CPU0:router(config-if-pos)# no transmit-delay
```

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>show interfaces</td>
</tr>
</tbody>
</table>
transmit-delay
PPP Commands

This module provides command line interface (CLI) commands for configuring Point-to-Point Protocol (PPP) on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

Point-to-Point Protocol (PPP) is an encapsulation scheme that can be used on Packet-over-SONET (POS), serial, and multilink interfaces. PPP is a standard protocol used to send data over synchronous serial links. PPP also provides a Link Control Protocol (LCP) for negotiating properties of the link. LCP uses echo requests and responses to monitor the continuing availability of the link.

PPP provides the following Network Control Protocols (NCPs) for negotiating properties of data protocols that will run on the link:

- Cisco Discovery Protocol Control Protocol (CDPCP) to negotiate CDP properties
- IP Control Protocol (IPCP) to negotiate IP properties
- IP Version 6 Control Protocol (IPv6CP) to negotiate IPv6 properties
- Multiprotocol Label Switching Control Protocol (MPLSCP) to negotiate MPLS properties
- Open System Interconnection Control Protocol (OSICP) to negotiate OSI properties

- clear ppp sso state, on page 617
- clear ppp statistics, on page 618
- encapsulation ppp, on page 619
- group, on page 620
- multi-router aps, on page 621
- peer ipv4 address, on page 622
- ppp authentication (BNG), on page 623
- ppp chap password, on page 626
- ppp chap refuse, on page 628
- ppp ipcp dns, on page 630
- ppp ipcp neighbor-route disable, on page 631
- ppp ipcp peer-address default, on page 632
- ppp max-bad-auth (BNG), on page 633
- ppp max-configure (BNG), on page 635
- ppp max-failure (BNG), on page 637
- ppp max-terminate, on page 639
• ppp ms-chap hostname, on page 640
• ppp ms-chap password, on page 641
• ppp ms-chap refuse, on page 642
• ppp multilink multiclass, on page 643
• ppp multilink multiclass local, on page 644
• ppp multilink multiclass remote apply, on page 645
• ppp pap refuse, on page 646
• ppp pap sent-username password, on page 648
• ppp timeout authentication, on page 650
• ppp timeout retry, on page 652
• redundancy, on page 653
• security ttl, on page 654
• show ppp interfaces (BNG), on page 655
• show ppp sso alerts, on page 661
• show ppp sso state, on page 662
• show ppp sso summary, on page 664
• ssrp group, on page 666
• ssrp location, on page 667
• ssrp profile, on page 668
clear ppp sso state

To clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for the specified standby interface or for all interfaces on the specified node, use the clear ppp sso state command in EXEC mode.

```
clear ppp sso state {interface interface-path-id | all} location node-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-path-id</td>
<td>Physical interface or virtual interface. Note: Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>all location node-id</td>
<td>Specifies the full qualified path of a specific node in the format rack/slot/module.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command sets the PPP sessions in the Standby-Up state to the Standby-Down state. All replicated data received from the peer is purged, and SSRP Request messages are re-sent to the peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the replicated ICSSO states for the specified standby interface:

```
RP/0/RSP0/CPU0:router# clear ppp sso state interface 0/1/0/1
```

The following example shows how to clear the replicated Inter-Chassis Stateful Switchover (ICSSO) states for all interfaces on the specified node:

```
RP/0/RSP0/CPU0:router# clear ppp sso state all location 1/0/1
```
clear ppp statistics

To clear all Point-to-Point Protocol (PPP) statistics for a PPP interface, use the clear ppp statistics command in EXEC mode.

### clear ppp statistics interface interface-path-id

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**
Use the show interfaces command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear PPP statistics for a PPP interface:

```
RE/0/RSP0/CPU0:router# clear ppp statistics interface 0/1/0/1
```
encapsulation ppp

To enable encapsulation for communication with routers or bridges using the Point-to-Point Protocol (PPP), use the `encapsulation ppp` command in interface configuration mode. To disable PPP encapsulation, use the `no` form of this command.

```
encapsulation ppp
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

PPP encapsulation is disabled.

**Command Modes**

Interface configuration

**Command History**

Release | Modification
---------|------------
3.9.0 | This command was introduced.

**Usage Guidelines**

Use the `encapsulation ppp` command to enable PPP encapsulation on an interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set up PPP encapsulation on interface POS 0/1/0/1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
```

The following example shows how to set up PPP encapsulation on a serial interface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# interface serial 0/0/1/2/4:3
RP/0/RSP0/CPU0:router# encapsulation ppp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ppp interfaces (BNG)</code>, on page 655</td>
<td>Displays PPP state information for an interface.</td>
</tr>
</tbody>
</table>
To create a Session State Redundancy Protocol (SSRP) group and associate it with a profile, use the `group` command in Global Configuration mode. To remove this group, use the no form of this command.

```
group  group-id  profile  profile_name  [default]
```

**Syntax Description**

- `group-id`  
  SSRP group identifier. The range is 1 to 65535.
- `profile profile_name`  
  Profile to associate with this group.
- `default`  
  Associates the group to the default profile.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Any interfaces on this card can be configured to use this group. The group number must be unique across the router.

**Examples**

The following example shows how to create an SSRP group:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RSP0/CPU0:router(config-ssrp-node)# group 1 profile default
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssrp location</code>, on page 667</td>
<td>specify the node on which to create a SSRP group and enter the SSRP node configuration mode.</td>
</tr>
</tbody>
</table>
multi-router aps

To configure Multi-Router Automatic Protection Switching (MR-APS) and enter APS redundancy configuration mode, use the `multi-router aps` command in redundancy configuration mode. To deactivate Multi-Router Automatic Protection Switching (MR-APS), use the no form of this command.

`multi-router aps`

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
Redundancy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# redundancy
RP/0/RSP0/CPU0:router(config-redundancy)# multi-router aps
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redundancy, on page 653</code></td>
<td>Enters the redundancy configuration mode to configure MR-APS.</td>
</tr>
</tbody>
</table>
peer ipv4 address

To configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer, use the peer ipv4 address command in SSRP configuration mode. To remove the address, use the no form of this command.

peer ipv4 address  ip-address

**Syntax Description**

*ip-address*  IP address of the peer interface whose states will be replicated by SSRP.

**Command Default**

No default behavior or values

**Command Modes**

SSRP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the IPv4 address for a Session State Redundancy Protocol (SSRP) peer:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RSP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssrp profile, on page 668</td>
<td>Configures a SSRP profile and enters the SSRP configuration mode.</td>
</tr>
</tbody>
</table>
To enable Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, or Password Authentication Protocol (PAP), and to specify the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface, use the `ppp authentication` command in an appropriate configuration mode. To disable PPP authentication, use the `no` form of this command.

```
ppp authentication  protocol  [protocol  [protocol]]  {list-name  |  default}
```

**Syntax Description**

- `protocol` Name of the authentication protocol used for PPP authentication. See Table 49: PPP Authentication Protocols for Negotiation, on page 624 for the appropriate keyword. You may select one, two, or all three protocols, in any order.

- `list-name` (Optional) Used with authentication, authorization, and accounting (AAA). Name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the `aaa authentication ppp` command.

- `default` (Optional) Specifies the name of the list of methods created with the `aaa authentication ppp` command.

**Command Default**

PPP authentication is not enabled.

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

- Release 3.9.0  This command was introduced.
- Release 4.2.0  This command was supported in the dynamic template configuration mode for BNG.

**Usage Guidelines**

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a response message. The local router attempts to match the remote device’s name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device’s ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.
If you use a list-name value that was not configured with the `aaa authentication ppp` command, then authentication does not complete successfully and the line does not come up.

**Table 49: PPP Authentication Protocols for Negotiation**, on page 624 lists the protocols used to negotiate PPP authentication.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chap</td>
<td>Enables CHAP on an interface.</td>
</tr>
<tr>
<td>ms-chap</td>
<td>Enables Microsoft’s version of CHAP (MS-CHAP) on an interface.</td>
</tr>
<tr>
<td>pap</td>
<td>Enables PAP on an interface.</td>
</tr>
</tbody>
</table>

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication. In this case, authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Enabling or disabling PPP authentication does not affect the local router authenticating itself to the remote device.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In this example, CHAP is enabled on POS 0/4/0/1 and uses the authentication list MIS-access:

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/4/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap MIS-access
```

This is an example of configuring the `ppp authentication` command:

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp authentication chap ms-chap pap
```
PPP Commands

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa authentication ppp</strong></td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td><strong>encapsulation</strong></td>
<td>Sets the encapsulation method used by the interface.</td>
</tr>
<tr>
<td><strong>username</strong></td>
<td>Configures a new user with a username, establishes a password, and grants permissions for the user.</td>
</tr>
</tbody>
</table>
**ppp chap password**

To enable a router calling a collection of routers to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password, use the **ppp chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

```plaintext
ppp chap password [{clear | encrypted}] password
```

**Syntax Description**

- **clear** (Optional) Specifies the cleartext encryption parameter for the password.
- **encrypted** (Optional) Indicates that the password is already encrypted.
- **password** Cleartext or already-encrypted password.

**Command Default**

The password is disabled.

**Command Modes**

Interface configuration

**Command History**

- **Release** Modification
  - Release 3.9.0 This command was introduced.

**Usage Guidelines**

The **ppp chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. This command is useful for routers that do not support this command (such as routers running older Cisco IOS XR images).

The CHAP secret password is used by the routers in response to challenges from an unknown peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In this example, a password (xxxx) is entered as a cleartext password:

```plaintext
RP/0/RSP0/CPU0:router(config-if)# ppp chap password xxxx
```

When the password is displayed (as shown in the following example, using the **show running-config** command), the password xxxx appears as 030752180500:

```plaintext
RP/0/RSP0/CPU0:router(config)# show running-config interface POS 1/0/1/0
interface POS0/1/4/2
```
description Connected to P1 POS 0/1/4/3
ipv4 address 10.12.32.2 255.255.255.0
encapsulation ppp
ppp authentication chap pap
ppp chap password encrypted 030752180500

On subsequent logins, entering any of the three following commands would have the same effect of makingxxxx the password for remote CHAP authentication:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 1/0/1/0
RP/0/RSP0/CPU0:router(config-if)# ppp chap password xxxx
RP/0/RSP0/CPU0:router(config-if)# ppp chap password clear xxxx
RP/0/RSP0/CPU0:router(config-if)# ppp chap password encrypted 1514190900
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa authentication ppp</strong></td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td><strong>ppp authentication (BNG), on page 623</strong></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
<tr>
<td><strong>ppp chap refuse, on page 628</strong></td>
<td>Refuses CHAP authentication from peers requesting it.</td>
</tr>
<tr>
<td><strong>ppp max-bad-auth (BNG), on page 633</strong></td>
<td>Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.</td>
</tr>
</tbody>
</table>
### ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the `ppp chap refuse` command in interface configuration mode. To allow CHAP authentication, use the `no` form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
CHAP authentication is disabled.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `ppp chap refuse` command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the `ppp authentication` command), PAP is suggested as the authentication method in the refusal packet.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to specify POS interface 0/3/0/1 and disable CHAP authentication from occurring if a peer calls in requesting CHAP authentication. The method of encapsulation on the interface is PPP.

```console
RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CP00:router(config-if)# encapsulation ppp
RP/0/RSP0/CP00:router(config-if)# ppp chap refuse
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authentication ppp</code></td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>ppp authentication (BNG), on page 623</code></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
<tr>
<td><code>ppp max-bad-auth (BNG), on page 633</code></td>
<td>Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.</td>
</tr>
<tr>
<td><code>ppp pap sent-username password, on page 648</code></td>
<td>Enables remote PAP support for an interface, and includes the <code>sent-username</code> and <code>password</code> commands in the PAP authentication request packet to the peer.</td>
</tr>
</tbody>
</table>
To configure the primary and secondary Domain Name System (DNS) IP addresses for the Internet Protocol Control Protocol (IPCP), use the `ppp ipcp dns` command in interface configuration mode. To remove the addresses, use the no form of this command.

`ppp ipcp dns primary-ip-address [sec-ip-address]`

**Syntax Description**
- `primary-ip-address` Primary DNS IP address, in the format A.B.C.D.
- `sec-ip-address` Secondary DNS IP address, in the format W.X.Y.Z.

**Command Default**
No default behavior or values

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure the primary and secondary DNS IP addresses for Internet Protocol Control Protocol (IPCP):

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp ipcp dns 10.10.10.10 10.10.10.11
```
**ppp ipcp neighbor-route disable**

To disable installation of a route to the peer address negotiated by Internet Protocol Control Protocol (IPCP), use the `ppp ipcp neighbor-route disable` command in interface configuration mode. To re-enable installation of a route to the peer address negotiated by IPCP, use the no form of this command.

![Command](https://example.com/command.png)

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to disable installation of a route to the peer address negotiated by IPCP:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp ipcp neighbor-route disable
```
**ppp ipcp peer-address default**

To specify the default IPv4 address that is assigned to the peer by the Internet Protocol Control Protocol (IPCP), use the **ppp ipcp peer-address default** command in interface configuration mode. To remove the address, use the no form of this command.

```
ppp ipcp peer-address default  ip-address
```

**Syntax Description**

*ip-address*  Specifies the IP address for the peer node.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify the default IPv4 address that is assigned to the peer by IPCP.

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp ipcp peer-address default 10.10.10.10
```
ppp max-bad-auth (BNG)

To configure a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the `ppp max-bad-auth` command in the appropriate configuration mode. To reset to the default of immediate reset, use the `no` form of this command.

`ppp max-bad-auth retries`

**Syntax Description**

| retries | Number of retries after which the interface is to reset itself. Range is from 0 to 10. Default is 0 retries. |

**Command Default**

`retries: 0`

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ppp max-bad-auth` command applies to any interface on which PPP encapsulation is enabled. To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In this example, POS interface 0/3/0/1 is set to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap
RP/0/RSP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

This example shows how to allow two additional retries after an initial authentication failure in the dynamic template configuration mode:
ppp max-bad-auth (BNG)

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp max-configure 5
```
ppp max-configure (BNG)

To specify the maximum number of configure requests to attempt (without response) before stopping the requests, use the `ppp max-configure` command in an appropriate configuration mode. To disable the maximum number of configure requests and return to the default, use the `no` form of this command.

```
ppp max-configure retries
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>Maximum number of retries. Range is 4 through 20. Default is 10.</td>
</tr>
</tbody>
</table>

**Command Default**

```
retries: 10
```

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ppp max-configure` command to specify how many times an attempt is made to establish a Link Control Protocol (LCP) session between two peers for a particular interface. If a configure request message receives a reply before the maximum number of configure requests are sent, further configure requests are abandoned.

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows a limit of four configure requests:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp max-configure 4
```

This example shows how a limit of four configure requests is specified in the dynamic template configuration mode:
```plaintext
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ppp ipcp
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp max-failure (BNG), on page 637</strong></td>
<td>Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.</td>
</tr>
</tbody>
</table>
**ppp max-failure (BNG)**

To configure the maximum number of consecutive Configure Negative Acknowledgments (CONFNAKs) to permit before terminating a negotiation, use the `ppp max-failure` command in an appropriate configuration mode. To disable the maximum number of CONFNAKs and return to the default, use the `no` form of this command.

```
ppp max-failure retries
```

**Syntax Description**

- `retries` Maximum number of CONFNAKs to permit before terminating a negotiation. Range is from 2 to 10. Default is 5.

**Command Default**

`retries: 5`

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enter the dynamic template configuration mode, run `dynamic-template` command in the Global Configuration mode.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The `ppp max-failure` command specifies that no more than three CONFNAKs are permitted before terminating the negotiation:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp max-failure 3
```

This example shows how no more than three CONFNAKs are permitted before terminating the negotiation in the dynamic template configuration mode:
**ppp max-failure (BNG)**

RP/0/RSP0/CPU0:router#  **configure**  
RP/0/RSP0/CPU0:router(config)#  **dynamic-template type ppp p1**  
RP/0/RSP0/CPU0:router(config-dynamic-template-type)#  **ppp max-failure 4**

<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ppp max-configure (BNG)</em></td>
<td><strong>on page 635</strong></td>
<td>Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.</td>
</tr>
</tbody>
</table>
ppp max-terminate

To configure the maximum number of terminate requests (TermReqs) to send without reply before closing down the Link Control Protocol (LCP) or Network Control Protocol (NCP), use the `ppp max-terminate` command in interface configuration mode. To disable the maximum number of TermReqs and return to the default, use the `no` form of this command.

**Command Default**

- **number**: 2

**Command Modes**

- Interface configuration

**Command History**

- **Modification**
  - Release 3.9.0 This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **read**, **write**

**Examples**

In the following example, a maximum of five TermReqs are specified to be sent before terminating and closing LCP or NCP:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp max-terminate 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ppp max-configure (BNG), on page 635</strong></td>
<td>Specifies the maximum number of configure requests to attempt (without response) before stopping the requests.</td>
</tr>
<tr>
<td><strong>ppp max-failure (BNG), on page 637</strong></td>
<td>Configures the maximum number of consecutive CONFNAKs to permit before terminating a negotiation.</td>
</tr>
</tbody>
</table>
ppp ms-chap hostname

To configure the hostname for MS-CHAP authentication on an interface, use the `ppp ms-chap hostname` command in interface configuration mode. To remove the hostname, use the `no` form of this command.

```
ppp ms-chap hostname hostname
```

**Syntax Description**
- `hostname` Specifies the hostname for MS-CHAP authentication.

**Command Default**
No default behavior or values

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure the hostname for MS-CHAP authentication on an interface:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp ms-chap hostname Host_1
```
ppp ms-chap password

To configure a common Microsoft Challenge Handshake Authentication (MS-CHAP) secret password, use the **ppp ms-chap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

```
ppp ms-chap password [{clear | encrypted}] password
```

**Syntax Description**

- **clear** (Optional) Specifies the cleartext encryption parameter for the password.
- **encrypted** (Optional) Indicates that the password is already encrypted.
- **password** Cleartext or already-encrypted password.

**Command Default**

The password is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ppp ms-chap password** command is sent in CHAP responses and is used by the peer to authenticate the local router. This does not affect local authentication of the peer. The **ppp ms-chap password** command is useful for routers that do not support this command (such as routers running older software images).

The MS-CHAP secret password is used by the routers in response to challenges from an unknown peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter a password (xxxx) as a cleartext password:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp ms-chap password clear xxxx
```
**ppp ms-chap refuse**

To refuse Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication from peers requesting it, use the `ppp ms-chap refuse` command in interface configuration mode. To allow MS-CHAP authentication, use the **no** form of this command.

```
ppp ms-chap refuse
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

MS-CHAP authentication is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ppp ms-chap refuse` command specifies that MS-CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using MS-CHAP are refused.

If outbound Password Authentication Protocol (PAP) has been configured (using the `ppp authentication` command), PAP is suggested as the authentication method in the refusal packet.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to specify POS interface 0/3/0/1 and disable MS-CHAP authentication from occurring if a peer calls in requesting MS-CHAP authentication. The method of encapsulation on the interface is PPP.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp ms-chap refuse
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp authentication (BNG), on page 623</code></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
</tbody>
</table>
ppp multilink multiclass

To enable multiclass multilink PPP, use the **ppp multilink multiclass** command in interface configuration mode. To disable multiclass multilink PPP, use the no form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable multiclass multilink PPP:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp multilink multiclass
```
ppp multilink multiclass local

To configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer, use the `ppp multilink multiclass local` command in interface configuration mode. To remove these settings, use the no form of this command.

```
ppp multilink multiclass local initial init-number maximum max-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial</td>
<td>Specifies the initial number of receive classes in the Conf-Request. The range is 1 to 16.</td>
</tr>
<tr>
<td>maximum</td>
<td>Specifies the maximum number of receive classes in the Conf-Request. The range is 1 to 16.</td>
</tr>
</tbody>
</table>

**Command Default**

When MCMP is enabled, the default initial value is 2 and the default maximum value is 4.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The maximum number of receive classes configures the number of transmission classes on the local host.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the initial number and maximum number of Multiclass Multilink PPP (MCMP) receive classes in a Conf-Request sent from a local host to its peer:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# ppp multilink multiclass local initial 1 maximum 16
```
**ppp multilink multiclass remote apply**

To configure the minimum number of Multiclass Multilink PPP (MCMP) receive classes that a local host will accept from its peer in a Conf-Request, use the `ppp multilink multiclass` command in interface configuration mode. To remove this setting, use the no form of this command.

```
ppp multilink multiclass remote apply min-number
```

**Syntax Description**

- `min-number` Specifies the minimum number of receive classes in the Conf-Request. The range is 1 to 16.

**Command Default**

The default is 2 if MCMP is enabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to coerce the peer to accept a minimum number of MCMP classes. If the peer does not accept the minimum number of MCMP classes specified by this command, the local router will not bring up the PPP link.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to use the `ppp multilink multicast remove apply` command.

```
RP/0/RSP0/CPU0# config
RP/0/RSP0/CPU0(config)# interface Multilink 0/0/0/1
RP/0/RSP0/CPU0(config-if)# ppp multilink multiclass remote apply 16
```
**ppp pap refuse**

To refuse Password Authentication Protocol (PAP) authentication from peers requesting it, use the `ppp pap refuse` command in interface configuration mode. To allow PAP authentication, use the `no` form of this command.

```plaintext
ppp pap refuse
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

PAP authentication is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ppp pap refuse` command specifies that PAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using PAP are refused.

If outbound Challenge Handshake Authentication Protocol (CHAP) has been configured (using the `ppp authentication` command), CHAP is suggested as the authentication method in the refusal packet.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify POS 0/3/0/1 using PPP encapsulation on the interface. This example shows PAP authentication being specified as disabled if a peer calls in requesting PAP authentication.

```plaintext
RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CP00:router(config-if)# encapsulation ppp
RP/0/RSP0/CP00:router(config-if)# ppp pap refuse
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication ppp</td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>ppp authentication (BNG), on page 623</strong></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
<tr>
<td><strong>ppp max-bad-auth (BNG), on page 633</strong></td>
<td>Configures a PPP interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.</td>
</tr>
<tr>
<td><strong>ppp pap sent-username password, on page 648</strong></td>
<td>Enables remote PAP support for an interface, and includes the <code>sent-username</code> and <code>password</code> commands in the PAP authentication request packet to the peer.</td>
</tr>
</tbody>
</table>
**ppp pap sent-username password**

To enable remote Password Authentication Protocol (PAP) support for an interface, and to use the values specified for username and password in the PAP authentication request, use the `ppp pap sent-username password` command in interface configuration mode. To disable remote PAP support, use the `no` form of this command.

```
ppp pap sent-username username password [{clear | encrypted}] password
```

**Syntax Description**

- `username` Username sent in the PAP authentication request.
- `clear` (Optional) Specifies the cleartext encryption parameter for the password.
- `encrypted` (Optional) Indicates that the password is already encrypted.
- `password` Cleartext or already-encrypted password.

**Command Default**

Remote PAP support is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.9.0   | This command was introduced.

**Usage Guidelines**

Use the `ppp pap sent-username password` command to enable remote PAP support (for example, to respond to the peer’s request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

You must configure the `ppp pap sent-username password` command for each interface.

**Task ID**

- **Task ID**
  - `ppp` read, write
  - `aaa` read, write

**Examples**

In the following example, a password is entered as a cleartext password, xxxx:

```
RP/0/RSP0/CP00:router(config-if)# ppp pap sent-username xxxx password notified
```

When the password is displayed (as shown in the following example, using the `show running-config` command), the password notified appears as 05080F1C2243:

```
RP/0/RSP0/CP00:router(config-if)# show running-config
```
interface POS0/1/0/0
  description Connected to P1 POS 0/1/4/2
  ipv4 address 10.12.32.2 255.255.255.0
  encapsulation ppp
  ppp pap sent-username P2 password encrypted 05080F1C2243

On subsequent logins, entering any of the three following commands would have the same effect of making xxxx the password for remote PAP authentication:

```plaintext
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified
RP/0/RSP0/CPU0:router(config-if)# ppp pap sent-username xxxx password clear notified
RP/0/RSP0/CPU0:router(config-if)# ppp pap sent-username xxxx encrypted 1514190900
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authentication ppp</code></td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td><code>ppp authentication (BNG), on page 623</code></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
<tr>
<td><code>ppp multilink multiclass, on page 643</code></td>
<td>Refuses PAP authentication from peers requesting it</td>
</tr>
<tr>
<td><code>ppp timeout authentication, on page 650</code></td>
<td>Sets PPP authentication timeout parameters.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.</td>
</tr>
</tbody>
</table>
**ppp timeout authentication**

To set PPP authentication timeout parameters, use the **ppp timeout authentication** command in interface configuration mode. To reset the default value, use the **no** form of this command.

`ppp timeout authentication seconds`

**Syntax Description**

*seconds* Maximum time, in seconds, to wait for a response to an authentication packet. Range is from 3 to 30 seconds. Default is 10 seconds.

**Command Default**

*seconds*: 10

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default authentication time is 10 seconds, which should allow time for a remote router to authenticate and authorize the connection and provide a response. However, it is also possible that it will take much less time than 10 seconds. In such cases, use the **ppp timeout authentication** command to lower the timeout period to improve connection times in the event that an authentication response is lost.

**Note**

The timeout affects connection times only if packets are lost.

**Note**

Although lowering the authentication timeout is beneficial if packets are lost, sending authentication requests faster than the peer can handle them results in churn and a slower connection time.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, PPP timeout authentication is set to 20 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp timeout authentication 20
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa authentication ppp</strong></td>
<td>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td><strong>ppp authentication (BNG), on page 623</strong></td>
<td>Enables CHAP, MS-CHAP, or PAP, and specifies the order in which CHAP, MS-CHAP, and PAP authentication is selected on the interface.</td>
</tr>
</tbody>
</table>
**ppp timeout retry**

To set PPP timeout retry parameters, use the `ppp timeout retry` command in interface configuration mode. To reset the time value, use the `no` form of this command.

```
ppp timeout retry seconds
```

**Syntax Description**

- `seconds`: Maximum time, in seconds, to wait for a response during PPP negotiation. Range is from 1 to 10 seconds. Default is 3 seconds.

**Command Default**

```
seconds: 3
```

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ppp timeout retry` command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

**Task ID**

- Task ID
- Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the retry timer being set to 8 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# ppp timeout retry 8
```
**redundancy**

To enter the redundancy configuration mode to configure Multi-Router Automatic Protection Switching (MR-APS), use the `redundancy` command in Global Configuration mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
Global Configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enter the redundancy configuration mode:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# redundancy
RP/0/RSP0/CPU0:router(config-redundancy)#
```
security ttl

To specify that the time-to-live (TTL) value in the IP header of the packet is used to validate that a packet is from the expected source, use the `security ttl` command in SSRP configuration mode. To remove the TTL requirement, use the no form of this command.

```
security ttl max-hops number
```

**Syntax Description**

- `max-hops number` Maximum number of hops between the peer routers.

**Command Default**

The `max-hops` default is 255.

**Command Modes**

SSRP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If `max-hops` is not specified, the TTL value must be 255 for a packet to be accepted.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify that the time-to-live (TTL) value in the IP header of a packet is used to validate that the packet is from the expected source:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RSP0/CPU0:router(config-ssrp)# peer ipv4 address 10.10.10.10
RP/0/RSP0/CPU0:router(config-ssrp)# security ttl max-hops number 50
```
show ppp interfaces (BNG)

To display PPP state information for an interface, use the `show ppp interfaces` command in EXEC mode.

```
show ppp interfaces [{brief | detail}] {all | type interface-path-id | location node-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>brief</th>
<th>(Optional) Displays brief output for all interfaces on the router, for a specific POS interface instance, or for all interfaces on a specific node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed output for all interfaces on the router, for a specific interface instance, or for all interfaces on a specific node.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Displays detailed PPP information for all nodes.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Displays detailed PPP information for the designated node. The <code>node-id</code> argument is entered in the rack/slot/module notation.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>This command was supported in the dynamic template configuration mode for BNG.</td>
</tr>
<tr>
<td>Release 5.3.2</td>
<td>The command was modified to include a new output display field, <strong>SRG-state</strong>, as part of geo redundancy support for PPPoE sessions in BNG router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There are seven possible PPP states applicable for either the Link Control Protocol (LCP) or the Network Control Protocol (NCP).

The command output displays a summary of the interface as it is in the PPP Interface Descriptor Block (IDB). The output includes the following information (where applicable):
• Interface state
• Line protocol state
• Link Control Protocol (LCP) state
• Network Control Protocol (NCP) state
• Multilink PPP state
• Multilink PPP configuration
• Keepalive configuration
• Authentication configuration
• Negotiated MRUs
• Negotiated IP addresses

This command can display information for a single interface, all interfaces on a specified node, or all interfaces on the router.

Multilink PPP and POS are not supported for BNG Geo Redundancy.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display PPP state information for a POS interface:

```
RP/0/RSP0/CPU0:router# show ppp interface POS 0/2/0/3
POS0/2/0/3 is up, line protocol is up
  LCP: Open
  Keepalives enabled (10 sec)
  Local MRU: 4470 bytes
  Peer MRU: 4470 bytes
  Authentication
    Of Us:  CHAP (Completed as 'test-user')
    Of Peer: PAP (Completed as 'peer-user')
  CDPCP: Listen
  IPCP: Open
    Local IPv4 address: 55.0.0.1
    Peer IPv4 address: 55.0.0.2
    Peer DNS Primary: 55.0.0.254
    Peer DNS Secondary: 155.0.0.254
  IPV6CP: Open
    Local IPv6 address: fe80::3531:35ff:fe55:5747/128
    Peer IPv6 address: fe80::3531:35ff:fe55:4213/128
  MPLSCP: Stopped
```

This example shows how to display PPP state information for a POS interface that is running as a Layer 2 attachment circuit:

```
RP/0/0/CPU0:# show ppp interface POS0/2/0/2
POS0/2/0/2 is up, line protocol is up
  LCP: Open
    Running as L2 AC
```

This example shows how to display PPP state information for a multilink interface:
This example shows how to display PPP state information for a serial interface:

```
show ppp interface Serial 0/3/1/3/1
```

This is a sample output of the `show ppp interfaces` command in the BNG router, having subscriber redundancy group (SRG) in geo redundancy enabled for PPPoE sessions:

```
show ppp interfaces
```

```
Bundle-Ether2.1.pppoe16534 is down, line protocol is up
SRG Role: Slave
LCP: Open
```
Keepalives enabled (60 sec, retry count 5)
Local MRU: 1492 bytes
Peer MRU: 65531 bytes
Authentication
  Of Peer: PAP (Completed as user1@domain.com)
  Of Us: <None>
IPCP: Open
  Local IPv4 address: 12.16.0.1
  Peer IPv4 address: 12.0.250.23
IPv6CP: Initial
  Local IPv6 address: fe80::
  Peer IPv6 address: fe80::

Table 50: show ppp interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ack-Rcvd</td>
<td>Configuration acknowledgment was received; waiting for peer to send configuration request.</td>
</tr>
<tr>
<td>Ack-Sent</td>
<td>Configuration acknowledgment was sent; waiting for peer to respond to configuration request.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Type of user authentication configured on the local equipment and on the peer equipment. Possible PPP authentication protocols are Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, and Password Authentication Protocol (PAP).</td>
</tr>
<tr>
<td>Closed</td>
<td>Lower layer is up, but this layer is not required.</td>
</tr>
<tr>
<td>Closing</td>
<td>Shutting down due to local change.</td>
</tr>
<tr>
<td>Initial</td>
<td>Connection is idle.</td>
</tr>
<tr>
<td>IPCP</td>
<td>IP Control Protocol (IPCP) state. The seven possible states that may be displayed are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state.</td>
</tr>
<tr>
<td></td>
<td>• Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent.</td>
</tr>
<tr>
<td></td>
<td>• Closed—IPCP is not currently trying to negotiate.</td>
</tr>
<tr>
<td></td>
<td>• Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received.</td>
</tr>
<tr>
<td></td>
<td>• Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered.</td>
</tr>
<tr>
<td></td>
<td>• Stopping—A Terminate-Request has been sent and the Restart timer is running, but a IPCP-Ack has not yet been received. Req-Sent.</td>
</tr>
<tr>
<td></td>
<td>• ACKsent—IPCP has received a request and has replied to it.</td>
</tr>
<tr>
<td></td>
<td>• ACKrcvd—IPCP has received a reply to a request it sent.</td>
</tr>
<tr>
<td></td>
<td>• Open—IPCP is functioning properly.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Keepalive</td>
<td>Keepalive setting and interval in seconds for echo request packets.</td>
</tr>
</tbody>
</table>
| LCP          | Indicates the current state of LCP. The state of the LCP will report the following states:  
|              | • Initial—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state.  
|              | • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent.  
|              | • Closed— LCP is not currently trying to negotiate.  
|              | • Stopped—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received.  
|              | • Closing—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered.  
|              | • Stopping—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent.  
|              | • ACKsent—LCP has received a request and has replied to it.  
|              | • ACKrcvd—LCP has received a reply to a request it sent.  
|              | • Open—LCP is functioning properly  
| Local IPv4 address | IPv4 address for the local interface.                                      |
| Local MRU    | Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the local equipment. |
| Open         | Connection open.                                                            |
Open System Interconnection Control Protocol (OSICP) state. The possible states that may be displayed are as follows:

- **Initial**—Lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running in the Initial state.
- **Starting**—An administrative Open has been initiated, but the lower layer is still unavailable (Down). The Restart timer is not running in the Starting state. When the lower layer becomes available (Up), a Configure-Request is sent.
- **Closed**—OSICP is not currently trying to negotiate.
- **Stopped**—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received.
- **Closing**—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Upon reception of a Terminate-Ack, the Closed state is entered. Upon the expiration of the Restart timer, a new Terminate-Request is transmitted, and the Restart timer is restarted. After the Restart timer has expired Max-Terminate times, the Closed state is entered.
- **Stopping**—A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received. Req-Sent.
- **ACKsent**—OSICP has received a request and has replied to it.
- **ACKrcvd**—OSICP has received a reply to a request it sent.
- **Open**—OSICP is functioning properly.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSICP</td>
<td>Open System Interconnection Control Protocol (OSICP) state. The possible states that may be displayed are as follows:</td>
</tr>
<tr>
<td>Peer IPv4 address</td>
<td>IPv4 address for the peer equipment.</td>
</tr>
<tr>
<td>Peer MRU</td>
<td>Maximum receive unit. The maximum size of the information transported, in bytes, in the PPP packet received by the peer equipment.</td>
</tr>
<tr>
<td>Req-Sent</td>
<td>Configuration request was sent; waiting for peer to respond.</td>
</tr>
<tr>
<td>Starting</td>
<td>This layer is required, but lower layer is down.</td>
</tr>
<tr>
<td>Stopped</td>
<td>Listening for a configuration request.</td>
</tr>
<tr>
<td>Stopping</td>
<td>Shutting down as a result of interactions with peer.</td>
</tr>
</tbody>
</table>
**show ppp sso alerts**

To display all Inter-Chassis Stateful Switchover (ICSSO) alerts that have occurred, use the `show ppp sso alerts` command in EXEC mode.

```
show ppp sso alerts location node-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>location</strong> node-id</td>
<td>Specifies the full qualified path of a specific node in the format rack/slot/module.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the following information for alerts that have prevented a standby session from being brought to the Standby-Up state using replicated data.

- The interfaces on which the alerts have occurred
- The layer in which the error has occurred
- A short description of the error

**Note**

Only one error is reported for each layer for each interface. The error displayed is the most recent error that has occurred.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display all ICSSO alerts that have occurred:

```
RP/0/RSP0/CPU0:router# show ppp sso errors location 0/3/cpu0
```

<table>
<thead>
<tr>
<th>Intf</th>
<th>Layer</th>
<th>SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>with error</td>
<td>Error</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
<td>--------</td>
</tr>
<tr>
<td>Mu0/3/0/100</td>
<td>IPCP</td>
<td>Unsupported IPCP option 0x07</td>
</tr>
<tr>
<td>Se0/3/1/1:0</td>
<td>LCP</td>
<td>Unacceptable value for LCP MRU option</td>
</tr>
<tr>
<td>Se0/3/1/3:2:0</td>
<td>of-us-auth</td>
<td>Incorrect Authentication protocol, CHAP</td>
</tr>
<tr>
<td>Se0/3/1/3:3:0</td>
<td>of-peer-auth</td>
<td>Invalid CHAP Authentication options</td>
</tr>
<tr>
<td>Se0/3/1/3:4:0</td>
<td>LCP</td>
<td>Inconsistent LCP MRRU options</td>
</tr>
</tbody>
</table>
show ppp sso state

To display the Inter-Chassis Stateful Switchover (ICSSO) states of a Point-to-Point Protocol (PPP) session running under a particular Multi-Router Automatic Protection Switching (MR-APS) group, use the `show ppp sso state` command in EXEC mode.

```
show ppp sso state group group-id location node-id
```

**Syntax Description**

- `group group-id` Specifies the redundancy group number. The range is 1 to 32.
- `location node-id` Specifies the full qualified path of a specific node in the format `rack/slot/module`.

**Command Default**

If group is not specified, states are displayed for all redundancy groups.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command shows the states of these session layers:

- LCP
- of-us authentication
- of-peer authentication
- IPCP

**Note**

When an interface is in Standby mode, it is ready to forward traffic immediately after a switchover, if all the session layers, including IPCP, are in the S-Negd state.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display the ICSSO states for PPP running under a redundancy group:

```
RP/0/RSP0/CPU0:router# show ppp sso state location 0/3/cpu0
```

- Not-Ready : The session is not yet ready to run as Active or Standby
- S-UnNegd : In Standby mode, no replication state received yet
- A-Down : In Active mode, lower layer not yet up
- Deact'ing : Session was Active, now going Standby
- A-UnNegd : In Active mode, not fully negotiated yet
**S-Negd**: In Standby mode, replication state received and pre-programmed  
**Act'ing**: Session was Standby and pre-programmed, now going Active  
**A-Negd**: In Active mode, fully negotiated and up  
**-**: This layer not running

<table>
<thead>
<tr>
<th>SSO-Group</th>
<th>of-us</th>
<th>of-peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LCP</td>
<td>auth</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilink0/3/0/0/100</td>
<td>S-Negd</td>
<td>S-Negd</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilink0/3/0/0/101</td>
<td>S-UnNegd</td>
<td>S-UnNegd</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/1</td>
<td>S-Negd</td>
<td>S-Negd</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/2</td>
<td>A-Negd</td>
<td>A-Negd</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/3</td>
<td>A-Down</td>
<td>Not-Ready</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/4</td>
<td>A-Up</td>
<td>A-Up</td>
</tr>
</tbody>
</table>

SSO-Group 1 | of-us | of-peer |       |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LCP</td>
<td>auth</td>
<td>auth</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilink0/3/0/0/102</td>
<td>S-Negd</td>
<td>S-Negd</td>
<td>S-Negd</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/5</td>
<td>S-Negd</td>
<td>S-Negd</td>
<td>S-Negd</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/3/1/3/6</td>
<td>A-Negd</td>
<td>A-Negd</td>
<td>A-Negd</td>
</tr>
</tbody>
</table>
show ppp sso summary

To display the number of sessions in each Inter-Chassis Stateful Switchover (ICSSO) state for each session layer, use the `show ppp sso summary` command in EXEC mode.

```
show ppp sso summary location node-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location node-id</td>
<td>Specifies the full qualified path of a specific node in the format rack/slot/module.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays information for these session layers:

- LCP
- of-us
- of-peer authentication
- IPCP

**Note**

Only sessions with Session State Redundancy Protocol (SSRP) configured are displayed.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to display the number of sessions in each ICSSO state for each session layer.

```
RP/0/RSP0/CPU0:router# show ppp sso summary location 0/3/cpu0
```

- Not-Ready : The session is not yet ready to run as Active or Standby
- Stby-UnNegd : In Standby mode, no replication state received yet
- Act-Down : In Active mode, lower layer not yet up
- Deactivating : Session was Active, now going Standby
- Act-UnNegd : In Active mode, not fully negotiated yet
- Stby-Negd : In Standby mode, replication state received and pre-programmed
- Activating : Session was Standby and pre-programmed, now going Active
- Act-Negd : In Active mode, fully negotiated and up
- - : This layer not running
### PPP Commands

**show ppp sso summary**

<table>
<thead>
<tr>
<th>Layer</th>
<th>Total</th>
<th>Ready</th>
<th>UnNegd</th>
<th>Down</th>
<th>Act-Deactiv</th>
<th>Act-UnNegd</th>
<th>Act-Negd</th>
<th>Stby-Negd</th>
<th>Stby-Activ</th>
<th>Active-Negd</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCP</td>
<td>20</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>of-us-auth</td>
<td>20</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>of-peer-auth</td>
<td>20</td>
<td>10</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>IPCP</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
ssrp group

To attach a Session State Redundancy Protocol (SSRP) group on an interface, use the `ssrp group` command in interface configuration mode. To remove the SSRP group from the interface, use the `no` form of this command.

```
ssrp group  group-number  id  id-number  ppp
```

**Syntax Description**

- `group-number`: SSRP group number. The range is 1 to 65535.
- `id  id-number`: SSRP identifier number. The range is 1 to 4294967295.
- `ppp`: Specifies point-to-point protocol.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The group must be configured first on a specific location (linecard) and then assigned to the interface. The redundancy ID must be unique within the group. This command specifies a list the protocols that the group can replicate. Currently only PPP is supported.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface Multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# ssrp group 1 id 1 ppp
```
ssrp location

To specify the node on which to create a Session State Redundancy Protocol (SSRP) group and enter the SSRP node configuration mode, use the **ssrp location** command in Global Configuration mode.

```
ssrp location node_id
```

**Syntax Description**

- **node_id** Specifies the full qualified path of a specific node in the format rack/slot/module.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration mode

**Command History**

```
Release     Modification
-----------  -------------------
3.9.0       This command was introduced.
```

**Usage Guidelines**

The location specifies the card on which an SSRP group is created.

**Task ID**

```
Task ID Operations
---------- ----------
ppp        read, write
```

**Examples**

This example shows how to create an SSRP group on a specified node for use by any interface on the card:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ssrp location 0/1/cpu0
RP/0/RSP0/CPU0:router(config-ssrp-node)#
```
ssrp profile

To configure a Session State Redundancy Protocol (SSRP) profile and enter the SSRP configuration mode, use the `ssrp profile` command in Global Configuration mode. To remove the profile, use the `no` form of this command.

```
ssrp profile profile-name
```

**Syntax Description**

- `profile-name`: Name of this SSRP profile.

**Command Default**

No default behavior or values

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A Session State Redundancy Protocol (SSRP) profile allows the same SSRP configuration to be shared across multiple groups. The same profile can be attached to multiple groups across the router. The group must be configured before the interface that uses the group can be configured. The group number is used in the TCP port number so, the group number must be unique across the router.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure an SSRP profile:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ssrp profile Profile_1
RP/0/RSP0/CPU0:router(config-ssrp)#
```
Serial Interface Commands

This module provides CLI commands for configuring serial interfaces on the Cisco ASR 9000 Series Router. To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- clear iphc ipv4, on page 671
- crc (serial), on page 673
- description (IPH C profile), on page 675
- encapsulation (serial), on page 676
- feedback disable, on page 678
- fragment end-to-end, on page 679
- interface serial, on page 680
- invert, on page 682
- iphc profile, on page 683
- ipv4 iphc profile, on page 684
- keepalive (serial), on page 685
- max-header, on page 687
- non-tcp compression, on page 688
- non-tcp context absolute, on page 689
- refresh max-period, on page 690
- refresh max-time, on page 691
- refresh rtp, on page 692
- rtp, on page 693
- scramble, on page 694
- serial, on page 695
- show iphc idb, on page 696
- show iphc ipv4 rtp, on page 698
- show iphc ipv4 tcp, on page 700
- show iphc platform trace, on page 702
- show iphc profile, on page 704
- show iphc trace all, on page 707
- show tech trace iphc, on page 709
- tcp compression, on page 711
- tcp context absolute, on page 712
• transmit-delay (serial), on page 713
clear iphc ipv4

To clear all Real Time Protocol (RTP) and Transport Control Protocol (TCP) statistics for IP header compression (IPHC) packets sent and received on an interface, use the clear iphc ipv4 command in EXEC mode.

```
clear iphc ipv4 {interface {serial | multilink} interface-path-id | location node-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies the interface to be configured, by type and the interface-path-id argument.</td>
</tr>
<tr>
<td>serial</td>
<td>Specifies a serial network interface.</td>
</tr>
<tr>
<td>multilink</td>
<td>Specifies a multilink network interface.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**location**

Specifies the interface to be configured by its node-id.

**node-id**

Fully qualified path of the node in the rack/slot/module notation.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

The `clear counters` command also clears the IPHC statistics for all the interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear RTP and TCP statistics on an interface:

```
RP/0/RSP0/CPU0:router# clear iphc ipv4 interface Serial 0/1/0/1:26:0
```
The following example shows how to clear RTP and TCP statistics on a node:

```
RP/0/RSP0/CPU0# clear iphc ipv4 location 0/3/CPU0
```

Mon Oct 12 22:47:51.430 DST
**crc (serial)**

To set the length of the cyclic redundancy check (CRC) on a serial interface, use the `crc` command in serial configuration mode. To return the CRC setting on a serial interface to the default setting, use the `no` form of this command.

```
crc {16 | 32}
```

**Syntax Description**

- `16` Sets 16-bit CRC mode.
- `32` Sets 32-bit CRC mode.

**Command Default**
The default is 16 bits for serial interfaces.

**Command Modes**
Serial configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used error checking method throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE standard 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the 32-bit CRC on serial interface 0/3/0/0:10 is enabled:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/0/0:10
RP/0/RSP0/CPU0:router(config-if)# serial
RP/0/RSP0/CPU0:router(config-if-serial)# crc 32
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces, on page 440</td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>
description (IPHC profile)

To add a description to an IPHC profile, use the `description` command in IPHC profile configuration mode. To remove a description for an IPHC profile, use the `no` form of this command.

```
description description
no description
```

**Syntax Description**

- `description` Description to be added to the IPHC profile.

**Command Default**

By default, no description is attached to an IPHC profile.

**Command Modes**

IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `ip-services` read, write

**Examples**

In the following example, a description is attached to the IPHC profile test:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile test type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# description testprofile
RP/0/RSP0/CPU0:router(config-iphc-profile)# commit
```
encapsulation (serial)

To set the Layer 2 encapsulation of an interface, use the `encapsulation` command in interface configuration mode. To restore the system to the default encapsulation, use the `no` form of this command.

```
encapsulation {hdlc | ppp | frame-relay | mfr}
```

**Syntax Description**

- **hdlc**: Enables Cisco High-Level Data Link Control (HDLC) encapsulation on the interface. This is the default encapsulation type.
- **ppp**: Enables PPP encapsulation on the interface.
- **frame-relay**: Enables Frame Relay encapsulation on the interface.
- **mfr**: Enables multilink Frame Relay encapsulation on the interface.

**Command Default**

For serial interfaces, the default encapsulation is HDLC.

**Command Modes**

Interface configuration

**Command History**

- **Release 3.9.0**: This command was introduced.
- **Release 4.0.0**: Frame Relay and Multilink Frame Relay encapsulation was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable PPP encapsulation on serial interface 0/3/0/1:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/1
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces, on page 440</td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show ppp interfaces (BNG), on page 655</td>
<td>Displays PPP state information for an interface.</td>
</tr>
</tbody>
</table>
feedback disable

To disable the IP header compression (IPHC) context status feedback messages on an interface, use the feedback disable command in IPHC profile configuration mode. To re-enable feedback messages after they are disabled, use the no form of this command.

feedback disable

Syntax Description
This command has no keywords or arguments.

Command Default
Feedback messages are enabled by default.

Command Modes
IPHC profile configuration

Command History
Release 4.0.0 This command was introduced.

Usage Guidelines
Feedback disable can be configured only within an IPHC profile.

Note

Task ID
Task ID Operations
ip-services read, write

Examples
The following example shows how to disable the IP header compression (IPHC) context status feedback messages within an IPHC profile:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# feedback disable
```
fragment end-to-end

To enable fragmentation of Frame Relay frames on an interface, use the `fragment end-to-end` command in serial Frame Relay PVC configuration mode. To disable Frame Relay fragmentation, use the `no` form of this command.

```
fragment end-to-end  fragment-size
```

**Syntax Description**

- `fragment-size`: Number of payload bytes from the original Frame Relay frame that go into each fragment. This number excludes the Frame Relay header of the original frame.

  All the fragments of a Frame Relay frame, except the last, have a payload size equal to `fragment-size`; the last fragment has a payload less than or equal to `fragment-size`. Valid values are from 64 to 512 bytes, depending on your hardware.

**Command Default**

Fragmentation is disabled by default.

**Command Modes**

Frame Relay virtual circuit configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Cisco 8-Port Channelized T1/E1 SPA supports fragment sizes of 128, 256, and 512 bytes.

**Examples**

The following example shows how to enter serial Frame Relay virtual circuit configuration mode, set the fragmentation size of Frame Relay frames on subinterface 0/6/2/4.1 to 512 bytes:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/6/2/4.1 point-to-point
RP/0/RSP0/CPU0:router(config-subif)# pvc 100
RP/0/RSP0/CPU0:router(config-fr-vc)# fragment end-to-end 512
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface serial, on page 680</td>
<td>Configures a serial interface and enters interface or subinterface configuration mode.</td>
</tr>
</tbody>
</table>
interface serial

To configure a serial interface and enter interface or subinterface configuration mode, use the `interface serial` command in global configuration mode. To delete a serial configuration, use the `no` form of this command.

```
interface serial interface-path-id [ . subinterface ] { point-to-point | l2transport }
```

**Syntax Description**

- **interface-path-id [subinterface]**: Physical interface or virtual interface followed by the optional subinterface path ID. Naming notation is `interface-path-id.subinterface`. The period in front of the subinterface value is required as part of the notation.
  - For more information about the syntax for the router, use the question mark (?) online help function.

- **point-to-point**: Interface functions as one endpoint of a point-to-point link.

- **l2transport**: Interface functions as one endpoint on an Layer 2 link.

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The <code>. subinterface</code> argument, and the <code>point-to-point</code> and <code>l2transport</code> keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- A slash between values is required as part of the notation.

  - The naming notation for T1 interfaces on a channelized SPA is `rack/slot/module/port/channel-num:channel-group-number`, as shown in the following example:

    ```
    interface serial 0/0/1/2/4:3
    ```

  - If a subinterface is configured under the serial interface, then the router includes the subinterface number at the end of the serial interface address. In this case, the naming notation is `rack/slot/module/port[/channel-num:channel-group-number].subinterface`, as shown in the following example:

    ```
    interface serial 0/0/1/2.1
    ```

  - The naming notation syntax for serial interfaces is as follows:
• **rack**—Chassis number of the rack.

• **slot**—Physical slot number of the modular services card or line card.

• **module**—Module number. Shared port adapters (SPAs) are referenced by their subslot number.

• **port**—Physical port number of the controller.

• **channel-num**—T1 channel number. T1 channels range from 0 to 23.

• **channel-group-number**—Time slot number. T1 time slots range from 1 to 24. The channel-group-number is preceded by a colon and not a slash.

• **subinterface**—Subinterface number.

Use the question mark (?) online help function following the **serial** keyword to view a list of all valid interface choices.

Serial interfaces on channelized T3 can be deleted using the **no channel-group** command in T1 configuration mode. If there are nondefault serial parameters defined, you need to use the **no interface serial** command first to revert to the default configuration, and then delete the serial interface using the **no channel-group** command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enter interface configuration mode for a serial interface in slot 6, subslot 2, port 4, T1 channel number 10 and channel group 8:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/6/2/4/10:8
RP/0/RSP0/CPU0:router(config-if)#
```

The following example shows how to reference the serial interface on channel group 3 of T1 channel group 4 on port 2 of a SPA in subslot 1 and enter subinterface configuration mode:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/0/1/2/4:3
RP/0/RSP0/CPU0:router(config-if)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>channel-group, on page 815</strong></td>
<td>Configures a DS0 channel group and enters channel group configuration mode.</td>
</tr>
<tr>
<td><strong>show interfaces, on page 440</strong></td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>
invert

To invert the data stream on a serial interface, use the `invert` command in serial configuration mode. To disable data inversion, use the `no` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Data is not inverted.

**Command Modes**

Serial configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To verify that data inversion is configured on the interface, use the `show interfaces serial` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, data inversion is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/0/0:10
RP/0/RSP0/CPU0:router(config-if)# serial
RP/0/RSP0/CPU0:router(config-if-serial)# invert
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces, on page 440</code></td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>


**iphc profile**

To create an IP header compression (IPHC) profile and enter the IPHC profile configuration mode, use the **iphc profile** command in configuration mode. To remove the profile, use the **no** form of this command.

**Syntax Description**

```
iphc profile profile-name type {ietf | iphc}
```

- **profile-name**: Text name for the IPHC profile. The maximum number of characters is 50.
- **type**: Specifies the type of compression format.
  - **ietf**: Specifies Internet Engineering Task Force (IETF) standard format. Uses RFC2507 and RFC2508 compression schemes.
  - **iphc**: Specifies Internet Protocol Header Compression (IPHC) format. Provides options similar to IETF.

**Command Default**

No default behavior or values

**Command Modes**

Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you create a profile and enter the IPHC profile configuration mode, you can configure IPHC features in the profile and attach the profile to multiple interfaces. The maximum number of profiles allowed on a router is 250.

A profile cannot be deleted if it is attached to any interfaces. You must remove the profile from all interfaces first. Then, delete the profile using the **no** form of this command.

On-the-fly modifications to IPHC profiles are not supported.

A profile name cannot exceed 50 characters. If you attempt to create a profile name that exceeds 50 characters, you receive the following error message:

```
iphc profile test1test1test1test1test1test1test1test1test1test1 test1 type iphc
!!% 'iphc_profilemgr' detected the 'warning' condition
'Name is longer than allowed character length of 50'
```

**Examples**

The following example shows how to create the IPHC profile Profile_1

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)#
```
ipv4 iphc profile

To attach an IP header compression (IPHC) profile to an interface, use the `ipv4 iphc profile` command in interface configuration mode. To remove the profile from the interface, use the `no` form of this command.

```
ipv4 iphc profile profile-name [mode service-policy]
```

**Syntax Description**

- `profile-name`: Text name of the configured IPHC profile to attach to this interface.
- `mode service-policy`: (Optional) Specifies that the IPHC profile applies to a QoS service policy.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the profile name is not recognized the system returns the following error message:

```
!! 'iphc_ma' detected the 'warning' condition 'Profile doesn't exist'
```

If the encapsulation on the interface is not supported, the system returns the following error message:

```
!! 'iphc_ma' detected the 'warning' condition 'IPHC capability: Encap type not supported'
```

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
<tr>
<td>ipv4</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to attach an IP header compression (IPHC) profile to an interface.

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ipv4 iphc profile Profile_1
```

The following example shows how to attach an IPHC profile that applies to a QoS service policy to an interface:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/1
RP/0/RSP0/CPU0:router(config-if)# ipv4 iphc profile Profile_1 mode service-policy
```
**keepalive (serial)**

To set the keepalive timer for a specific serial interface, use the `keepalive` command in interface configuration mode. To reset the keepalive timer to the default of 10 seconds, use the `no` form of this command.

```
keepalive {interval [retry] | disable}
no keepalive
```

**Syntax Description**

- `interval` Number of seconds (from 1 to 30) between keepalive messages. The default is 10.
- `disable` Turns off the keepalive timer.
- `retry` (Optional) Number of keepalive messages (from 1 to 255) that can be sent to a peer without a response before transitioning the link to down state. The default is 5.

**Command Default**

The default interval is 10 seconds between keepalive messages. The default retry is 5 keepalive messages that can be sent without a response. However, when more than 5 keepalive messages are sent to a peer without a response, the link transitions to the down state.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

HDLC keepalives require that the `keepalive` command is configured the same way on both ends of a single connection. The two connected routers have no way of negotiating the keepalive value because there is no way for one router to tell the other about its configured values. The keepalive value configured on each router (local or partner) sets the rate at which the Cisco IOS XR software sends packets. It also sets the rate at which the local end expects to receive incoming packets.

To set the keepalive value to the default value, use the `keepalive` command without specifying a value for the `interval` argument.

By default, if more than five keepalive messages are sent to a peer and no response is received from the peer, then the link transitions to the down state.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure keepalives for 3 seconds on serial interface 0/7/0/1:

```
RP/0/RSP0/CPU0:router(config)# interface serial 0/7/0/1
RP/0/RSP0/CPU0:router(config-if)# keepalive 3
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces, on page 440</code></td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>
max-header

To define the maximum size header that can be compressed, use the `max-header` command in IPHC profile configuration mode. To return to the default maximum size, use the `no` form of this command.

```
max-header number-of-bytes
no max-header [number-of-bytes]
```

**Syntax Description**

- `number-of-bytes` Maximum size, in bytes, of a header that can be compressed. The range is from 20 to 40. The default is 40.

**Command Default**

`Number-of-bytes`; 40.

**Command Modes**

IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The maximum header size can be configured only within an IPHC profile.

**Task ID**

- `Task ID` Operations
  - `ip-services` read,
  - `write`

**Examples**

The following example shows how to define the maximum size header that can be compressed.

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# max-header 20
```
**non-tcp compression**

To enable non-TCP compression in an IP header compression (IPHC) profile, use the `non-tcp compression` command in IPHC profile configuration mode. To disable non-TCP compression in the profile, use the `no` form of this command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

No default behavior or values

### Command Modes

IPHC profile configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

**Note**

NON-TCP compression can be enabled only within an IPHC profile. Non-TCP compression does not work unless it is enabled under a profile.

### Examples

The following example shows how to enable NON-TCP compression within an IP header compression (IPHC) profile:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# non-tcp compression
```
The following example shows how to enable non-TCP compression within an IP header compression (IPHC) profile:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# non-tcp context absolute 255
```
refresh max-period

To configure the maximum number of compressed IP header packets exchanged on a link before IPHC context is refreshed, use the `refresh max-period` command in IPHC profile configuration mode. To return to the default context refresh settings, use the `no` form of this command.

```
refresh max-period {max-number | infinite}
```

**Syntax Description**

- `max-number`: Maximum number of compressed IP header packets allowed between full headers or before the context is refreshed. Range is from 0 to 65535.
- `infinite`: Allows an unlimited number of packets to be exchanged before context refresh.

**Command Default**

```
max-number: 256
```

**Command Modes**

IPHC profile configuration

**Command History**

Release 4.0.0  This command was introduced.

---

**Usage Guidelines**

To enable the configured context refresh settings for RTP packets, the `refresh rtp` command must be used.

---

**Note**

The maximum period between context refreshes can be set only within an IPHC profile.

**Task ID**

```
Task ID  Operations
ip-services read, write
```

**Examples**

The following example shows how to configure the maximum number of compressed IP header packets that are exchanged on a link before the context is refreshed, in an IPHC profile.

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# refresh max-period 50
```
**refresh max-time**

To configure the maximum time allowed between context refreshes, use the `refresh max-time` command in IPHC profile configuration mode. To return to the default context refresh settings, use the `no` form of this command.

```
refresh max-time {max-time | infinite}
```

**Syntax Description**

- `max-time` Time, in seconds, between context refreshes. Range is from 0 to 255.
- `infinite` Allows an unlimited time to pass between context refreshes.

**Command Default**

`max-time: 5`

**Command Modes**

IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enable the configured context refresh settings for RTP packets, the `refresh rtp` command must be used.

**Note**

The maximum time between context refreshes can be set only within an IPHC profile.

**Examples**

The following example shows how to configure the maximum allowed time between context refreshes as 60 seconds, in the IPHC profile ‘Profile 1’:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# refresh max-time 60
```
refresh rtp

To enable the configured context refresh settings for RTP packets, use the **refresh rtp** command in IPHC profile configuration mode. To disable context refresh settings for RTP packets, use the **no** form of this command.

```
refresh rtp
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
By default, refresh RTP is disabled and only the first packet in the flow is sent as a ‘full-header’ packet.

**Command Modes**
IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable the configured refresh settings for RTP packets:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# refresh rtp
```
rtp

To enable Real Time Protocol (RTP) compression and decompression on the interface, use the rtp command in IPHC profile configuration mode. To remove RTP from the interface, use the no form of this command.

rtp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

IPHC profile configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Note

RTP can be enabled only within an IPHC profile.

You must enable RTP before attaching a profile to an interface. If you do not enable RTP first, the router will display the following message: ’!!! 'iphc_capability' detected the 'warning' condition 'IPHC Capability: RTP Compression NOT enabled in the profile'!

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# rtp
```
**scramble**

To enable payload scrambling (encryption) on a serial interface, use the `scramble` command in interface configuration mode. To disable scrambling, use the `no` form of this command.

**scramble**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Scrambling is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns—in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

The local interface configuration must match the remote interface configuration. For example, if you enable scrambling on the local port, you must also do the same on the remote port.

To verify that scrambling is configured on the interface, use the `show interfaces serial` command.

**Task ID**

**Examples**

In the following example, scrambling is enabled on serial interface 0/3/0/0/0:10:

```
RP/0/RSP0/CPU0:router (config) # interface serial 0/3/0/0/0:10
RP/0/RSP0/CPU0:router (config-if) # serial
RP/0/RSP0/CPU0:router (config-if-serial) # scramble
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers t3</code>, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
To configure the serial parameters and enter serial configuration mode, use the `serial` command in interface configuration mode. To return to the default state of the serial interface, use the `no` form of this command.

**serial**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Serial interfaces are automatically created for unchannelized ports; for channelized ports, serial interfaces are created when you add T1/E1 channel groups.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdlc</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enter serial configuration mode:

```
RP/0/RSP0/CPU0:router(config-if)# serial
RP/0/RSP0/CPU0:router(config-if-serial)#
```
**show iphc idb**

To display status information for an IP header compression (IPHC) interface description block (IDB), use the `show iphc idb` command in EXEC mode.

```
show iphc idb {detail | interface type interface-path-id [detail] | location node-id [detail]}
```

**Syntax Description**

- **detail**: Includes statistics information and internal data.
- **interface**: Specifies the interface for which IPHC information is to be displayed.
- **type**: Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id**: Physical interface or virtual interface.
  
  **Note**: Use the `show interfaces` command to see a list of all interfaces currently configured on the router.
  
  For more information about the syntax for the router, use the question mark (?) online help function.
- **location**: Specifies the node location for which IPHC information is to be displayed.
- **node-id**: Specifies the fully qualified path of a node.
  
  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

The default (no parameters) displays information for all interfaces configured for IPHC.

**Command Modes**

EXEC

**Command History**

- **Release 4.0.0**: This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to display status information for an IP header compression (IPHC) interface description block (IDB).

```
RP/0/RSP0/CPU0:router# show iphc idb interface Serial 0/1/0/1/26:0
Thu Jan 8 20:25:41.079 UTC
EA Status Codes: Neg Status Code:
```

696
Serial Interface Commands

show iphc idb

Thu Jan  8 20:25:44.731 UTC
EA Status Codes: Neg Status Code:
CFG_AS: Cfg Apply Succeed  NEG_I: Negotiation Init
CFG_AF: Cfg Apply Failed    NEG_P: Negotiation Progress
NEG_AS: Neg Apply Succeed   NEG_D: Negotiation Done
NEG_AF: Neg Apply Failed    NEG_F: Negotiation Failed

Interface_Name: Serial0/1/0/1/26:0  Ifhandle : 0x02008e00
EA Status : NEG_AS               Neg Status: NEG_D
MQC Mode   : F                    Prof_Name : iphcfmt

show iphc idb interface Serial 0/1/0/1/26:0  detail

Thu Jan  8 20:25:44.731 UTC
EA Status Codes: Neg Status Code:
CFG_AS: Cfg Apply Succeed  NEG_I: Negotiation Init
CFG_AF: Cfg Apply Failed    NEG_P: Negotiation Progress
NEG_AS: Neg Apply Succeed   NEG_D: Negotiation Done
NEG_AF: Neg Apply Failed    NEG_F: Negotiation Failed

Interface_Name: Serial0/1/0/1/26:0  Ifhandle : 0x02008e00
EA Status : NEG_AS               Neg Status: NEG_D
MQC Mode   : F                    Prof_Name : iphcfmt

<table>
<thead>
<tr>
<th>Tcp</th>
<th>Non-Tcp</th>
<th>Max</th>
<th>Max</th>
<th>Max</th>
<th>RTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space</td>
<td>Space</td>
<td>Header</td>
<td>Period</td>
<td>Time</td>
<td></td>
</tr>
<tr>
<td>Cfg_Option</td>
<td>1</td>
<td>60</td>
<td>40</td>
<td>256</td>
<td>5</td>
</tr>
<tr>
<td>Neg_Option</td>
<td>1</td>
<td>50</td>
<td>40</td>
<td>256</td>
<td>5</td>
</tr>
</tbody>
</table>
**show iphc ipv4 rtp**

To display IPv4 statistics for Real Time Protocol (RTP) and User Datagram Protocol (UDP) packets sent and received on an interface, use the `show iphc ipv4 rtp` command in EXEC mode.

```
show iphc ipv4 rtp interface type interface-path-id [location node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>location</code></td>
<td>(Optional) Specifies the location of the interface</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>(Optional) Node-id entered in the rack/slot/module notation.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Caution

These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly, there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display IPv4, Real Time Protocol (RTP), User Datagram Protocol (UDP), and Non-Transmission Control Protocol (non-TCP) statistics about IP header compression (IPHC) packets sent and received on an interface:
show iphc ipv4 rtp interface Serial 0/0/1/26:0

Thu Jan  8 20:28:47.569 UTC
RTP/UDP/IP header compression statistics:
  Interface Serial0/0/1/26:0
  Rcvd: 100 total, 93 compressed, 7 full header
  0 dropped, 0 status msgs
  Sent: 0 total, 0 compressed, 0 fullheader, 0 status msgs
  0 bytes saved, 0 bytes sent
  1.00 efficiency improvement factor
show iphc ipv4 tcp

To display IPv4 Transport Control Protocol (TCP) statistics about IP header compression (IPHC) packets sent and received on an interface, use the `show iphc ipv4 tcp` command in EXEC mode.

```
show iphc ipv4 tcp [interface type interface-path-id [location node-id]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>(Optional) Specifies the location of the interface</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>(Optional) Node-id entered in the <code>rack/slot/module</code> notation.</td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

⚠️ **Caution**

These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly, there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display IPv4, Transport Control Protocol (TCP) statistics about IP header compression (IPHC) packets sent and received on an interface:

```
RP/0/RSP0/CPU0:router# show iphc ipv4 tcp interface Serial 0/1/0/1/26:0
```
TCP/IP header compression statistics:
Interface Serial0/1/0/1/26:0
   Rcvd:  100 total, 93 compressed, 7 full header
         0 dropped, 0 status msgs
   Sent:  0 status msgs
show iphc platform trace

To display platform trace information, such as errors or statistics for a file or a node, use the `show iphc platform trace` command in EXEC mode.

```
show iphc platform trace [{all | events | errors [events] [all] | internal [{all | errors [events] [all] | events [all]}]} [{unique | wrapping}] [hexdump] [last number-of-entries] [reverse] [stats] [tailf] [verbose] [{file file-name original location node-id | location {node-id | all | mgmt-nodes}}]
```

**Syntax Description**

- `all` (Optional) Displays all platform trace information.
- `events` (Optional) Displays event platform trace information.
- `unique` (Optional) Displays trace information for unique entries with counts.
- `wrapping` (Optional) Displays wrapping entries.
- `hexdump` (Optional) Displays trace information in hexadecimal format.
- `last number_of_entries` (Optional) Displays trace information for the last specified number of entries. The range is 1 to 4294967295.
- `reverse` (Optional) Displays trace information in reverse order (latest traces first).
- `stats` (Optional) Displays statistics information for the trace.
- `tailf` (Optional) Displays new traces as they are added.
- `verbose` (Optional) Displays internal debugging information.
- `file file-name` (Optional) Displays trace information for the specified file.
- `original` (Optional) Specifies the original location of file.
- `location node_id` (Optional) Displays trace information for the specified card location.
- `all` (Optional) Displays trace information for all nodes.
- `mgmt-nodes` (Optional) Displays trace information for all management nodes.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

**Release** | **Modification**
--- | ---
Release 4.0.0 | This command was introduced.

**Usage Guidelines**

The keywords `hexdump`, `last`, `reverse`, `stats`, `tailf`, and `verbose` may be entered in any order.
Use of the keywords `file` and `location` allows any number of desired files or locations to be entered. For more information, use the question mark (?) online help function.

⚠️ Caution

These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly, there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display platform trace information for a specified location:

```
RP/0/RSP0/CPU0:router# show iphc platform trace all location 0/2/CPU0
Mon Aug 16 06:05:17.906 PDT
6 wrapping entries (24576 possible, 0 filtered, 6 total)
Aug 16 05:53:59.674 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: LC Platform preinit
Aug 16 05:54:00.255 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: LC Platform init
Aug 16 05:54:00.255 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: max iphc interfaces 2048
Aug 16 05:54:00.284 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: ea respawn count 1
Aug 16 05:54:00.284 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: LC Platform replay end
Aug 16 05:54:00.284 iphc_ea/internal 0/2/CPU0 t1 PAL IPHC: replay end 0 stale entries
```
show iphc profile

To display the configuration information of an IP header compression (IPHC) profile, use the `show iphc profile` command in EXEC mode.

```
show iphc profile {profile-name | all} [detail]
```

**Syntax Description**
- `profile-name` Text name of the IPHC profile for which to display information.
- `all` Displays information for all profiles on the router.
- `detail` (Optional) Displays the interfaces to which the profile is attached.

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**
- **Release** 4.0.0 This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- **Task ID** Operations
  - ip-services read

**Examples**
The following examples show how to display information about an IPHC profile:

```
RP/0/RSP0/CPU0:router# show iphc profile ietf-test1
Tue Aug 10 06:53:19.711 PDT
IPHC Profile: ietf-test1
Type: IETF
Compressing : TCP NON-TCP (RTP)
Context : TCP fixed at 1 NON-TCP fixed at 10
Refresh : NON-TCP every 60 seconds or 100 packets
Feedback : ON
Max_Header : 40
Refresh RTP : OFF

RP/0/RSP0/CPU0:router# show iphc profile Profile_1 detail
Thu Jan 8 20:22:24.276 UTC
IPHC Profile: Profile_1
Type: IPHC
Compressing : TCP NON-TCP (RTP)
Context : TCP fixed at 1 NON-TCP fixed at 60
Refresh : NON-TCP every 5 seconds or 256 packets
Feedback : ON
```
show iphc profile all
displaying iphc profiles

IPHC Profiles: 3

IPHC Profile: p1
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

IPHC Profile: p2
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

IPHC Profile: test
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

show iphc profile all detail
displaying iphc profiles in detail

IPHC Profiles: 3

IPHC Profile: p1
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

*** No of Intf 1 ****
Serial0_4_3_1_1:0

IPHC Profile: p2
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

*** No of Intf 2 ****
Serial0_4_3_1_2:0
Serial0_4_3_1_8:0

IPHC Profile: test
Type: IETF
Compressing: TCP NON-TCP (RTP)
Context: TCP fixed at 1 NON-TCP fixed at 16
Refresh: NON-TCP every 5 seconds or 256 packets
Feedback: ON
Max_Header: 40

*** No of Intf 0 ****
### show iphc trace all

To display trace results for all IP header compression (IPHC) configurations on the router, use the `show iphc trace all` command in EXEC mode.

```
show iphc trace all [unique | wrapping] [hexdump] [last number-of-entries] [reverse] [stats] [tailf] [verbose] [{file file-name original location node-id | location {node-id | all | mgmt-nodes}}]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unique</td>
<td>(Optional) Displays trace information for unique entries with counts.</td>
</tr>
<tr>
<td>wrapping</td>
<td>(Optional) Displays wrapping entries.</td>
</tr>
<tr>
<td>hexdump</td>
<td>(Optional) Displays trace information in hexadecimal format.</td>
</tr>
<tr>
<td>last</td>
<td>(Optional) Displays trace information for the last specified number of entries. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td>reverse</td>
<td>(Optional) Displays trace information in reverse order (latest traces first).</td>
</tr>
<tr>
<td>stats</td>
<td>(Optional) Displays statistics information for the trace.</td>
</tr>
<tr>
<td>tailf</td>
<td>(Optional) Displays new traces as they are added.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Displays internal debugging information.</td>
</tr>
<tr>
<td>file file-name</td>
<td>(Optional) Displays trace information for the specified file.</td>
</tr>
<tr>
<td>original</td>
<td>(Optional) Specifies the original location of file.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Displays trace information for the specified card location.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Displays trace information for all nodes.</td>
</tr>
<tr>
<td>mgmt-nodes</td>
<td>(Optional) Displays trace information for all management nodes.</td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values

#### Command Modes

EXEC mode

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The keywords `hexdump`, `last`, `reverse`, `stats`, `tailf`, and `verbose` may be entered in any order. The keywords `unique` or `wrapping` may only be entered as the first keyword in the command. The keywords `file` or `location` may only be entered as the last keyword in the command.

Use of the keywords `file` and `location` allows any number of desired files or locations to be entered. For more information, use the question mark (?) online help function.
These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. If used incorrectly, there is some risk that they may cause performance or other issues that impact products, and we highly recommend that you contact Cisco Technical Support before using any of these commands.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows how to display IPHC trace information:

```
RP/0/RSP0/CPU0:router# show iphc trace all

20 wrapping entries (3072 possible, 0 filtered, 20 total)
Jul 22 03:31:39.770 iphc/profilemgr/int 0/5/CPU0 t1 : Event Mgr Create Success
Jul 22 03:31:39.799 iphc/profilemgr/int 0/5/CPU0 t1 : Sysmgr Init Successful
Jul 22 03:31:39.894 iphc/profilemgr/int 0/5/CPU0 t1 : Ens Init Successful
Jul 22 03:31:39.910 iphc/profilemgr/int 0/5/CPU0 t1 : Sysdb Init Successful
Jul 22 03:31:39.911 iphc/profilemgr/int 0/5/CPU0 t1 : Stats thread Init Success
Jul 22 03:31:39.942 iphc/profilemgr/int 0/5/CPU0 t1 : Cfg thread Init Success
Jul 22 03:31:39.951 iphc/profilemgr/int 0/5/CPU0 t1 : Registered verifier call
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1 : Scanning Profile: *** Fr*
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1 : +++++ Profile Verification
Jul 22 03:31:39.952 iphc/profilemgr/eve 0/5/CPU0 t1 : Verify Profile (Profile_n
Jul 22 03:31:39.981 iphc/profilemgr/int 0/5/CPU0 t1 : Registered applier calle
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
show tech-support iphc

To collect and display IP header compression (IPHC) data for an interface, node, or rack, and store that data in a file, use the `show tech-support iphc` command in EXEC mode.

```
show tech-support iphc [{file|interface type interface-path-id [{location node-id|rack rack_name}] | location node-id | rack rack_name}] file location file_name [background] [{compressed | uncompressed}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>(Optional) Specifies a file name and location for IPHC data to be saved to.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Collects IPHC data for the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Collects IPHC data for the specified card location (node-id).</td>
</tr>
<tr>
<td>rack rack_name</td>
<td>(Optional) Collects IPHC data for the specified rack.</td>
</tr>
<tr>
<td>file location</td>
<td>Stores the collected data in the specified file (file_name) in one of the following valid file locations:</td>
</tr>
<tr>
<td>file_name</td>
<td>• bootflash:—stores the collected data to a bootflash file-system file.</td>
</tr>
<tr>
<td></td>
<td>• compactflash:—stores the collected data to a compactflash file-system file.</td>
</tr>
<tr>
<td></td>
<td>• compactflasha:—stores the collected data to a compactflasha file-system file.</td>
</tr>
<tr>
<td></td>
<td>• disk0:—stores the collected data to a disk0 file-system file.</td>
</tr>
<tr>
<td></td>
<td>• disk0a:—stores the collected data to a disk0a file-system file.</td>
</tr>
<tr>
<td></td>
<td>• disk1:—stores the collected data to a disk1 file-system file.</td>
</tr>
<tr>
<td></td>
<td>• disk1a:—stores the collected data to a disk1a file-system file.</td>
</tr>
<tr>
<td></td>
<td>• ftp:—stores the collected data to an ftp file-system file.</td>
</tr>
<tr>
<td></td>
<td>• harddisk:—stores the collected data to a harddisk file-system file.</td>
</tr>
<tr>
<td></td>
<td>• harddiska:—stores the collected data to a harddiska file-system file.</td>
</tr>
<tr>
<td></td>
<td>• harddiskjb:—stores the collected data to a harddiskjb file-system file.</td>
</tr>
<tr>
<td></td>
<td>• lcedisk0:—stores the collected data to a lcedisk0 file-system file.</td>
</tr>
<tr>
<td></td>
<td>• lcedisk0a:—stores the collected data to a lcedisk0a file-system file.</td>
</tr>
<tr>
<td></td>
<td>• nvram:—stores the collected data to an nvram file-system file.</td>
</tr>
<tr>
<td></td>
<td>• rcp:—stores the collected data to an rcp file-system file.</td>
</tr>
<tr>
<td></td>
<td>• tftp:—stores the collected data to a tftp file-system file.</td>
</tr>
<tr>
<td>background</td>
<td>(Optional) Runs this command in the background.</td>
</tr>
</tbody>
</table>
show tech-support iphc

<table>
<thead>
<tr>
<th>compressed</th>
<th>(Optional) Compresses the output.</th>
</tr>
</thead>
<tbody>
<tr>
<td>uncompressed</td>
<td>(Optional) Does not compress the output.</td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values

**Command Modes**
EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-services</td>
<td>read</td>
</tr>
<tr>
<td>cisco-support</td>
<td>read</td>
</tr>
<tr>
<td>ipv4</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to collect and display IP header compression (IPHC) data:

```
RP/0/RSP0/CPU0:router# show tech-support iphc
Mon Oct 12 20:30:58.660 DST  
++ Show tech start time: 2009-Oct-12.203059.DST ++
Mon Oct 12 20:31:05 DST 2009 Waiting for gathering to complete
......
Mon Oct 12 20:31:46 DST 2009 Compressing show tech output
Show tech output available at 0/5/CPU0 : disk0:/showtech/showtech-iphc-2009-Octz
++ Show tech end time: 2009-Oct-12.203148.DST ++
```
tcp compression

To enable TCP compression in an IP header compression (IPHC) profile, use the `tcp compression` command in IPHC profile configuration mode. To disable TCP compression in the profile, use the `no` form of this command.

### tcp compression

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Where the IPHC profile used by a router is configured using this command, the router will negotiate TCP compression with its peer router and decompress any compressed TCP packets sent by its peer. TCP packets transmitted to the peer are transmitted uncompressed.

**Note**

TCP compression can be enabled only within an IPHC profile. TCP compression does not work unless it is enabled under a profile.

**Task ID**

**Task ID** | **Operations**
---|---
ip-services | read, write

**Examples**

The following example shows how to enable TCP compression within an IP header compression (IPHC) profile:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# tcp compression
```

```
tcp context absolute

To configure the maximum number of TCP contexts that are allowed for IPHC under a profile, use the `tcp context absolute` command in IPHC profile configuration mode. To remove the TCP context from the profile, use the `no` form of this command.

**tcp context absolute number-of-contexts**

**Syntax Description**

`number-of-contexts` Numeric value that specifies the maximum number of TCP contexts allowed for IPHC under this profile. The range is from 0 to 255.

**Command Default**

If `number-of-contexts` is not specified, and only TCP compression is enabled, the default `number-of-contexts` is 1.

**Command Modes**

IPHC profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The maximum allowed number of tcp contexts on a Line Card, across all IPHC profiles and interfaces, is 255.

**Note**

TCP context can be set only within an IPHC profile.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable TCP compression within an IP header compression (IPHC) profile:

```
RP/0/RSP0/CPU0:router(config)# config
RP/0/RSP0/CPU0:router(config)# iphc profile Profile_1 type iphc
RP/0/RSP0/CPU0:router(config-iphc-profile)# tcp context absolute 255
```
transmit-delay (serial)

To specify a number of High-Level Data Link Control (HDLC) flag sequences to be inserted between the packets, use the `transmit-delay` command in serial configuration mode. To restore the default, use the `no` form of this command.

```
transmit-delay  microseconds
```

### Syntax Description

- **microseconds**: Number of microseconds of minimum delay after sending a packet. Range is from 0 to 128. The default is 0 (disabled).

### Command Default

- **microseconds**: 0 (disabled)

### Command Modes

- Serial configuration

### Command History

- **Releases**
  - Release 3.9.0: This command was introduced.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Examples

In the following example, a delay of 2 microseconds is specified on serial interface 0/3/0/0/0:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/RSP0/CPU0:router(config-if)# serial
RP/0/RSP0/CPU0:router(config-if-serial)# transmit-delay 2
```

In the following example, the transmit delay on serial interface 0/3/0/0/0:0 is disabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/RSP0/CPU0:router(config-if)# serial
RP/0/RSP0/CPU0:router(config-if-serial)# no transmit-delay
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces</code>, on page 440</td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>
transmit-delay (serial)
SONET Controller Commands

This module provides command line interface (CLI) commands for configuring SONET operation, using Layer 1 SONET transport technology, on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

The configuration of the SONET controller includes SONET Automatic Protection Switch (APS), which is a feature offering recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. You must configure a SONET controller before you can configure a Packet-over-SONET/SDH (POS) interface or a serial interface.

All SONET-related configurations of a SONET-based physical port are grouped under the SONET controller configuration submode. The SONET path-related configuration commands are grouped under the SONET path submode.

- ais-shut (SONET), on page 717
- ais-shut (SONET path), on page 718
- aps group, on page 719
- aps group (global), on page 722
- au, on page 724
- authenticate (PGP), on page 726
- b3-ber-prdi, on page 728
- channel local, on page 729
- channel remote, on page 731
- clear counters sonet, on page 733
- clock source (SONET), on page 735
- controller (SONET), on page 736
- delay clear, on page 738
- delay trigger, on page 739
- down-when-looped, on page 740
- framing (SONET), on page 741
- line delay clear, on page 742
- line delay trigger, on page 743
- lockout, on page 744
- loopback (SONET), on page 745
- mode (SONET), on page 746
• overhead (SONET), on page 748
• overhead (SONET path), on page 750
• path delay clear, on page 752
• path delay trigger, on page 753
• path (SONET), on page 754
• report (SONET), on page 756
• report (SONET path), on page 758
• revert, on page 760
• scrambling disable (SONET path), on page 762
• show aps, on page 763
• show aps agents, on page 765
• show aps group, on page 767
• show controllers pos, on page 769
• show controllers sonet, on page 775
• show sonet-local trace frr, on page 782
• shutdown (SONET), on page 783
• signalling, on page 784
• sts, on page 785
• timers (APS), on page 786
• threshold (SONET), on page 788
• threshold (SONET path), on page 790
• tug3, on page 791
• uneq-shut (SONET path), on page 792
• unidirectional, on page 793
• width, on page 795
ais-shut (SONET)

To enable automatic insertion of a line alarm indication signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the `ais-shut` command in SONET/SDH configuration mode. To disable automatic insertion of a LAIS, use the `no` form of this command.

**ais-shut**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

This command is disabled by default; no AIS is sent.

**Command Modes**

SONET configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 3.9.0 This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the line is placed in administrative shutdown state, use the `ais-shut` command to send a signal to downstream equipment that indicates that there is a problem with the line.

The `ais-shut` command is ignored if automatic protection switching (APS) is running for the corresponding port, because the setting must be enabled for proper APS operation.

For SONET ports that do not have hardware support for LAIS insertion, the `ais-shut` command is disabled.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the alarm indication is forced on the SONET OC-3 controller:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# ais-shut
```
ais-shut (SONET path)

To enable automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state, use the ais-shut command in SONET/SDH path configuration mode. To disable automatic insertion of PAIS in the SONET signal, use the no form of this command.

ais-shut

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

SONET/SDH path configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the ais-shut command to enable automatic insertion of PAIS in the appropriate sent SONET path overhead whenever the corresponding SONET path enters the administratively down state.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows the alarm indication being enabled on all paths:

RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# ais-shut

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
**aps group**

To manually switch an automatic protection switching (APS) channel, use the `aps group` command in EXEC mode.

```
aps group number {force | manual} {0 | 1} {disable | enable}
```

**Syntax Description**

- `number`: Number of the APS group. Range is from 1 to 255.
- `force`: Sends a forced APS request at the local end of a SONET link with the assigned channel number.
- `manual`: Sends a manual APS request at the local end of a SONET link with the assigned channel number, which is implemented when no other higher-priority user-initiated or automatic requests are in effect.
- `0`: Specifies that the protect channel should be switched.
- `1`: Specifies that the working channel should be switched.
- `disable`: Stops sending the SONET K1/K2 bit pattern that informs the remote end to switch ports.
- `enable`: Starts sending a SONET K1/K2 bit pattern to inform the remote end to switch ports.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In a multirouter APS topology, a manual or force request is supported only on the protect router.

Specify 0 or 1 to identify on which channel the traffic should be stopped and switched to the other channel. Therefore, `force 0` or `manual 0` moves traffic from the protect to the working channel, and `force 1` or `manual 1` moves traffic from the working to the protect channel.

Use the `force` keyword to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (using the `lockout` command) overrides a force request.

**Note**

If a request of equal or higher priority is in effect, you cannot use the `force` keyword to initiate a forced APS request at the local end of the SONET link.

Use the `manual` keyword to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the `manual` keyword to revert the communication link to the working channel before the
wait to restore (WTR) time period has expired. The WTR time period is set by the \texttt{revert} command. Use the \texttt{no} form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

### Examples

The following examples show how to use the \texttt{aps group} command in EXEC mode to force or manually switch traffic, and enable and disable sending of the K1/K2 bit pattern to signal the switchover to the remote end:

**Forced Switchover Request From Working to Protect Channel**

```
RP/0/RSP0/CPU0:router# aps group 1 force 1 enable
RP/0/RSP0/CPU0:router# aps group 1 force 1 disable
```

**Manual Switchover Request From Working to Protect Channel**

```
RP/0/RSP0/CPU0:router# aps group 1 manual 1 enable
RP/0/RSP0/CPU0:router# aps group 1 manual 1 disable
```

**Forced Switchover Request from Protect to Working Channel**

```
RP/0/RSP0/CPU0:router# aps group 1 force 0 enable
RP/0/RSP0/CPU0:router# aps group 1 force 0 disable
```

**Manual Switchover Request From Protect to Working Channel**

```
RP/0/RSP0/CPU0:router# aps group 1 manual 0 enable
RP/0/RSP0/CPU0:router# aps group 1 manual 0 disable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{aps group} (global), on page 722</td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td>\texttt{lockout}, on page 744</td>
<td>Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.</td>
</tr>
<tr>
<td>\texttt{revert}, on page 760</td>
<td>Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.</td>
</tr>
<tr>
<td>\texttt{signalling}, on page 784</td>
<td>Configures the K1K2 overhead byte signaling protocol used for APS.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show aps</code>, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
aps group (global)

To add an automatic protection switching (APS) group and enter APS group configuration mode, use the `aps group` command in Global Configuration mode. To remove a group, use the no form of this command.

```
aps group number
```

**Syntax Description**

- `number` Number of the group. Range is from 1 to 255.

**Command Default**

No APS groups are defined.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An APS group contains one protect (P) SONET port and one working (W) SONET port. The working and protect ports can reside on the same logical channel (LC), on different LCs in the same router, or on different routers. One APS group must be configured for each protect port and its corresponding working ports.

Use the `aps group (global)` command to enter APS group configuration mode and configure APS connections with other SONET equipment.

**Examples**

The following example shows how to use the `aps group` command in global configuration mode to configure APS group 1 and enter APS group configuration mode:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group</code>, on page 719</td>
<td>Manually switches an APS channel.</td>
</tr>
<tr>
<td><code>authenticate (PGP)</code>, on page 726</td>
<td>Configures the authentication string for the PGP message exchange between the protect and working routers.</td>
</tr>
<tr>
<td><code>channel local</code>, on page 729</td>
<td>Assigns local SONET physical ports as SONET APS channels in the current APS group.</td>
</tr>
<tr>
<td><code>channel remote</code>, on page 731</td>
<td>Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lockout, on page 744</td>
<td>Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.</td>
</tr>
<tr>
<td>revert, on page 760</td>
<td>Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.</td>
</tr>
<tr>
<td>signalling, on page 784</td>
<td>Configures the K1K2 overhead byte signaling protocol used for APS.</td>
</tr>
<tr>
<td>timers (APS), on page 786</td>
<td>Changes the time between hello packets and the time before the protect interface process declares a working interface router to be down.</td>
</tr>
<tr>
<td>unidirectional, on page 793</td>
<td>Configures a protect interface for unidirectional mode.</td>
</tr>
<tr>
<td>show aps, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
au

To specify the administrative unit (AU) group number and enter the AU controller configuration mode, use the **au** command in SONET controller configuration mode.

**au number**

**Syntax Description**

- **number**  Administrative unit group number in the range from 1 to 48.

**Command Default**

The default is 1.

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **au** command enables you to begin configuring the interface in the AU controller configuration mode, where you can configure tributary unit groups (TUGs), virtual containers (VCs), and DS3s, such as shown in the following path example:

STM-1 -> AU-4 -> TUG-3 -> VC-3 -> DS-3

One AU-4 path is equivalent to three AU-3 paths. An administrative unit type 4 (AU-4) consists of three STM-1s or one STM-3. An administrative unit type 3 (AU-3) consists of one STM-1.

**Note**

Use the **au** command to configure one of the AUGs available for your card. The **au** command is not used to configure the type of AU path that you are configuring, such as AU-3 or AU-4, but rather is used to identify one AU group number in the supported range for the card and AU type that you are configuring. For example, the 1-Port Channelized OC-48/STM-16 SPA supports 16 AU-4 groups. Therefore, you can specify a number between 1 and 16 for the **au** command to configure SDH AU-4 on that card.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify AU 1.

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# au 1
RP/0/RSP0/CPU0:router(config-auPath)#
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tug3, on page 791</td>
<td>Specifies the tributary unit group (TUG) number and enters the TUG3 controller configuration mode.</td>
</tr>
</tbody>
</table>
authenticate (PGP)

To configure the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers, use the `authenticate` command in APS group configuration mode. To revert to the default authentication string, use the `no` form of this command.

```
authenticate string
```

**Syntax Description**

| `string` | Authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted. |

**Command Default**

The default authentication string is “cisco.”

**Command Modes**

APS group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `authenticate` command to configure the authentication string for the PGP message exchange between the protect and working routers. Use the `no` form of this command to revert to the default authentication string.

The `authenticate` command applies only in multirouter automatic protection switching (APS) group configurations.

In multirouter APS topologies, the protect and working routers communicate with each other through the User Datagram Protocol (UDP)-based Pretty Good Privacy protocol. Each Pretty Good Privacy packet contains an authentication string used for packet validation. The authentication string on all routers involved in the same APS group operation must match for proper APS operation.

**Examples**

The following example enables authentication for APS group 1 in abctown:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# authenticate abctown
```

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aps group (global), on page 722</td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>channel local, on page 729</td>
<td>Assigns local SONET physical ports as SONET APS channels in the current APS group.</td>
</tr>
<tr>
<td>channel remote, on page 731</td>
<td>Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.</td>
</tr>
<tr>
<td>show aps, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
b3-ber-prdi

To enable sending of a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded, use the **b3-ber-prdi** command in SONET/SDH path configuration mode. To disable sending a PRDI, use the **no** form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

This command is disabled by default; a PRDI is not sent.

**Command Modes**

SONET/SDH path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows a PRDI enabled on all paths:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# b3-ber-prdi
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path (SONET), on page 754</td>
<td>Enters SONET/SDH path configuration mode.</td>
</tr>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
channel local

To assign local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group, use the `channel local` command in APS group configuration mode. To return to the default setting, use the `no` form of this command.

```
channel {0 | 1} local [preconfigure] sonet interface-path-id
no channel {0 | 1} local [preconfigure] sonet interface-path-id
```

**Syntax Description**

| {0 | 1} | Assigns a protect or working channel type. 0 is protect, 1 is working. |
|---|---|
| preconfigure | (Optional) Specifies a SONET preconfiguration. This keyword is used only when a modular services or line card is not physically installed in a slot. |
| sonet | Specifies a SONET interface type. |
| interface-path-id | Physical interface or virtual interface. |

**Note** Use the `show controllers sonet` command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

A SONET APS local channel is not assigned.

**Command Modes**

APS group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the `channel local` command to designate SONET physical ports as SONET APS channels in the current APS group. Use the `channel remote` command to assign channels that are physically located in a different router.
Preconfigured interfaces are supported.

If the protect channel is local, it must be assigned using a `channel` command before any of the working channels are assigned. The reason is that having only a working channel assigned is a valid configuration for a working router in a multirouter APS topology and further attempts to configure a local protect channel are rejected.

The interface type must be a SONET controller.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure SONET 0/2/0/2 as a local protect channel:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group (global), on page 722</code></td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td><code>channel remote, on page 731</code></td>
<td>Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.</td>
</tr>
<tr>
<td><code>show aps, on page 763</code></td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
channel remote

To assign a port and interface that is physically located in a remote router as a SONET working or protect automatic protection switching (APS) channel, use the `channel remote` command in APS group configuration mode. To return to the default setting, use the `no` form of this command.

```
channel {0 | 1} remote ip-address
```

**Syntax Description**

{0 | 1} Assigns a protect or working channel type. 0 is protect, 1 is working.

`ip-address` Remote router IP address in A.B.C.D format.

**Command Default**

A SONET APS remote channel is not assigned.

**Command Modes**

APS group configuration

**Command History**

`Release`   `Modification`

Release 3.9.0   This command was introduced.

**Usage Guidelines**

Use the `channel remote` command to assign working or protect channels that are physically located in a different router.

Use the `channel local` command to assign channels in the local router.

The IP address of the remote router is required only if a working channel configured as the protect router contacts all working routers.

Specifying a remote protect channel is optional. If you do not specify a remote protect channel, the default value of 0.0.0.0 is used. The protect router is always the one that contacts the working router. The working router replies to the protect router using the source address extracted from the incoming messages as the destination address. If an address other than 0.0.0.0 (the default value) is specified, the working router always uses that address when sending messages to the protect router.

**Task ID**

Task ID   Operations

sonet-sdh   read, write

**Examples**

In the following examples, a remote channel with IP address 192.168.1.1 is assigned as the working channel:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group (global), on page 722</code></td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td><code>channel local, on page 729</code></td>
<td>Assigns local SONET physical ports as SONET APS channels in the current APS group.</td>
</tr>
<tr>
<td><code>show aps, on page 763</code></td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
clear counters sonet

To clear SONET counters for a specific SONET controller, use the `clear counters sonet` command in EXEC mode.

**clear counters sonet interface-path-id**

**Syntax Description**

- `interface-path-id` Physical interface or virtual interface.

  **Note** Use the `show controllers sonet` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the `clear counters sonet` command to clear SONET counters for a specific SONET controller.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
<tr>
<td>basic-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the SONET counters being cleared on the SONET interface:
RP/0/RSP0/CPU0:router# clear counters sonet 0/1/0/0

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
<td></td>
</tr>
</tbody>
</table>
clock source (SONET)

To set the clock source of the sent signal on SONET ports, use the clock source command in SONET/SDH configuration mode. To cancel a clock source setting, use the no form of this command.

clock source {internal | line}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Specifies that the controller will clock its sent data from its internal clock.</td>
</tr>
<tr>
<td>line</td>
<td>Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. This is the default value.</td>
</tr>
</tbody>
</table>

Command Default

The clock source for the controller is line.

Command Modes

SONET/SDH configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the clock source command to configure which reference clock is used by the sender.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

In the following example, the SONET controller is configured to clock its sent data from its internal clock:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# clock source internal
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
controller (SONET)

To enter SONET/SDH configuration mode so that you can configure a specific SONET controller, use the `controller (SONET)` command in Global Configuration mode. To return to the default state, use the `no` form of this command.

```
controller [preconfigure] sonet interface-path-id
```

**Syntax Description**

- **preconfigure** (Optional) Specifies a SONET preconfiguration. Use the `preconfigure` keyword only when a modular services card is not physically installed in a slot.
- **sonet** Enters the SONET configuration mode or configures the SONET port controller specified by `interface-path-id`.
- **interface-path-id** Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the `path (SONET)` command to enter SONET/SDH path configuration mode to specify other SONET options for a SONET path.

**Task ID**

**Examples**

The following example shows how to enter SONET/SDH configuration mode for the SONET controller in slot number 2:
The following example shows how to configure the SONET controller path (0/2/0/1) to send a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded.

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/2/0/1
RP/0/RSP0/CPU0:router(config-sonet)#
```

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/2/0/1 path b3-ber-prdi
RP/0/RSP0/CPU0:router(config-sonet)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path (SONET), on page 754</td>
<td>Enters SONET/SDH path configuration mode.</td>
</tr>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
delay clear

To configure the amount of time before a Synchronous Transport Signal (STS) path delay trigger alarm is cleared, use the delay clear command in STS path configuration mode. To return the command to its default setting, use the no form of this command.

delay clear value

**Syntax Description**

- **value**: Value, in milliseconds, before an STS path delay trigger alarm is cleared. The range is from 0 to 180000. The default is 10 seconds.

**Command Default**

The default is 10 seconds.

**Command Modes**

STS path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **sonet-sdh**: read, write

**Examples**

The following example shows how to specify that STS path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/RSP0/CPU0:router(config-sonet)# sts 1
RP/0/RSP0/CPU0:router(config-stsPath)# delay clear 7000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay trigger, on page 739</td>
<td>Configures a time value for the STS path delay trigger.</td>
</tr>
</tbody>
</table>
delay trigger

To configure a time value for the Synchronous Transport Signal (STS) path delay trigger, use the `delay trigger` command in STS path configuration mode. To return the command to its default setting, use the `no` form of this command.

```
delay trigger value
```

**Syntax Description**

- `value`: Value, in milliseconds, for the STS path delay trigger. The range is from 0 through 60000. The default is 0 seconds, which means that there is no delay.

**Command Default**

- The default is 0 seconds, which means that there is no delay.

**Command Modes**

- STS path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the timer for the STS path delay trigger expires, an alarm is declared.

**Examples**

The following example shows how to set the STS path delay trigger to 6000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/RSP0/CPU0:router(config-sonet)# sts 1
RP/0/RSP0/CPU0:router(config-stsPath)# delay trigger 6000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay clear</code>, on page 738</td>
<td>Configures the amount of time before a STS path delay trigger alarm is cleared.</td>
</tr>
</tbody>
</table>
**down-when-looped**

To configure a SONET controller to inform the system that it is down when loopback is detected, use the **down-when-looped** command in SONET/SDH configuration mode.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The default is disabled.

**Command Modes**

SONET/SDH configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command does not have a **no** form.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a SONET controller to inform the system that the associated line is down if a loopback is detected:

```plaintext
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# down-when-looped
```

`down-when-looped` is a traffic-affecting operation

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback (SONET), on page 745</td>
<td>Configures the SONET controller for loopback mode.</td>
</tr>
</tbody>
</table>
framing (SONET)

To specify the framing used on the SONET controller, use the `framing` command in SONET/SDH configuration mode. To disable framing on the SONET controller, use the `no` form of this command.

```
framing  {sdh | sonet}
```

**Syntax Description**
- `sdh` Selects Synchronous Digital Hierarchy (SDH) framing. This framing mode is typically used in Europe.
- `sonet` Selects SONET framing. This is the default.

**Command Default**
The default framing on SONET controllers is `sonet`.

**Command Modes**
SONET/SDH configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The <code>sdh</code> keyword was supported.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `framing` command to select either SONET or SDH framing on the selected physical port, if supported. For physical ports that do not support either of these two options, the `framing` command is disabled.

Use the `no` form of this command to disable SONET or SDH framing on the SONET controller.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the SONET controller is configured for SDH framing:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# framing sdh
```

In the following example, the SONET controller is configured for SONET framing:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# framing sonet
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers sonet</code>, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
line delay clear

To configure the amount of time before a SONET/SDH line delay trigger alarm is cleared, use the `line delay clear` command in SONET controller configuration mode. To return the command to its default setting, use the `no` form of this command.

```
line delay clear value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Value, in milliseconds, before a SONET/SDH line delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is 10.

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the timer for the SONET/SDH line delay clear expires, an alarm is cleared.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify that SONET/SDH line delay trigger alarms should be cleared after 4000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/RSP0/CPU0:router(config-sonet)# line delay clear 4000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line delay trigger, on page 743</td>
<td>Configures a time value for the SONET/SDH line delay trigger.</td>
</tr>
</tbody>
</table>
line delay trigger

To configure a time value for the SONET/SDH line delay trigger, use the `line delay trigger` command in SONET controller configuration mode. To return the command to its default setting, use the `no` form of this command.

```
line delay trigger value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value: Value, in milliseconds, for the SONET/SDH line delay trigger. The range is 0 to 60000.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is 0, which means that there is no delay.

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the timer for the SONET/SDH line delay trigger expires, an alarm is raised.

**Task ID**

- sonet-sdh read,
- write

**Examples**

The following example shows how to set the SONET/SDH line delay trigger to 3000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/RSP0/CPU0:router(config-sonet)# line delay trigger 3000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line delay clear, on page 742</td>
<td>Configures the amount of time before a SONET/SDH line delay trigger alarm is cleared.</td>
</tr>
</tbody>
</table>
lockout

To override a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic, use the lockout command in APS group configuration mode. To remove the lockout, use the no form of this command.

lockout  [0]

**Syntax Description**

[0] (Optional) Specifies blocking of the protect channel from a manual or forced APS request. This is the default.

**Command Default**

The default is 0.

**Command Modes**

APS group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A lockout switch request can be used to override a force, an automatic (Signal Failed or Signal Degraded), or a manual switch request. No other request can override a lockout request; it has the highest possible priority.

In a multirouter APS topology, a lockout request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the no form of the command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to lock out or prevent the channel from switching to a protect router in the event that the working channel becomes unavailable:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# lockout 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aps group (global), on page 722</td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td>aps group, on page 719</td>
<td>Manually switches an APS channel.</td>
</tr>
</tbody>
</table>
loopback (SONET)

To configure the SONET controller for loopback mode, use the `loopback` command in SONET/SDH configuration mode. To remove the loopback SONET command from the configuration file, use the `no` form of this command.

```
loopback {internal | line}
```

**Syntax Description**

- **internal**: Specifies that all the packets be looped back from the source.
- **line**: Specifies that the incoming network packets be looped back to the SONET network.

**Command Default**

This command is disabled by default.

**Command Modes**

SONET/SDH configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The SONET and Synchronous Digital Hierarchy (SDH) transport layers support two loopback operation modes for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

**Examples**

In the following example, all packets are looped back to the SONET controller:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# loopback internal
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers sonet</code>, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
**mode (SONET)**

To set the mode of an STS path, AU path, T3 controller, or TUG3 controller, use the `mode` command in the applicable controller configuration mode. To disable the mode, use the `no` form of this command.

**STS Controller Configuration Mode**

```bash
mode {t3 | vt15-t1 | pos}
```

**AU Controller Configuration Mode**

```bash
mode {e3 | t3 | tug 3}
```

**T3 Controller Configuration Mode**

```bash
mode {e1 | serial | t1}
```

**TUG3 Controller Configuration Mode**

```bash
mode {c12 | c12-e1 | e3 | serial | t3}
```

**Syntax Description**

- `t3` Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying T3.
- `vt15-t1` Specifies the mode of the port to be channelized VT15-T1.
- `pos` Specifies the mode of the port to be channelized POS.
- `tug3` Specifies the mode of the port to be channelized TUG3.
- `e1` Specifies the mode of the port to be channelized E1.
- `serial` Specifies the mode of the port to be clear channel serial.
- `t1` Specifies the mode of the port to be channelized T1.
- `c12` Specifies the mode of the port to be channelized as a TUG3 path carrying TU-12.
- `c12-e1` Specifies the mode of the port to be channelized be TUG3 path carrying c12 to E1.
- `e3` Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying E3.

**Command Default**

No default behavior or values

**Command Modes**

- STS controller configuration
- AU controller configuration
- T3 controller configuration
- TUG3 controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The <code>pos</code>, <code>tug3</code>, <code>e1</code>, <code>c12</code>, <code>c12-e1</code>, and <code>e3</code> keywords were supported.</td>
</tr>
</tbody>
</table>
Usage Guidelines

For channelized SPAs, you must use the `mode` command before you can configure any channelized controllers.

Task ID  Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to set the mode of a T3 controller to channelized T1:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-t3)# mode t1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>width, on page 795</td>
<td>Sets the number of paths in a stream.</td>
</tr>
</tbody>
</table>
**overhead (SONET)**

To set the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendor, use the `overhead` command in SONET/SDH configuration mode. To remove the setting of the SONET overhead bytes from the configuration file and restore the default condition, use the `no` form of this command.

```
overhead {j0 | s1s0} byte-value
```

**Syntax Description**

- **j0**: Sets the J0/C1 byte value in the SONET section overhead. For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. Default is 0xcc.

- **s1s0**: Sets the SS bits value of the H1 byte in the SONET line overhead.

  Use the following values to tell the SONET transmission equipment the S1 and S0 bit:
  - For SONET mode, use 0 (this is the default).
  - For SDH mode, use 2.

  Range is from 0 to 3. Default is 0. Values 1 and 3 are undefined.

- **byte-value**: Byte value to which the `j1` or `s1s0` keyword should be set. Range is from 0 to 255.

**Command Default**

```
byte-value: 0x01 (j0)
byte-value: 0 (s1s0)
```

**Command Modes**

SONET/SDH configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `overhead` command to set the SONET overhead bytes in the frame header to a specific standards requirement.

Use the `no` form of this command to remove the setting of the SONET overhead bytes from the configuration file and restore the default condition.

For the `j0` keyword, the value that you use for the trace byte depends on the type of equipment being used. For the `s1s0` keyword, the value that you use depends on whether you are using the SONET or SDH mode. For SONET mode, use the value 0 (the default). For SDH mode, use the value 2.

**Task ID**

```
Task ID  Operations
sonet-sdh  read, write
```
The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 2 for SDH:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RSP0/CPU0:router(config-sonet)# overhead sls0 2
```

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 0 for SONET:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RSP0/CPU0:router(config-sonet)# overhead sls0 0
```
overhead (SONET path)

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the `overhead` command in SONET/SDH path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the `no` form of this command.

```
overhead {c2 byte-value | expected-trace LINE ascii-text | j1 ascii-value}
```

### Syntax Description

- **c2 byte-value**
  - Specifies Synchronous Transport Signal (STS) synchronous payload envelope (SPE) content (C2) byte. The transmitted c2 value is automatically set to 0xCF for unscrambled payload and 0x16 for scrambled payload. If c2 is configured to a user-specified value, the user-specified value is always applied regardless of scrambling.
  - Replace the `byte-value` argument with the byte value to which the `c2` keyword should be set. Range is from 0 to 255. Default value is 0.

- **j1 ascii-value**
  - Configures the SONET path trace (j1) buffer.
  - Replace the `ascii-value` argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 — POS) interface name, and IP address, if applicable.

- **expected-trace LINE ascii-text**
  - Configures the SONET/SDH path trace. The trace monitoring feature allows a node to perform trace monitoring by using the SONET/SDH capabilities.
  - Replace the `LINE` with the expected trace message
  - Replace the `ascii-text` argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 — POS) interface name, and IP address, if applicable.
  - the `LINE` is the expected trace message which should match else ptim mismatch would be reported

### Command Default

```
byte-value: 0xCF
byte-value: 0
```

### Command Modes

SONET/SDH path configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The SONET standards permit or require user access for configuration of some bytes or bits in the SONET path overhead. Use the `overhead` command to set the SONET path overhead bytes in the frame header to a specific standards requirement. Use the `no` form of this command to remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition.

Use the `c2` keyword to configure the desired C2 byte value in the SONET path overhead.
Use the \texttt{j1} keyword to configure a user-defined path trace message in the \texttt{j1} bytes of the SONET path overhead. For the \texttt{j1} keyword, use the default message or insert your own message that has a maximum of 62 characters. If no user-defined message is configured, a default message is automatically generated, containing the router name, the controller name, its IP address, and the values of the sent and received K1 and K2 bytes in the SONET line overhead.

**Examples**

The following example shows how to set the STS SPE C2 byte in the SONET path frame header:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>scrambling disable (SONET path), on page 762</td>
<td>Disables payload scrambling on a SONET path.</td>
</tr>
</tbody>
</table>
**path delay clear**

To configure the amount of time before a SONET/SDH path delay trigger alarm is cleared, use the `path delay clear` command in SONET controller configuration mode. To return the command to its default setting, use the `no` form of this command.

```
path delay clear value
```

**Syntax Description**

- `value` Value, in milliseconds, before a SONET/SDH path delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10 seconds.

**Command Default**

The default is 10 seconds.

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify that SONET/SDH path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/RSP0/CPU0:router(config-sonet)# path delay clear 7000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path delay trigger, on page 753</td>
<td>Configures a time value for the SONET/SDH path delay trigger.</td>
</tr>
</tbody>
</table>
path delay trigger

To configure a time value for the SONET/SDH path delay trigger, use the `path delay trigger` command in SONET controller configuration mode. To return the command to its default setting, use the `no` form of this command.

`path delay trigger value`

**Syntax Description**

`value`  Value, in milliseconds, for the SONET/SDH path delay trigger. The range is 0 to 60000.

**Command Default**

The default is 0, which means that there is no delay.

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the timer for the SONET/SDH path delay trigger expires, an alarm is declared.

**Task ID**

`sonet-sdh read, write`

**Examples**

The following example shows how to set the SONET/SDH path delay trigger to 6000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/RSP0/CPU0:router(config-sonet)# path delay trigger 6000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>path delay clear</code>, on page 752</td>
<td>Configures the amount of time before a SONET/SDH path delay trigger alarm is cleared.</td>
</tr>
</tbody>
</table>
path (SONET)

To enter SONET/SDH path configuration mode, use the `path` command in SONET controller configuration mode.

**path**

### Syntax Description
This command has no keywords or arguments.

### Command Default
No default behavior or values

### Command Modes
SONET controller configuration

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
No specific guidelines impact the use of this command.

### Task ID
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples
The following example shows how to access SONET path submode from SONET controller configuration mode:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# path
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ais-shut (SONET path), on page 718</code></td>
<td>Enables automatic insertion of PAIS in the sent SONET signal whenever the SONET path enters the administratively down state.</td>
</tr>
<tr>
<td><code>b3-ber-prdi, on page 728</code></td>
<td>Enables sending of a PRDI when the BER bit interleaved parity (BIP) B3 threshold is exceeded.</td>
</tr>
<tr>
<td><code>delay clear, on page 738</code></td>
<td>Configures the amount of time before a STS path delay trigger alarm is cleared.</td>
</tr>
<tr>
<td><code>delay trigger, on page 739</code></td>
<td>Configures a time value for the STS path delay trigger.</td>
</tr>
<tr>
<td><code>overhead (SONET path), on page 750</code></td>
<td>Sets the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor.</td>
</tr>
<tr>
<td><code>report (SONET path), on page 758</code></td>
<td>Configures whether or not selected SONET alarms are logged to the console for a SONET path controller.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>scrambling disable (SONET path), on page 762</td>
<td>Disables payload scrambling on a SONET path.</td>
</tr>
<tr>
<td>threshold (SONET path), on page 790</td>
<td>Sets the bit error rate (BER) threshold values of the specified alarms for a SONET path.</td>
</tr>
<tr>
<td>uneq-shut (SONET path), on page 792</td>
<td>Enables automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte.</td>
</tr>
</tbody>
</table>
To permit selected SONET alarms to be logged to the console for a SONET controller, use the `report` command in SONET/SDH configuration mode. To disable logging of select SONET alarms, use the `no` form of this command.

```
report  [{b1-tca | b2-tca | lais | lrdi | sd-ber | sf-ber | slof | slos}]
```

### Syntax Description

- **b1-tca** (Optional) Reports bit 1 (B1) bit error rate (BER) threshold crossing alert (TCA) errors.
- **b2-tca** (Optional) Reports bit 2 (B2) BER TCA errors.
- **lais** (Optional) Reports line alarm indication signal (LAIS) errors.
- **lrdi** (Optional) Reports line remote defect indication errors.
- **sd-ber** (Optional) Reports signal degradation BER errors.
- **sf-ber** (Optional) Reports signal failure BER errors.
- **slof** (Optional) Reports section loss of frame (SLOF) errors.
- **slos** (Optional) Reports section loss of signal (SLOS) errors.

### Command Default
Alarms from the following keywords are reported by default:

- b1-tca
- b2-tca
- sf-ber
- slof
- slos

### Command Modes
SONET/SDH configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can check the current state of masked alarm, a problem indication that is a candidate for an alarm, by displaying the “Masked Alarms” line in the `show controllers sonet` command output.

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.
Path AIS is sent by line terminating equipment to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path loss of pointer (LOP) is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

SLOF is detected when an error-framing defect on the incoming SONET signal persists for 3 microseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal is observed. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the controller, use the `show controllers sonet` command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable the reporting of line AIS alarms on the path controller:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RSP0/CPU0:router(config-sonet)# report lais
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers sonet</code>, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
report (SONET path)

To configure whether or not selected SONET alarms are logged to the console for a SONET path controller, use the `report` command in SONET/SDH path configuration mode. To disable or re-enable the logging of select SONET alarms, use the `no` form of this command.

```
report [ { b3-tca | pais | plop | pplm | prdi | ptim } ]
```

**Syntax Description**

- `b3-tca` (Optional) Reports bit 3 (B3) bit error rate (BER) threshold crossing alert (TCA) errors.
- `pais` (Optional) Reports path alarm indication signal (PAIS) errors.
- `plop` (Optional) Reports path loss of pointer (PLOP) errors.
- `pplm` (Optional) Reports path payload mismatch (PPLM) defect errors.
- `prdi` (Optional) Reports path remote defect indication (PRDI) errors.
- `ptim` (Optional) Reports path trace identity mismatch (PTIM) defect errors.

**Command Default**

Alarms from the following keywords are reported:

- `b3-tca`
- `plop`

**Command Modes**

SONET/SDH path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a masked alarm, a problem indication that is a candidate for an alarm, by inspecting the “Masked Alarms” line displayed in the `show controllers sonet` command output.

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

Path AIS is sent by line-terminating equipment to alert the downstream path-terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path LOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

To determine the alarms that are reported on the controller, use the `show controllers sonet` command.

All report commands accept the default option. The default reporting values are determined based upon the SONET standards specifications and are clearly identified in the corresponding command’s help string.
The reporting of B3 BER TCA errors and path LOP errors is enabled by default.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

In the following example, reporting of path PAIS alarms is enabled:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# report pais
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the revert command in APS configuration mode. To disable automatic switchover, use the no form of this command.

```
revert minutes
```

**Syntax Description**

- `minutes` Number of minutes until the circuit is switched back to the working interface after the working interface is available.

**Command Default**

- `minutes`: 0
  Automatic switchover is disabled.

**Command Modes**

- APS group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the revert command to enable and disable revertive APS operation mode, if needed. The revertive APS operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment. Use the no form of this command to disable automatic switchover.

The revertive APS operation mode is the recommended operation mode because it offers better traffic protection during various possible software failures and upgrade or downgrade scenarios.

The `minutes` argument indicates how many minutes will elapse until automatic protection switching (APS) decides to switch traffic back from protect to working after the condition that caused an automatic (Signal Failed or Signal Degrade) switch to protect disappears. A value of 0 (default) disables APS revertive mode.

In a multirouter APS topology, the revert command is allowed only on the protect router.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable APS to revert to the protect or working channel after 5 minutes have elapsed:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# revert 5
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group (global), on page 722</code></td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td><code>show aps, on page 763</code></td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
scrambling disable (SONET path)

To disable payload scrambling on a SONET path, use the `scrambling disable` command in SONET/SDH path configuration mode. To enable payload scrambling after it has been disabled, use the `no` form of this command.

```
scrambling disable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The default is enable (SONET payload scrambling is on).

**Command Modes**

SONET/SDH path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the synchronous payload envelope (SPE) of the controller to ensure sufficient bit transition density. Both ends of the connection must be configured using SONET path scrambling.

If the hardware payload scrambling support is not user-configurable, or is not supported, the `scrambling disable` command may be rejected.

**Examples**

In the following example, scrambling is disabled for the path:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# scrambling disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
show aps

To display the operational status for all configured SONET automatic protection switching (APS) groups, use the `show aps` command in EXEC mode.

**show aps**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show aps` command to display operational status for all configured SONET APS groups.

Displaying the SONET APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

**Examples**

The following is sample output from the `show aps` command:

```
RP/0/RSP0/CP00:router# show aps

APS Group 1:
Protect ch 0 (SONET3_0):Enabled
  SONET framing, SONET signalling, bidirectional, revertive (300 sec)
  Rx K1:0x21 (Reverse Request - Working)
    K2:0x15 (bridging Working, 1+1, bidirectional)
  Tx K1:0x81 (Manual Switch - Working)
    K2:0x15 (bridging Working, 1+1, bidirectional)
Working ch 1 (SONET2_0):Disabled
  Rx K1:0x00 (No Request - Null)
    K2:0x00 (bridging Null, 1+1, non-aps)
  Tx K1:0x00 (No Request - Null)
    K2:0x00 (bridging Null, 1+1, non-aps)

APS Group 3:
PGP:protocol version: native 2 adopted 2
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (SONET3_1):Disabled
  SONET framing, SONET signalling, bidirectional, non-revertive
  Rx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
  Tx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
Working ch 1 (192.168.1.1):Enabled

APS Group 49:
Protect ch 0 (SONET0_2_0_0):Disabled
  SONET framing, SONET signalling, unidirectional, non-revertive
```
Rx K1:0x00 (No Request - Null)
K2:0x00 (bridging Null, 1+1, non-aps)
Tx K1:0x00 (No Request - Null)
K2:0x04 (bridging Null, 1+1, unidirectional)

Working ch 1 (SONET0_2_0_1): Enabled
SONET framing, unidirectional
Rx K1:0x00 (No Request - Null)
K2:0x00 (bridging Null, 1+1, non-aps)
Tx K1:0x00 (No Request - Null)
K2:0x00 (bridging Null, 1+1, non-aps)

APS Group 6:
PGP: protocol version: native 2 adopted 2
PGP: Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (192.168.3.2 - auto): Disabled
Working ch 1 (SONET6_0): Enabled
Rx K1:0x00 (No Request - Null)
K2:0x00 (bridging Null, 1+1, non-aps)
Tx K1:0x00 (No Request - Null)
K2:0x00 (bridging Null, 1+1, non-aps)

Table 51: show aps Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APS Group</td>
<td>Assigned number of the APS group. Range is from 1 through 255.</td>
</tr>
<tr>
<td>Protect ch</td>
<td>Number and address of the protect channel interface.</td>
</tr>
<tr>
<td>Working ch</td>
<td>Number and address of the working channel interface.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aps agents, on page 765</td>
<td>Displays the status of the APS WP distributed communication subsystem.</td>
</tr>
<tr>
<td>show aps group, on page 767</td>
<td>Displays information about the APS groups.</td>
</tr>
</tbody>
</table>
show aps agents

To display the status of the automatic protection switching (APS) working to protect (WP) distributed communication subsystem, use the show aps agents command in EXEC mode.

**show aps agents**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the show aps agents command to display the status of the APS WP distributed communication subsystem.

The WP communication is critical for the APS functionality. The show aps agents command is typically used as a debugging aid for unexpected or unusual APS operation.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

**Examples**

The following is sample output from the show aps agents command:

```
RP/0/RSP0/CPU0:r1-gte1# show aps agents

SONET APS Manager working-Protect (WP) connections:
Remote peer (192.168.3.2 - auto) is up:
  Group 6 [P.Ch0] 192.168.3.2 === Manager === SONET6_0 (node6) === [W.Ch1]
Remote peer (10.1.1.1) is up:
  Group 3 [W.Ch1] 192.168.1.1 === Manager === SONET3_1 (node3) === [P.Ch0]
Local agent (node2) is up:
  Group 1 [W.Ch1] === SONET2_0 === SONET3_0 (node3) === [P.Ch0]
Local agent (node3) is up:
  Group 1 [P.Ch0] === SONET3_0 === SONET2_0 (node2) === [W.Ch1]
  Group 3 [P.Ch0] === SONET3_1 === Manager === 192.168.1.1 [W.Ch1]
  Group 5 [P.Ch0] === SONET3_2 === SONET3_3 (node3) === [W.Ch1]
  Group 5 [W.Ch1] === SONET3_3 === SONET3_2 (node3) === [P.Ch0]
Local agent (node6) is up:
  Group 6 [W.Ch1] === SONET6_0 === Manager === 192.168.3.2 [P.Ch0]
```
### Table 52: show aps agents Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote peer</td>
<td>IP address of the remote Protect Group Protocol (PGP) peer for the working router in an APS group. An IP address of 0.0.0.0 indicates a dynamically discovered PGP peer not yet contacted, shown on working routers only. (The protect router contacts the working router.)</td>
</tr>
<tr>
<td>Local agent</td>
<td>Node name of the local agent, such as (node2).</td>
</tr>
<tr>
<td>Group</td>
<td>The interface location or IP address of the SONET APS group.</td>
</tr>
<tr>
<td></td>
<td>Internal WP communication channel segments are represented as “---” if the segment is operational or “-/” if the connection is broken.</td>
</tr>
<tr>
<td></td>
<td>PGP segments are represented as “===” if operational or “==” if broken.</td>
</tr>
</tbody>
</table>

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aps, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
**show aps group**

To display information about the automatic protection switching (APS) groups, use the **show aps group** command in EXEC mode.

```
show aps group [number]
```

**Syntax Description**

- `number` (Optional) The assigned group number.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show aps group** command displays information about APS groups, and is useful if multiple APS groups are configured.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show aps group** command:

```
RP/0/RSP0/CP00:router# show aps group 3
APS Group 3:
    PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
    Protect ch 0 (SONET3_1):Admin Down, Disabled
    SONET framing, SONET signalling, bidirectional, non-revertive
    Rx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
    Tx K1:0x00 (No Request - Null)
    K2:0x05 (bridging Null, 1+1, bidirectional)
    Working ch 1 (192.168.1.1):Admin Down, Enabled
```
Table 53: show aps group Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APS Group</td>
<td>Group number assigned to the displayed APS group. For each channel in the group, the following information is displayed:</td>
</tr>
<tr>
<td></td>
<td>• Authentication string</td>
</tr>
<tr>
<td></td>
<td>• Hello timer value</td>
</tr>
<tr>
<td></td>
<td>• Hold timer value</td>
</tr>
<tr>
<td></td>
<td>• Role of the channel (working or protect)</td>
</tr>
<tr>
<td></td>
<td>• Channel number</td>
</tr>
<tr>
<td></td>
<td>• Name of the assigned physical port</td>
</tr>
<tr>
<td></td>
<td>• Channel status (Enabled, Disabled, Admin Down, Signal Fail, Signal Degraded, or Not Contacted)</td>
</tr>
<tr>
<td></td>
<td>• Group-related information (for protect channels only) that includes:</td>
</tr>
<tr>
<td></td>
<td>• Framing of the SONET port</td>
</tr>
<tr>
<td></td>
<td>• Kilobytes signaling protocol</td>
</tr>
<tr>
<td></td>
<td>• Unidirectional or bidirectional APS mode</td>
</tr>
<tr>
<td></td>
<td>• APS revert time, in seconds (in revertive operation mode only)</td>
</tr>
<tr>
<td>Rx</td>
<td>Received error signaling bytes and their APS decoded information.</td>
</tr>
<tr>
<td>Tx</td>
<td>Sent error signaling bytes and their APS decoded information.</td>
</tr>
<tr>
<td>Working ch</td>
<td>IP address of the corresponding Protect Group Protocol (PGP) peer.</td>
</tr>
</tbody>
</table>

The information displayed for the channels local to the routers is identical to the channel information displayed for single-router APS groups.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aps, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
<tr>
<td>show aps agents, on page 765</td>
<td>Displays the status of the APS WP distributed communication subsystem.</td>
</tr>
</tbody>
</table>
show controllers pos

To display information on the Packet-over-SONET/SDH (POS) controllers, use the **show controllers pos** command in EXEC mode.

```plaintext
show controllers pos interface-path-id [ {all | framer {internal | register | statistics} | internal} ] [ {begin line | exclude line | file filename | include line} ]
```

### Syntax Description

- **interface-path-id**: Physical interface or virtual interface.
  - **Note**: Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

- **all**: (Optional) Displays information for all POS interface controllers.
- **framer**: (Optional) Displays all POS framer information.
- **internal**: (Optional) Displays all POS internal information.
- **register**: (Optional) Displays the POS framer registers.
- **statistics**: (Optional) Displays the POS framer cumulative counters.
- **begin line**: (Optional) Displays information beginning with the line that includes the regular expression given by the `line` argument.
- **exclude line**: (Optional) Displays information excluding all lines that contain regular expressions that match the `line` argument.
- **file filename**: (Optional) Saves the configuration to the designated file. For more information on which standard filenames are recognized, use the question mark (?) online help function.
- **include line**: (Optional) Displays only those lines that contain the regular expression given by the `line` argument.

### Command Default

No default behavior or values

### Command Modes

EXEC mode

### Command History

- **Release 4.0.0** This command was introduced.

### Usage Guidelines

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
• **rack**: Chassis number of the rack.

• **slot**: Physical slot number of the line card.

• **module**: Module number. A physical layer interface module (PLIM) is always 0.

• **port**: Physical port number of the interface.

• If specifying a virtual interface, the number range varies, depending on interface type.

The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

### Examples

The following is sample output from the `show controllers pos` command:

```
RP/0/RSP0/CPU0:router# show controllers POS 0/3/0/2

Port Number : 2
Interface : POS0/3/0/2
Ifhandle : 0x1380120
CRC : 32
MTU : 4474
Port Bandwidth Kbps : 2488320
Admin state : Up
Driver Link state : Up

Bundle member : No
Bundle MTU : 4474
Bundle Adminstate : Up
```

The following is sample output from the `show controllers pos all` command:

```
RP/0/RSP0/CPU0:router# show controllers POS 0/3/0/2 all

Port Number : 2
Interface : POS0/3/0/2
Ifhandle : 0x1380120
CRC : 32
MTU : 4474
Port Bandwidth Kbps : 2488320
Admin state : Up
Driver Link state : Up

Bundle member : No
Bundle MTU : 4474
Bundle Adminstate : Up

POS Driver Internal Cooked Stats Values for port 2
--------------------------------------------------
Rx Statistics | Tx Statistics
```
### Sky4402 ASIC #2 Registers:

<table>
<thead>
<tr>
<th>Register</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000 general_cntrl</td>
<td>0x00</td>
</tr>
<tr>
<td>0x002 sys_intf_cntrl_1</td>
<td>0x06</td>
</tr>
<tr>
<td>0x003 sys_intf_cntrl_2</td>
<td>0x00</td>
</tr>
<tr>
<td>0x004 JTAG3</td>
<td>0x10</td>
</tr>
<tr>
<td>0x005 JTAG2</td>
<td>0x10</td>
</tr>
<tr>
<td>0x006 JTAG1</td>
<td>0x10</td>
</tr>
<tr>
<td>0x007 JTAG0</td>
<td>0x2f</td>
</tr>
<tr>
<td>0x010 active_led</td>
<td>0x01</td>
</tr>
<tr>
<td>0x011 gpio_port_mode</td>
<td>0x01</td>
</tr>
<tr>
<td>0x012 gpio_port_fault</td>
<td>0x00</td>
</tr>
<tr>
<td>0x013 gpio_port_data</td>
<td>0x58</td>
</tr>
<tr>
<td>0x015 gpio_port_ctrl</td>
<td>0x3f</td>
</tr>
<tr>
<td>0x017 gpio_port_transition</td>
<td>0x00</td>
</tr>
<tr>
<td>0x019 gpio_port_intr_mask</td>
<td>0xff</td>
</tr>
<tr>
<td>0x01b gpio_port_intr</td>
<td>0x3f</td>
</tr>
<tr>
<td>0x01c master_intr_status</td>
<td>0x00</td>
</tr>
<tr>
<td>0x01d master_mask</td>
<td>0x00</td>
</tr>
<tr>
<td>0x020 interrupt_4</td>
<td>0x04</td>
</tr>
<tr>
<td>0x021 interrupt_3</td>
<td>0x00</td>
</tr>
<tr>
<td>0x022 interrupt_2</td>
<td>0x00</td>
</tr>
<tr>
<td>0x023 interrupt_1</td>
<td>0x00</td>
</tr>
<tr>
<td>0x024 status_4</td>
<td>0x04</td>
</tr>
<tr>
<td>0x025 status_3</td>
<td>0x00</td>
</tr>
<tr>
<td>0x026 status_2</td>
<td>0x0c</td>
</tr>
<tr>
<td>0x027 status_1</td>
<td>0x80</td>
</tr>
<tr>
<td>0x028 mask_4</td>
<td>0x07</td>
</tr>
<tr>
<td>0x029 mask_3</td>
<td>0x03</td>
</tr>
<tr>
<td>0x02a mask_2</td>
<td>0x1c</td>
</tr>
<tr>
<td>0x02b mask_1</td>
<td>0x8f</td>
</tr>
<tr>
<td>0x02d link_state_ctrl</td>
<td>0x80</td>
</tr>
<tr>
<td>0x041 diag</td>
<td>0x00</td>
</tr>
<tr>
<td>0x042 stkks</td>
<td>0x03</td>
</tr>
<tr>
<td>0x043 short_frame_ctrl</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c0 ror_ram_c2</td>
<td>0x16</td>
</tr>
<tr>
<td>0x0c1 ror_ram_g1</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c2 ror_ram_f2</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c3 ror_ram_h4</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c4 ror_ram_z3</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c5 ror_ram_z4</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c6 ror_ram_z5</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0c7 ror_ram_db_c2</td>
<td>0x16</td>
</tr>
<tr>
<td>0x0c8 ror_ram_db_g1</td>
<td>0x00</td>
</tr>
<tr>
<td>0x142 tor_ram_c2</td>
<td>0x16</td>
</tr>
<tr>
<td>0x143 tor_ram_g1</td>
<td>0x00</td>
</tr>
<tr>
<td>0x144 tor_ram_f2</td>
<td>0x00</td>
</tr>
<tr>
<td>0x145 tor_ram_h4</td>
<td>0x00</td>
</tr>
<tr>
<td>0x146 tor_ram_z3</td>
<td>0x00</td>
</tr>
<tr>
<td>0x147 tor_ram_z4</td>
<td>0x00</td>
</tr>
<tr>
<td>Address</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>0x148</td>
<td>tor_ram_z5</td>
</tr>
<tr>
<td>0x170</td>
<td>tor_ram_s1</td>
</tr>
<tr>
<td>0x171</td>
<td>tor_ram_e2</td>
</tr>
<tr>
<td>0x172</td>
<td>tor_ram_e1</td>
</tr>
<tr>
<td>0x173</td>
<td>tor_ram_f1</td>
</tr>
<tr>
<td>0x174</td>
<td>tor_ram_k1</td>
</tr>
<tr>
<td>0x175</td>
<td>tor_ram_k2</td>
</tr>
<tr>
<td>0x177</td>
<td>tor_ram_z2</td>
</tr>
<tr>
<td>0x180</td>
<td>rsp_cntrl_1</td>
</tr>
<tr>
<td>0x181</td>
<td>rsp_cntrl_2</td>
</tr>
<tr>
<td>0x184</td>
<td>rtop_f1_ovrhd</td>
</tr>
<tr>
<td>0x185</td>
<td>rtop_k1_ovrhd</td>
</tr>
<tr>
<td>0x186</td>
<td>rtop_k2_ovrhd</td>
</tr>
<tr>
<td>0x187</td>
<td>rtop_s1_ovrhd</td>
</tr>
<tr>
<td>0x188</td>
<td>rtop_e1_ovrhd</td>
</tr>
<tr>
<td>0x189</td>
<td>rtop_e2_ovrhd</td>
</tr>
<tr>
<td>0x18a</td>
<td>rtop_deb_si_ovrhd</td>
</tr>
<tr>
<td>0x18c</td>
<td>rtop_b1_mismatch_cnt_u</td>
</tr>
<tr>
<td>0x18d</td>
<td>rtop_b1_mismatch_cnt_l</td>
</tr>
<tr>
<td>0x190</td>
<td>rtop_b2_mismatch_cnt_u</td>
</tr>
<tr>
<td>0x191</td>
<td>rtop_b2_mismatch_cnt_l</td>
</tr>
<tr>
<td>0x194</td>
<td>rtop_rei_l_cnt_u</td>
</tr>
<tr>
<td>0x195</td>
<td>rtop_rei_l_cnt_l</td>
</tr>
<tr>
<td>0x198</td>
<td>rtop_ber_thresh_u</td>
</tr>
<tr>
<td>0x199</td>
<td>rtop_ber_thresh_l</td>
</tr>
<tr>
<td>0x19a</td>
<td>rtop_ber_leak_u</td>
</tr>
<tr>
<td>0x19b</td>
<td>rtop_ber_leak_l</td>
</tr>
<tr>
<td>0x19c</td>
<td>rtop_ber_delay_u</td>
</tr>
<tr>
<td>0x19d</td>
<td>rtop_ber_delay_l</td>
</tr>
<tr>
<td>0x1c0</td>
<td>rpop_signal_lbl_c2</td>
</tr>
<tr>
<td>0x1c2</td>
<td>rpop_valid_ptr_u</td>
</tr>
<tr>
<td>0x1c3</td>
<td>rpop_valid_ptr_l</td>
</tr>
<tr>
<td>0x1c4</td>
<td>rpop_b3_mismatch_cnt_u</td>
</tr>
<tr>
<td>0x1c5</td>
<td>rpop_b3_mismatch_cnt_l</td>
</tr>
<tr>
<td>0x1c8</td>
<td>rpop_rei_p_cnt_u</td>
</tr>
<tr>
<td>0x1c9</td>
<td>rpop_rei_p_cnt_l</td>
</tr>
<tr>
<td>0x1cc</td>
<td>rpop_ber_thresh_u</td>
</tr>
<tr>
<td>0x1cd</td>
<td>rpop_ber_thresh_l</td>
</tr>
<tr>
<td>0x1ce</td>
<td>rpop_ber_leak_u</td>
</tr>
<tr>
<td>0x1cf</td>
<td>rpop_ber_leak_l</td>
</tr>
<tr>
<td>0x1d0</td>
<td>rpop_ber_delay_u</td>
</tr>
<tr>
<td>0x1d1</td>
<td>rpop_ber_delay_l</td>
</tr>
<tr>
<td>0x200</td>
<td>rpp_cntrl_1</td>
</tr>
<tr>
<td>0x201</td>
<td>rpp_cntrl_2</td>
</tr>
<tr>
<td>0x202</td>
<td>rpp_cntrl_3</td>
</tr>
<tr>
<td>0x203</td>
<td>rpp_cntrl_4</td>
</tr>
<tr>
<td>0x204</td>
<td>rpp_cntrl_5</td>
</tr>
<tr>
<td>0x208</td>
<td>rpp_max_pkt_len_u</td>
</tr>
<tr>
<td>0x209</td>
<td>rpp_max_pkt_len_l</td>
</tr>
<tr>
<td>0x20a</td>
<td>rpp_min_pkt_len</td>
</tr>
<tr>
<td>0x244</td>
<td>tpp_inter_pkt_u</td>
</tr>
<tr>
<td>0x245</td>
<td>tpp_inter_pkt_l</td>
</tr>
<tr>
<td>0x246</td>
<td>tpp_idle_cell_hdr</td>
</tr>
<tr>
<td>0x247</td>
<td>tpp_idle_cell_filldata</td>
</tr>
<tr>
<td>0x248</td>
<td>tpp_cntrl</td>
</tr>
<tr>
<td>0x280</td>
<td>tpop_cntrl</td>
</tr>
<tr>
<td>0x2c0</td>
<td>ttog_cntrl</td>
</tr>
<tr>
<td>0x2c2</td>
<td>ttog_ovrhd_src_1</td>
</tr>
<tr>
<td>0x2c3</td>
<td>ttog_ovrhd_src_2</td>
</tr>
<tr>
<td>0x2c9</td>
<td>ttog_ovrhd_fill</td>
</tr>
</tbody>
</table>
### Table 54: `show controllers pos` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco POS ASIC Register Dump (Receive)</td>
<td>Header for display of the contents of the receive ASIC1 register log.</td>
</tr>
<tr>
<td>ASIC mode</td>
<td>Address in hex of the ASIC mode flag.</td>
</tr>
<tr>
<td>Error source</td>
<td>Address in hex of the error source flag.</td>
</tr>
<tr>
<td>Error mask</td>
<td>Address in hex of the error mask flag.</td>
</tr>
<tr>
<td>Error detail 1</td>
<td>Address in hex of the error detail 1 flag.</td>
</tr>
<tr>
<td>Error detail 2</td>
<td>Address in hex of the error detail 2 flag.</td>
</tr>
<tr>
<td>RX offset</td>
<td>Address in hex of the receive offset.</td>
</tr>
<tr>
<td>Channel Modes</td>
<td>Location in hex of the channel mode flag.</td>
</tr>
<tr>
<td>Port 0:</td>
<td>Port 0 (the first port) statistics display.</td>
</tr>
<tr>
<td>Port 1:</td>
<td>Port 1 (the second port) statistics display.</td>
</tr>
<tr>
<td>Port 2:</td>
<td>Port 2 (the third port) statistics display.</td>
</tr>
<tr>
<td>Port 3:</td>
<td>Port 3 (the fourth port) statistics display.</td>
</tr>
<tr>
<td>Runt Threshold</td>
<td>Limit in packets set for runts on the specified port.</td>
</tr>
<tr>
<td>Tx Delay</td>
<td>Transmit delay that has been set for the specified port.</td>
</tr>
<tr>
<td>Cisco POS ASIC Register Dump (Transmit)</td>
<td>Header for display of the contents of the transmit ASIC register log.</td>
</tr>
<tr>
<td>POS Driver Internal Cooked Stats Values for port 0</td>
<td>Statistics relating to the specified POS port (POS port 0).</td>
</tr>
<tr>
<td>Rx Statistics</td>
<td>Receive statistics for the indicated POS port.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, received by the system.</td>
</tr>
<tr>
<td>Good Bytes</td>
<td>Number of bytes received without errors.</td>
</tr>
<tr>
<td>Good Packets</td>
<td>Number of packets received without errors.</td>
</tr>
<tr>
<td>Aborts</td>
<td>Number of receive bytes that have been aborted</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>Number of FCS2 errors that have been received.</td>
</tr>
<tr>
<td>Runts</td>
<td>Number of received packets that are discarded because they are smaller than the minimum packet size of the medium.</td>
</tr>
<tr>
<td>FIFO Overflows</td>
<td>Number of received packets that exceeded the FIFO stack limit.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Giants</td>
<td>Number of received packets that are discarded because they exceed the maximum packet size of the medium.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of received packets that have been dropped from the system.</td>
</tr>
<tr>
<td>Tx Statistics</td>
<td>Transmit statistics for the indicated POS port.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total number of bytes, including data and MAC encapsulation, sent by the system.</td>
</tr>
<tr>
<td>Good Bytes</td>
<td>Number of bytes sent without errors.</td>
</tr>
<tr>
<td>Good Packets</td>
<td>Number of packets sent without errors.</td>
</tr>
<tr>
<td>Aborts</td>
<td>Number of sent bytes that have been aborted.</td>
</tr>
<tr>
<td>Min-len errors</td>
<td>Minimum queue length violations.</td>
</tr>
<tr>
<td>Max-len errors</td>
<td>Maximum queue length violations.</td>
</tr>
<tr>
<td>FIFO Underruns</td>
<td>First-in, first-out, a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. FIFO underruns reports the number of times that the transmitter has been running faster than the router can handle.</td>
</tr>
</tbody>
</table>

1. application-specific integrated circuit
2. frame check sequence
**show controllers sonet**

To display information about the operational status of SONET layers, use the `show controllers sonet` command in EXEC mode.

```
show controllers sonet  interface-path-id  {all | framers | internal-state}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td>For more information about the syntax for the router, use the question mark (?) online help function.</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>Displays all information.</td>
</tr>
<tr>
<td>framers</td>
<td>Displays framer information.</td>
</tr>
<tr>
<td>internal-state</td>
<td>Displays internal SONET state.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number. A physical layer interface module (PLIM) is always 0.
  - **port**: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the `show controllers sonet` command to display information about the operational status of SONET layers on a particular SONET port.

If the manageability PIE is not installed, you can use the `show controllers sonet` command to display the counters for the current 15 minutes only without history data. However, the SONET MIB is still available but is limited to the current bucket of data. History data is still available only when the manageability PIE is
The `show controllers sonet` command is available at any time to display current data, and history data is stored in the line card rather in the history bucket.

### Examples

The following is sample output from the `show controllers sonet` command:

```
RP/0/RSP0/CPU0:router# show controllers sonet 0/1/2/1
Port SONET0/1/2/1:
Status: Up
Loopback: None

SECTION
  LOF = 0  LOS = 0  BIP(B1) = 0
LINE
  AIS = 0  RDI = 1  FEBE = 0  BIP(B2) = 0
PATH
  AIS = 0  RDI = 0  FEBE = 0  BIP(B3) = 0
  LOF = 0  NEWPTR = 0  PSE = 0  NSE = 0
  PLM = 0  TIM = 0

Line delays trigger: 0 ms clear: 10000 ms
Path delays trigger: 0 ms clear: 10000 ms
Last clearing of "show controllers SONET" counters never

Detected Alarms: None
Asserted Alarms: None
Mask for Detected->Asserted: None
Detected Alerts: None
Reported Alerts: None
Mask for Detected->Reported: None
Alarm reporting enabled for: SLOS SLOF SF_BER PLOP
Alert reporting enabled for: B1-TCA B2-TCA B3-TCA

Framing: SONET
SPE Scrambling: Enabled
C2 State: Stable  C2_rx = 0x16 (22)  C2_tx = 0x16 (22) / Scrambling Derived
S1S0(tx): 0x0  S1S0(rx): 0x0 / Framing Derived

PATH TRACE BUFFER : STABLE
  Remote hostname : P1_CRS-8
  Remote interface: POS0/1/4/0
  Remote IP addr : 0.0.0.0

APS
No APS Group Configured
Protect Channel 0 DISABLED
  Rx(K1/K2): 0x00/0x00
  Tx(K1/K2): 0x00/0x00
Remote Rx(K1/K2): 01/0  Remote Tx(K1/K2): 01/0

BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
```
Optics type: OC48 SR/STM16 I-16
Clock source: internal (actual) internal (configured)
Rx S1: 0xf  Tx S1: 0x50

Optical Power Monitoring (accuracy: +/- 1dB)
Rx power = 0.3162 mW, -5.0 dBm
Tx power = 0.2883 mW, -5.4 dBm
Tx laser current bias = 17.2 mA

Table 55: show controllers sonet Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Slot number of the POS interface.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays whether the link associated with the specified port is up or down.</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback identifier, if applicable.</td>
</tr>
<tr>
<td>LOF</td>
<td>Section loss of frame is detected when a severely error-framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.</td>
</tr>
<tr>
<td>LOS</td>
<td>Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19(+/-3) microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.</td>
</tr>
<tr>
<td>BIP</td>
<td>Bit interleaved parity error reported.</td>
</tr>
<tr>
<td></td>
<td>• For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.</td>
</tr>
<tr>
<td></td>
<td>• For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.</td>
</tr>
<tr>
<td></td>
<td>• For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.</td>
</tr>
<tr>
<td>AIS</td>
<td>Alarm indication signal.</td>
</tr>
<tr>
<td></td>
<td>• Line alarm indication signal is sent by the STE1 to alert the downstream LTE2 that a LOS or LOF defect has been detected on the incoming SONET section.</td>
</tr>
<tr>
<td></td>
<td>• Path alarm indication signal is sent by the LTE to alert the downstream PTE3 that it has detected a defect on its incoming line signal.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RDI</td>
<td>Remote defect indication.</td>
</tr>
<tr>
<td></td>
<td>• Line remote defect indication is reported by the downstream LTE when it detects LOF4, LOS5, or AIS6.</td>
</tr>
<tr>
<td></td>
<td>• Path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.</td>
</tr>
<tr>
<td>FEBE</td>
<td>Far-end block errors.</td>
</tr>
<tr>
<td></td>
<td>• Line far-end block error (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP7 (B2) errors.</td>
</tr>
<tr>
<td></td>
<td>• Path far-end block error (accumulated from the G1 byte) is reported when the downstream PTE detects BIP (B3) errors.</td>
</tr>
<tr>
<td>LOP</td>
<td>Path loss of pointer is reported as a result of an invalid pointer (H1, H2) or an excess number of NDF8 enabled indications.</td>
</tr>
<tr>
<td>NEWPTR</td>
<td>Inexact count of the number of times the SONET framer has validated a new SONET pointer value (H1, H2).</td>
</tr>
<tr>
<td>PSE</td>
<td>Inexact count of the number of times the SONET framer has detected a positive stuff event in the received pointer (H1, H2).</td>
</tr>
<tr>
<td>NSE</td>
<td>Inexact count of the number of times the SONET framer has detected a negative stuff event in the received pointer (H1, H2).</td>
</tr>
<tr>
<td>PLM</td>
<td>Payload label mismatch. A different payload-specific functionality than the provisioned functionality is reported. For example, 02 to E0, or FD to FE.</td>
</tr>
<tr>
<td>TIM</td>
<td>Trace identifier mismatch. Reported TIM defects that occur primarily as a result of provisioning errors; for example, incorrect cross-connections in the network.</td>
</tr>
<tr>
<td>Line delays trigger</td>
<td>Line triggers delayed and cleared, in milliseconds.</td>
</tr>
<tr>
<td>Path delays trigger</td>
<td>Path triggers delayed and cleared, in milliseconds.</td>
</tr>
<tr>
<td>Last clearing of “show controllers SONET” counters</td>
<td>When the counters associated with the <code>show controllers sonet</code> command were last cleared.</td>
</tr>
<tr>
<td>Detected/Asserted Alarms</td>
<td>Any alarms detected by the controller are displayed here. Alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mask for Detected -&gt; Asserted</td>
<td>Masked alarms for the asserted alarm. For example, when SLOS is asserted, all low-level alarms are masked and are listed in this section of the output.</td>
</tr>
<tr>
<td>Detected Alerts</td>
<td>List of alerts that are detected.</td>
</tr>
<tr>
<td>Reported Alerts</td>
<td>List of reported alerts, such as B1-TCA B2-TCA B3-TCA, sent to the application layer.</td>
</tr>
<tr>
<td>Mask for Detected -&gt; Reported</td>
<td>List of masked alerts for asserted alarms that are reported.</td>
</tr>
<tr>
<td>Alarm reporting enabled for</td>
<td>Types of alarms that generate an alarm message.</td>
</tr>
<tr>
<td>Alert reporting enabled for</td>
<td>Types of alarms that generate an alert message.</td>
</tr>
<tr>
<td>Framing</td>
<td>Type of framing enabled on the controller.</td>
</tr>
<tr>
<td>SPE Scrambling</td>
<td>Status of synchronous payload envelope (SPE) scrambling: Enabled, Disabled.</td>
</tr>
<tr>
<td>C2 State</td>
<td>Value extracted from the SONET path signal label byte (C2).</td>
</tr>
<tr>
<td>S1S0(tx)</td>
<td>Two S bits received in the last H1 byte.</td>
</tr>
<tr>
<td>PATH TRACE BUFFER</td>
<td>SONET path trace buffer is used to communicate information regarding the remote hostname, interface name/number, and IP address. This use of the J1 (path trace) byte is proprietary to Cisco.</td>
</tr>
<tr>
<td>Remote hostname</td>
<td>Name of the remote host.</td>
</tr>
<tr>
<td>Remote interface</td>
<td>Interface of the remote host.</td>
</tr>
<tr>
<td>Remote IP addr</td>
<td>IP address of the remote host.</td>
</tr>
<tr>
<td>APS</td>
<td>Configuration status of the APS feature</td>
</tr>
<tr>
<td>APS Group</td>
<td>Indicates whether or not an APS group is configured.</td>
</tr>
<tr>
<td>Protect Channel 0</td>
<td>Indicates whether or not channel 0 is protected.</td>
</tr>
<tr>
<td>Rx(K1/K2)/Tx(K1/K2)</td>
<td>Contents of the received and transmitted K1 and K2 bytes at the local end in an APS configuration.</td>
</tr>
<tr>
<td>Remote Rx(K1/K2)/Tx(K1/K2)</td>
<td>Contents of the received and transmitted K1 and K2 bytes at the remote end in an APS configuration.</td>
</tr>
<tr>
<td>BER thresholds</td>
<td>List of the bit error rate (BER) thresholds you configured with the <code>threshold</code> (SONET) command.</td>
</tr>
<tr>
<td>TCA thresholds</td>
<td>List of threshold crossing alarms (TCA) you configured with the <code>threshold</code> (SONET) command.</td>
</tr>
<tr>
<td>Optics type</td>
<td>Type of small form-factor pluggable (SFP) used in the associated port.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Tx laser current bias** | Measured laser bias current, in milliamps (mA). The valid range is 0 through 131 mA.
**Clock source** | Actual and configured clock source.
**Optical Power Monitoring** | Power status of the SONET controller.
**Tx laser current bias** | Current information, in milliamps (mA), in the transmit direction.

The following is sample output from the `show controllers sonet` command with the `framers` option:

```
RP/0/RSP0/CPU0:router# show controllers sonet 0/1/2/1 framers

Common Regs
reg[0]  Master Reset and Identity 0x01
reg[1]  Master Cfg 0000
reg[3]  Master Clock Monitors 0x37
reg[100] Master Intr Status 1 0000
reg[101] Master Intr Status Ch 0-7 0000
reg[102] Master Intr Status Ch 8-15 0000
reg[1000] Master Clock Source Cfg 0000
reg[1001] Master DCC Interface Cfg 1 0x0f
reg[1002] Master DCC Interface Cfg 2 0000
reg[1004] APS Cfg and Status 0000
reg[1005] APS FIFO Cfg and Status 0x0f
reg[1006] APS Intr Status 1 0000
reg[1007] APS Intr Status 2 0000
reg[1008] APS Reset Ctrl 0000
reg[1010] TUL3 Interface Cfg 0x80
reg[1011] TUL3 Intr Status/Enable 1 0000
reg[1012] TUL3 Intr Status/Enable 2 0000
reg[1013] TUL3 ATM Level 3 FIFO Cfg 0x03
reg[1014] TUL3 ATM Level 3 Signal Label 0x01
reg[1015] TUL3 POS Level 3 FIFO Low Water Mark 0x15
reg[1016] TUL3 POS Level 3 FIFO High Water Mark 0x17
reg[1017] TUL3 POS Level 3 Signal Label 0000
reg[1018] TUL3 burst 0x0f
```

--More--

The following is sample output from the `show controllers sonet` command with the `internal-state` keyword:

```
RP/0/RSP0/CPU0:router# show controllers sonet 0/1/2/1 internal-state

Interface(layer)   admin_up if_state
```

---

1. section terminating equipment
2. line terminating equipment
3. path terminating equipment
4. loss of frame
5. loss of synchronization
6. alarm indication signal
7. bit interleaved parity
8. new data flag
Table 56: show controllers sonet Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface (layer)</td>
<td>Slot number of the POS interface.</td>
</tr>
<tr>
<td>admin_up</td>
<td>Whether the interface and its associated layers are in the admin-up state.</td>
</tr>
<tr>
<td>if_state</td>
<td>Whether the interface and its associated layers are in the up or down state.</td>
</tr>
</tbody>
</table>
show sonet-local trace frr

To display the alarms associated with Fast Re-Route (FRR) for all nodes or for a specific node, use the `show sonet-local trace frr` command in EXEC mode.

```
show sonet-local trace frr location node-id
```

**Syntax Description**

- `location node-id`: Full path location of the node. For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

Displays the FRR alarms for all nodes on the router.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to display the FRR alarms for a specific node:

```
RP/0/RSP0/CPU0:router# show sonet-local trace frr location 0/1/0/0
```

The following example shows how to display the FRR alarms for all nodes on the router:

```
RP/0/RSP0/CPU0:router# show sonet-local trace frr
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers sonet, on page 775</code></td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
shutdown (SONET)

To disable SONET controller processing, use the `shutdown` command in SONET/SDH configuration mode. To bring back up a SONET controller and enable SONET controller processing, use the `no form of this` command.

```
shutdown
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The SONET controller is up, and SONET controller processing is enabled.

**Command Modes**

SONET/SDH configuration

**Command History**

```
Release Modification
---                  -------
Release 3.9.0       This command was introduced.
```

**Usage Guidelines**

Use the `shutdown` command to shut down a SONET controller and disable SONET controller processing. Use the `no shutdown` command to bring back up a SONET controller and enable SONET controller processing.

The SONET controller must be brought up for the proper operation of the Layer 2 interface. The Layer 2 interface has a separate `shutdown` command available, which does not operate on the SONET controller’s administrative state.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows how to bring down the SONET controller and disable SONET controller processing:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/2
RP/0/RSP0/CPU0:router(config-sonet)# shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
signalling

To configure the K1K2 overhead byte signaling protocol used for automatic protection switching (APS), use the signalling command in APS group configuration mode. To reset APS signaling to the default, use the no form of this command.

```
signalling {sonet | sdh}
```

**Syntax Description**

- **sonet**: Sets signaling to SONET.
- **sdh**: Sets signaling to Synchronous Digital Hierarchy (SDH).

**Command Default**

SONET signaling is set by default.

**Command Modes**

APS group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>The sdh keyword was supported.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, APS uses the signaling mode matching the framing mode. The signalling command may be required, depending upon the transport equipment capabilities, only on “transition” links interconnecting SONET and SDH networks.

In a multi-router APS topology, the signalling command is allowed only on the protect router.

**Examples**

The following example shows how to reset the signaling protocol from the default SONET value to SDH:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# signalling sdh
```

The following example sets the signaling to SONET:

```
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# signalling sonet
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aps group (global), on page 722</td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td>show aps group, on page 767</td>
<td>Displays information about the APS groups.</td>
</tr>
</tbody>
</table>
sts

To specify the Synchronous Transport Signal (STS) path and enter the STS controller configuration mode, use the `sts` command in SONET controller configuration mode.

`sts number`

**Syntax Description**

*number* STS path number. The range varies by the type of line card.

**Command Default**

No default behavior or values

**Command Modes**

SONET controller configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify STS 1:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# sts 1
RP/0/RSP0/CPU0:router(config-stsPath)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>au, on page 724</code></td>
<td>Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.</td>
</tr>
</tbody>
</table>
timers (APS)

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the timers command in APS group configuration mode. To return to the default timers, use the no form of this command.

```
timers hello-seconds hold-seconds
```

**Syntax Description**
- `hello-seconds`: Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
- `hold-seconds`: Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Range is from 1 through 255 seconds. Default is 3 seconds.

**Command Default**
- `hello-seconds`: 1
- `hold-seconds`: 3

**Command Modes**
APS group configuration

**Command History**
```
ReleaseModification
--------------------------
3.9.0 This command was introduced.
```

**Usage Guidelines**
Use the timers command to change the time between hello packets and the time before the protect interface process declares a working interface router to be down.

The hello time, in seconds, represents the interval between the periodic message exchange between the Protect Group Protocol (PGP) peers. The hold time, in seconds, represents the maximum interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead. If the Hello timer is X seconds and Hold Timer is configured as Y seconds (where, X < Y), then the PGP link down announcement happens in a minimum of Y-X seconds and maximum of Y seconds.

If many multirouter APS groups are configured and the CPU load or the User Datagram Protocol (UDP) traffic associated with the PGP communication is considered too high, then the hello interval should be increased.

Increasing the hold time is suggested if the PGP link is flapping. The possible causes include high route processor (RP) CPU load, high traffic, or high error rates on the links between the working and the protect routers.

We recommend that you have a hold time at least three times longer than the hello time (allowing three or more consecutive failed periodic message exchange failures).

The timers command is typically used only on the protect router. After the PGP connection is established, the working router learns about the timer settings from the protect router and automatically adjusts accordingly, regardless of its own timer configuration.

The timers command is meaningful only in multirouter automatic protection switching (APS) topologies and is ignored otherwise.
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure APS group 3 with the hello timer at 2 seconds and the hold timer at 6 seconds:

```
RP/0/RSP0/CPU0:router(config)# aps group 3
RP/0/RSP0/CPU0:router(config-aps)# timers 2 6
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group (global), on page 722</code></td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td><code>show aps group, on page 767</code></td>
<td>Displays information about the APS groups.</td>
</tr>
</tbody>
</table>
threshold (SONET)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET controller, use the threshold command in SONET/SDH configuration mode. To remove the setting of the threshold from the configuration file and restore the default condition, use the no form of this command.

```
threshold \{b1-tca \| b2-tca \| sd-ber \| sf-ber\} bit-error-rate
```

**Syntax Description**

- **b1-tca**: Sets the B1 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
- **b2-tca**: Sets the B2 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
- **sd-ber**: Sets the signal degrade BER threshold. Range is from 3 through 9. Default is 10e-6.
- **sf-ber**: Sets the signal failure BER threshold. Range is from 3 through 9. Default is 10e-3.

**Syntax Examples**

```
bit-error-rate  BER from 3 to 9 (10 to the minus x).
```

**Command Default**

- **b1-tca**: 10e-6
- **b2-tca**: 10e-6
- **sd-ber**: 10e-6
- **sf-ber**: 10e-3

**Command Modes**

SONET/SDH configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Signal failure BER and signal degrade BER are sourced from B2 BIP-8 error counts (as is B2-TCA). The **b1-tca** and **b2-tca** keywords print only a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the controller, use the **show controllers sonet** command.

**Examples**

The following example shows how to configure thresholds on the SONET controller:
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# threshold sd-ber 8
RP/0/RSP0/CPU0:router(config-sonet)# threshold sf-ber 4
RP/0/RSP0/CPU0:router(config-sonet)# threshold bl-tca 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report (SONET), on page 756</td>
<td>Permits selected SONET alarms to be logged to the console for a SONET controller.</td>
</tr>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
threshold (SONET path)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET path, use the `threshold` command in SONET/SDH path configuration mode. To remove the setting of the SONET path threshold from the configuration file and restore the default condition, use the `no` form of this command.

```
threshold b3-tca bit-error-rate
```

**Syntax Description**

- `b3-tca` Sets the B3 BER threshold crossing alarm (TCA). Default is 6.

- `bit-error-rate` BER from 3 to 9 (10 to the minus x).

**Command Default**

- `b3-tca: 6`

**Command Modes**

SONET/SDH path configuration

**Command History**

- **Release 3.9.0** This command was introduced.

**Usage Guidelines**

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

In addition to BIP errors detected at the local end in the receive direction, B3 error counts detected in the G1 byte (P-REI or P-FEBE) by the far-end SONET equipment are returned.

The `b3-tca` keyword prints only a log message to the console (if reports for them are enabled).

**Examples**

In the following example, the BER is set to 4:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# threshold b3-tca 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report (SONET), on page 756</td>
<td>Permits selected SONET alarms to be logged to the console for a SONET controller.</td>
</tr>
<tr>
<td>show controllers sonet, on page 775</td>
<td>Displays information about the operational status of SONET layers.</td>
</tr>
</tbody>
</table>
**tug3**

To specify the tributary unit group (TUG) number and enter the TUG3 controller configuration mode, use the `tug3` command in SONET controller configuration mode.

```
tug3  number
```

**Syntax Description**

`number`  The tributary unit group (TUG) number. The ranges are:

- AU4—The only value is 1.
- AU3—The range is 1 to 3.

**Command Default**

The default is 1.

**Command Modes**

SONET controller configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

The `tug3` command enables you to begin configuring the interface in the TUG3 controller configuration mode, where you can configure virtual containers (VCs) and DS3s:

STM1 -> AU4 -> TUG3 -> VC-3 -> DS3

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows how to specify `tug3 1`.

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/RSP0/CPU0:router(config-sonet)# au 1
RP/0/RSP0/CPU0:router(config-auPath)# tug3 1
RP/0/RSP0/CPU0:router(config-tug3Path)#
```

**Related Commands**

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>au</code>, on page 724</td>
<td>Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.</td>
</tr>
</tbody>
</table>
```
uneq-shut (SONET path)

To enable automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte, use the `uneq-shut` command in SONET/SDH path configuration mode. To disable this feature, use the `no` form of this command.

**uneq-shut**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Automatic insertion is enabled.

**Command Modes**
SONET/SDH path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `uneq-shut` command to disable automatic insertion of P-UNEQ code in the sent SONET path overhead C2 byte whenever the SONET path enters the administratively down state.

**Examples**
In the following example, automatic insertion of P-UNEQ code is disabled in the sent SONET path overhead C2 byte:

```
RP/0/RSP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RSP0/CPU0:router(config-sonet)# path
RP/0/RSP0/CPU0:router(config-sonet-path)# uneq-shut
```
**unidirectional**

To configure a protect interface for unidirectional mode, use the `unidirectional` command in APS group configuration mode. To restore the default setting, bidirectional mode, use the `no` form of this command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

Bidirectional mode is the default mode for the protect interface.

### Command Modes

APS group configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `unidirectional` command to configure a protect interface for unidirectional mode. Use the `no` form of this command to restore the default setting.

The unidirectional or bidirectional automatic protection switching (APS) operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment.

Note

We recommend using bidirectional APS mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. Cooperation occurs automatically when the SONET network equipment is in bidirectional mode.

In a multirouter APS topology, the `unidirectional` command is allowed only on the protect router.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure an APS group for unidirectional mode:

```plaintext
RP/0/RSP0/CPU0:router(config)# aps group 1
RP/0/RSP0/CPU0:router(config-aps)# unidirectional
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aps group (global)</code>, on page 722</td>
<td>Adds an automatic protection switching (APS) group and enter APS group configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show aps, on page 763</td>
<td>Displays the operational status for all configured SONET APS groups.</td>
</tr>
</tbody>
</table>
width

To set the number of paths in a stream, use the `width` command in the STS or AU controller configuration mode.

```
width  number
```

**Syntax Description**

- `number` Number of STS streams that are concatenated. The possible values are:
  - 1—Indicating one STS stream
  - 3—Indicating three STS streams (STS-3c)
  - 12—Indicating concatenation of 12 STS streams (STS-12c)
  - 48—Indicating concatenation of 48 STS streams (STS-48c)

Widths 3, 12, and 48 are configured on STS paths at natural boundaries, which coincide with the following path numbers:

- 1, 4, 7, 10, and so on, for STS-3c
- 1, 13, 25, and 37 for STS-12c
- 1 for STS-48c

**Command Default**

The default is 1.

**Command Modes**

SONET controller configuration

**Command History**

- **Release** 4.0.0  This command was introduced.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**
  - sonet-sdh
  - read,
  - write

**Examples**

The following example shows how to specify a width of 3:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# width 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode (SONET), on page 746</td>
<td>Sets the mode of an STS path, AU path, T3 controller, or TUG3 controller.</td>
</tr>
</tbody>
</table>
width
T3, E3, T1, E1 Controller Commands on the Cisco ASR 9000 Series Router

This module provides command line interface (CLI) commands for configuring T3/E3 and T1/E1 controllers on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- bert e1, on page 799
- bert e3, on page 801
- bert error, on page 803
- bert interval, on page 805
- bert pattern, on page 807
- bert t1, on page 810
- bert t3, on page 812
- cablelength, on page 814
- channel-group, on page 815
- clear controller lnm, on page 817
- clear controller t1, on page 820
- clear controller t3, on page 822
- clock source (T1/E1), on page 824
- clock source (T3/E3), on page 826
- controller e1, on page 828
- controller e3, on page 830
- controller t1, on page 832
- controller t3, on page 834
- delay clear (T1/E1), on page 836
- delay clear (T3/E3), on page 837
- delay trigger (T1/E1), on page 838
- delay trigger (T3/E3), on page 839
- description (T1/E1), on page 840
- description (T3/E3), on page 841
- down-when-looped (T1/E1), on page 842
- down-when-looped (T3/E3), on page 843
- dsu bandwidth, on page 844
- dsu mode, on page 846
- dsu remote, on page 848
- fd1, on page 849
- framing (E1), on page 850
- framing (E3), on page 851
- framing (T1), on page 852
- framing (T3), on page 853
- linecode, on page 854
- lnm major-warning, on page 856
- lnm minor-warning, on page 859
- lnm remove, on page 862
- lnm syslog, on page 865
- loopback (T1/E1), on page 867
- loopback (T3/E3), on page 869
- mdl, on page 871
- mode, on page 873
- national bits (E1), on page 875
- national bits (E3), on page 876
- show controllers e1, on page 877
- show controllers e3, on page 880
- show controllers lnm, on page 884
- show controllers t1, on page 887
- show controllers t3, on page 894
- shutdown (T1/E1), on page 901
- shutdown (T3/E3), on page 902
- speed (DS0), on page 903
- timeslots, on page 904
- yellow, on page 906
**bert e1**

To start or stop a configured bit error rate test (BERT) on an E1 controller or channel group, use the `bert e1` command in EXEC mode. To return to the default state, use the `no` form of this command.

```
bert e1 interface-path-id [channel-group channel-group-number] [error] {start | stop}
```

**Syntax Description**

*interface-path-id*  
Physical interface or virtual interface.  

**Note**  
Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

*channel-group [channel-group-number]*  
(Optional) Channel group number. When an E1 data line is configured, channel group numbers can be values from 0 to 30.  

**Note**  
For any of the DS0 time slots within the time slot range provided for the channel group, use time slot -1 as the channel number.

*error*  
(Optional) Injects errors into the running BERT stream.

*start*  
Starts the BERT on the E1 controller or channel.

*stop*  
Stops the BERT on the E1 controller or channel.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number. A physical layer interface module (PLIM) is always 0.
  - **port**: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.
Before you can start a BERT on an E1 controller or channel group, you must configure a BERT pattern using the `bert pattern` command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the `bert interval` command. Both of these commands are available in E1 configuration mode and channel group configuration mode.

To view the BERT results, use the `show controllers e1` command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

### Examples

The following example shows how to start and stop a BERT on an E1 controller:

```
RP/0/RSP0/CPU0:router# bert e1 0/3/0/0 start
RP/0/RSP0/CPU0:router# bert e1 0/3/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an E1 controller:

```
RP/0/RSP0/CPU0:router# bert e1 0/3/0/0 error
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert interval</code>, on page 805</td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern</code>, on page 807</td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td><code>show controllers e1</code>, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
</tbody>
</table>
**bert e3**

To start or stop a configured bit error rate test (BERT) on an E3 controller or channel group, use the `bert e3` command in EXEC mode. To return to the default state, use the `no` form of this command.

```plaintext
bert e3 interface-path-id [error] {start | stop}
```

**Syntax Description**

- `interface-path-id` Physical interface or virtual interface.
  
  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- `error` (Optional) Injects errors into the running BERT stream.

- `start` Starts the BERT on the E3 controller or channel.

- `stop` Stops the BERT on the E3 controller or channel.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  
  - `rack`: Chassis number of the rack.
  
  - `slot`: Physical slot number of the line card.
  
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

**Note**

Before you can start a BERT on an E3 controller, you must configure a BERT pattern using the `bert pattern` command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the `bert interval` command. Both of these commands are available in E3 configuration mode.
To view the BERT results, use the `show controllers e3` command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

### Task ID Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to start and stop a BERT on an E3 controller:

```plaintext
RP/0/RSP0/CPU0:router# bert e3 0/3/0/0/0 start
RP/0/RSP0/CPU0:router# bert e3 0/3/0/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an E3 controller:

```plaintext
RP/0/RSP0/CPU0:router# bert e3 0/3/0/0 error
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert interval</code>, on page 805</td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern</code>, on page 807</td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td><code>show controllers e3</code>, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
</tbody>
</table>
bert error

To insert errors into a BERT stream on a T3/E3 or T1/E1 line, use the `bert error` command in T3 or T1 configuration mode. To disable a BERT pattern, use the `no` form of this command.

```
bert error [number]
```

**Syntax Description**

- `number` Specifies the number of BERT errors to introduce into the bit stream. The range is from 1 to 255. The default is 1.

**Command Default**

The default is 1.

**Command Modes**

- T3 configuration
- E3 configuration
- T1 configuration
- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 and E1 configuration modes was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `bert error` command with the `bert pattern` command.

**Task ID**

- `sonet-sdh` read, write

**Examples**

The following example shows how to insert 10 errors into the BERT bit stream on the T3 controller in slot 0, subslot 3:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/RSP0/CPU0:router(config-t3e3)# bert error 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert interval, on page 805</code></td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern, on page 807</code></td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers e3, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
bert interval

To specify the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line, use the `bert interval` command in the appropriate configuration mode. To revert to the default interval, use the `no` form of this command.

```
bert interval time
```

**Syntax Description**

- **time**  Duration (in minutes) of the BERT. The interval can be a value from 1 to 14400. The default is 1 minute.

**Command Default**

A BERT runs for 1 minute.

**Command Modes**

- T3 configuration
- E3 configuration
- T1 configuration
- E1 configuration
- Channel group configuration for T1 and E1

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 and E1 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `bert interval` command with the `bert pattern` command. If the `bert interval` command is not used, then the BERT runs for a default of 1 minute.

**Task ID**

- **sonet-sdh**: read, write

**Examples**

The following example shows how to limit the BERT to 10 minutes on the T3 controller in slot 0, subslot 3:

```bash
RP/0/RSP0/CPU0:router(config)# controller t3 0/0/3/1/10
RP/0/RSP0/CPU0:router(config-t3e3)# bert interval 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert error</code>, on page 803</td>
<td>Insert errors into a BERT stream on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern</code>, on page 807</td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers e3, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
bert pattern

To enable a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line or an individual channel group, use the `bert pattern` command in T3, E3, T1, E1, or channel group configuration mode. To disable a BERT pattern, use the `no` form of this command.

`bert pattern {0s | 1in8 | 1s | 2^11 | 2^15 | 2^20 | 2^20-QRSS | 2^23 | 2^9 | 3in24 | 55Daly | 55Octet | alt-0-1 | ds0-1 | ds0-2 | ds0-3 | ds0-4}`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>0s</code></td>
<td>Invokes a repeating pattern of zeros (...000...).</td>
</tr>
<tr>
<td><code>1in8</code></td>
<td>(T1 and E1 only) Invokes a repeating pattern of one (1) bit in eight (8).</td>
</tr>
<tr>
<td><code>1s</code></td>
<td>Invokes a repeating pattern of ones (...111...).</td>
</tr>
<tr>
<td><code>2^11</code></td>
<td>(Channel group only) Invokes a pseudorandom O.151 test pattern that is 32,768 bits in length.</td>
</tr>
<tr>
<td><code>2^15</code></td>
<td>Invokes a pseudorandom O.151 test pattern that is 32,768 bits in length.</td>
</tr>
<tr>
<td><code>2^20</code></td>
<td>Invokes a pseudorandom O.153 test pattern that is 1,048,575 bits in length.</td>
</tr>
<tr>
<td><code>2^20-QRSS</code></td>
<td>Invokes a pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.</td>
</tr>
<tr>
<td><code>2^23</code></td>
<td>Invokes a pseudorandom O.151 test pattern that is 8,388,607 bits in length.</td>
</tr>
<tr>
<td><code>2^9</code></td>
<td>(Channel group only) Invokes a pseudorandom 0.153 test pattern of 511 bits in length.</td>
</tr>
<tr>
<td><code>3in24</code></td>
<td>(T1 and E1 only) Invokes a repeating pattern in which three (3) bits in twenty-four (24) are set to one (1) and the others are set to zero (0).</td>
</tr>
<tr>
<td><code>55Daly</code></td>
<td>(T1 and E1 only) Invokes a repeating pattern of fifty-five (55) 8-bit octets of data. This pattern introduces rapid transitions from long sequences of low-density octets to high-density octets, high-density octets to low-density octets, and rapid 1010 bit transitions.</td>
</tr>
<tr>
<td><code>55Octet</code></td>
<td>(T1 and E1 only) Invokes a repeating pattern of fifty-five (55) 8-bit octets of data. This pattern has fifteen (15) consecutive zeros.</td>
</tr>
<tr>
<td><code>alt-0-1</code></td>
<td>Invokes a repeating pattern of alternating zeros and ones (...01010...).</td>
</tr>
<tr>
<td><code>ds0-1</code></td>
<td>(Channel group only) Invokes a repeating sequence of 100x FFh, followed by 100x 00h. This combination of minimum and maximum densities causes stressing of the signal recovery circuitry.</td>
</tr>
<tr>
<td><code>ds0-2</code></td>
<td>(Channel group only) Invokes a repeating sequence of 100x 7Eh, followed by 100x 00h. This combination provides minimum ones density stressing as well as Layer 2 flag bytes.</td>
</tr>
<tr>
<td><code>ds0-3</code></td>
<td>(Channel group only) Invokes a repeating sequence of 200x 4Ch. This combination represents the typical SDD traffic patterns.</td>
</tr>
<tr>
<td><code>ds0-4</code></td>
<td>(Channel group only) Invokes a repeating sequence of 200x 40h. This combination represents the typical DEC VT traffic.</td>
</tr>
</tbody>
</table>
**Command Default**

BERT pattern test is disabled

**Command Modes**

- T3 configuration
- E3 configuration
- T1 configuration
- E1 configuration

Channel group configuration for T1 and E1

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>• Support for E3 and E1 configuration mode was added.</td>
</tr>
<tr>
<td></td>
<td>• Support for the ds0-1, ds0-2, ds0-3, and ds0-4 keywords was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

BERT is supported on each of the T3/E3 or T1/E1 links. It is done only over an unframed T3/E3 or T1/E1 signal and is run on only one port at a time. It is also supported on an individual channel group.

To begin a BERT, commit the configuration and use the `bert t1`, `bert e1`, `bert t3`, or `bert e3` command in EXEC mode.

To view the BERT results, use the `show controllers t1` or `show controllers t3` command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

**Examples**

The following example shows how to enable the running of a BERT pattern of all zeros on the T3 controller in slot 0, subslot 3:

```
RP/0/RSP0/CP00:router(config)# controller t3 0/0/3/1/10
RP/0/RSP0/CP00:router(config-t3e3)# bert pattern 0s
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bert error, on page 803</td>
<td>Insert errors into a BERT stream on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td>bert interval, on page 805</td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers e3, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
**bert t1**

To start or stop a configured bit error rate test (BERT) on a T1 controller or channel group, use the `bert t1` command in EXEC mode.

```
bert t1 interface-path-id [channel-group channel-group-number] [error] {start | stop}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>channel-group channel-group-number</th>
<th>(Optional) Channel group number. When a T1 data line is configured, channel group numbers can be values from 0 to 23.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>error</code></td>
<td>(Optional) Injects errors into the running BERT stream.</td>
</tr>
<tr>
<td><code>start</code></td>
<td>Starts the BERT on the T1 controller or channel.</td>
</tr>
<tr>
<td><code>stop</code></td>
<td>Stops the BERT on the T1 controller or channel.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

Release 3.9.0  This command was introduced.

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.
Before you can start a BERT on a T1 controller or channel group, you must configure a BERT pattern using the `bert pattern` command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the `bert interval` command. Both of these commands are available in T1 configuration mode and channel group configuration mode.

To view the BERT results, use the `show controllers t1` command in EXEC mode mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to start and stop a BERT on a T1 controller:

```
RP/0/RSP0/CPU0# bert t1 0/3/0/0/0 start
RP/0/RSP0/CPU0# bert t1 0/3/0/0/0 stop
```

The following example shows how to inject errors into the BERT stream on an T1 controller:

```
RP/0/RSP0/CPU0# bert t1 0/3/0/0 error
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert interval</code>, on page 805</td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern</code>, on page 807</td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td><code>show controllers t1</code>, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
To start or stop a configured bit error rate test (BERT) on a T3 controller or channel group, use the `bert t3` command in EXEC mode.

```
bert t3 interface-path-id [error] {start | stop}
```

**Syntax Description**
- `interface-path-id` Physical interface or virtual interface.

**Note**
- Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- `error` (Optional) Injects errors into the running BERT stream.
- `start` Starts the BERT on the T3 controller or channel.
- `stop` Stops the BERT on the T3 controller or channel.

**Command Default**
- No default behavior or values

**Command Modes**
- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

**Note**

Before you can start a BERT on a T3 controller, you must configure a BERT pattern using the `bert pattern` command. If desired, you can also adjust the default setting (1 minute) of the BERT interval using the `bert interval` command. Both of these commands are available in T3 configuration mode.
To view the BERT results, use the `show controllers t3` command in EXEC mode. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT
- Total bit errors
- Total bits received

BERT is data intrusive. Regular data cannot flow on a line while the test is in progress. The line is put in an alarm state when a BERT is in progress and restored to a normal state after a BERT has been terminated.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to start and stop a BERT on a T3 controller:

```
RP/0/RSP0/CPU0:router# bert t3 0/3/0/0 start
RP/0/RSP0/CPU0:router# bert t3 0/3/0/0 stop
```

The following example shows how to inject errors into the BERT stream on a T3 controller:

```
RP/0/RSP0/CPU0:router# bert t3 0/3/0/0 error
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bert interval, on page 805</code></td>
<td>Specifies the duration of a bit error rate test (BERT) pattern on a T3/E3 or T1/E1 line.</td>
</tr>
<tr>
<td><code>bert pattern, on page 807</code></td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td><code>show controllers t3, on page 894</code></td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
cablelength

To specify the distance of the cable from the routers to the network equipment, use the `cablelength` command in T3 or E3 configuration mode. To restore the default cable length, use the `no` form of this command.

```
cablelength  feet
```

**Syntax Description**

- `feet` Number of feet in the range from 0 to 450. The default is 224 feet.

**Command Default**

The default is 224 feet.

**Command Modes**

- T3 configuration
- E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 3.9.0 This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>Release 4.0.0 Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can specify a cable length from 0 to 450 feet; however, the hardware recognizes only two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is still within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

**Task ID**

- Task ID  Operations
  - sonet-sdh  read, write

**Examples**

The following example shows how to set the cable length for the router to 300 feet:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/RSP0/CPU0:router(config-t3)# cablelength 300
```
channel-group

To configure a DS0 channel group and enter channel group configuration mode, use the channel-group command in T1 or E1 configuration mode. To unassign a channel group, use the no form of this command.

channel-group channel-group-number

Syntax Description

| channel-group-number Note | Channel group number. When a T1 controller is configured, channel group numbers can be values from 0 to 23. |

Command Default

No default behavior or values

Command Modes

- T1 configuration
- E1 configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for DS0 channel groups and E1 configuration was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The channel-group command is available only on channelized SPAs.

Use the channel-group command in configurations in which the router must communicate with a T1 or an E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. An associated serial interface is created with each defined channel group.

Before the channel group configuration is valid, you must define the associated DS0 time slots using the timeslots command.

Use the no channel group command to delete a channel group.

Examples

The following example shows how to enter channel group configuration mode for channel group number 5 and change the speed of the underlying DS0s in the channel group to 56 kbps:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1)# channel-group 5
RP/0/RSP0/CPU0:router(config-t1-channel_group)# speed 56
```

The following example shows how to associate DS0 time slots 1, 6, 8, 9, and 10 to channel group 5:
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1)# channel-group 5
RP/0/RSP0/CPU0:router(config-t1-channel_group)# timeslots 1:6:8-10

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bert pattern, on page 807</td>
<td>Enables a BERT pattern on a T3/E3 or T1/E1 line or an individual channel group.</td>
</tr>
<tr>
<td>framing (E1), on page 850</td>
<td>Selects the frame type for an E1 data line.</td>
</tr>
<tr>
<td>framing (T1), on page 852</td>
<td>Selects the frame type for a T1 data line.</td>
</tr>
<tr>
<td>mode, on page 873</td>
<td>Sets the mode of the T3/E3 or T1/E1 controller.</td>
</tr>
<tr>
<td>speed (DS0), on page 903</td>
<td>Specifies the speed of the underlying DS0s in a channel group.</td>
</tr>
<tr>
<td>timeslots, on page 904</td>
<td>Associates one or more DS0 time slots to a channel group and create an associated serial subinterface.</td>
</tr>
</tbody>
</table>
clear controller lnm

To clear link noise monitoring statistics or reset states, use the **clear controller lnm** command in EXEC mode.

```markdown
clear controller {t1 | e1} interface-path-id lnm {state | statistics}
```

**Syntax Description**

- **t1**: Specifies clearing of LNM states or statistics for a T1 controller.
- **e1**: Specifies clearing of LNM states or statistics for an E1 controller.
- **interface-path-id**: Physical interface or virtual interface.

**Note**

- Use the **show controllers** command to see a list of all controllers currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

- **state**: Resets the LNM event states for the specified controller.
- **statistics**: Clears the LNM statistics for the specified controller and resets them to zero.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When specifying a channelized T1 controller, use the following guidelines for the **interface-path-id**:

- The naming notation is **rack/slot/module/port/T3Num/T1num**.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card.
  - **module**: Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - **port**: Physical port number of the interface.
  - **T3num**: T3 controller number.
  - **T1num**: T1 controller number.
There should not normally be any need to clear the LNM controller states. The `state` option resets the LNM configuration which causes an update of the current LNM states in the system. Therefore, under normal conditions, if the controller is in alarm state, the reset should continue to report the alarm state; alternatively, if the controller is clear of any alarms, the reset will show the stable state. The use of the `clear controller lnm state` command does not actually clear any alarms, but causes a refresh of their values in the system. Therefore, this command can be used if the reported controller state should happen to be out of synchronization with the actual controller state.

To view the status of the controllers, use the `show controllers t1` command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to reset link noise monitoring states for the channelized T1 controller 1 that is located in chassis 0, for a SIP installed in slot 1 with a SPA in subslot 0, and port 0 with T3 controller 1, and channelized T1 controller 1:

```
RP/0/RSP0/CPU0:router# clear controller t1 0/1/0/0/1/1 lnm state
```

The following example shows how to clear link noise monitoring statistics for the channelized T1 controller 1 that is located in chassis 0, for a SIP installed in slot 1 with a SPA in subslot 0, and port 0 with T3 controller 1, and channelized T1 controller 1:

```
RP/0/RSP0/CPU0:router# clear controller t1 0/1/0/0/1/1 lnm statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller e1, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>controller t1, on page 832</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal major warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm major-warning, on page 856</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm minor-warning, on page 859</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal the noise attribute to PPP for removal of an MLPPP bundle link.</td>
</tr>
<tr>
<td>lnm remove, on page 862</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal the noise attribute to PPP for removal of an MLPPP bundle link.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>lnm syslog, on page 865</strong></td>
<td>Enables logging of link noise monitoring major, remove, and minor events and alarms.</td>
</tr>
<tr>
<td><strong>show controllers e1, on page 877</strong></td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td><strong>show controllers lnm, on page 884</strong></td>
<td>Displays information about LNM on T1 or E1 links.</td>
</tr>
<tr>
<td><strong>show controllers t1, on page 887</strong></td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
clear controller t1

To clear T1 controller data, use the **clear controller t1** command in EXEC mode.

```
clear controller t1 interface-path-id
```

**Syntax Description**
- `interface-path-id` Physical interface or virtual interface.

**Note**
- Use the **show controllers** command to see a list of all controllers currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- **Release 3.9.0** This command was introduced.

**Usage Guidelines**
- When specifying a channelized T1 controller, use the following guidelines for the `interface-path-id`:
  - The naming notation is `rack/slot/module/port/T3Num/T1num`.
  - The slash between values is required as part of the notation.
  - The following list describes the components of the notation:
    - `rack`—Chassis number of the rack.
    - `slot`—Physical slot number of the line card.
    - `module`—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
    - `port`—Physical port number of the interface.
    - `T3num`—T3 controller number.
    - `T1num`—T1 controller number.
  - If specifying a virtual interface, the number range varies, depending on interface type.
  - When specifying a virtual tributary group, the naming notation is `rack/slot/module/port/vtg/vt`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
    - `rack`—Chassis number of the rack.
    - `slot`—Physical slot number of the line card.
- **module**—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.

- **port**—Physical port number of the interface.

- **vrg**—Virtual tributary group.

- **vt**—Virtual tributary instance.

To view the status of the controllers, use the **show controllers t1** command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to clear controller data for the channelized T1 controller 1 that is located in chassis 0, for a SIP installed in slot 1 with a SPA in subslot 0, and port 0 with T3 controller 1, and channelized T1 controller 1:

```
RP/0/RSP0/CPU0:router# clear controller t1 0/1/0/0/1/1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller t1, on page 832</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
clear controller t3

To clear T3 controller data, use the `clear controller t3` command in EXEC mode.

```
clear controller t3 interface-path-id
```

**Syntax Description**

`interface-path-id` Physical interface or virtual interface.

**Note** Use the `show controllers` command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is `rack/slot/module/port/T3num`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`—Chassis number of the rack.
  - `slot`—Physical slot number of the line card or SIP.
  - `module`—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - `port`—Physical port number of the interface.
  - `T3num`—T3 controller number.

To view the status of the controllers, use the `show controllers t3` command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>dwdm</td>
<td>read,</td>
<td>write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>read,</td>
<td>write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Task ID Operations

| sonet-sdh | read, write |

### Examples

The following example shows how to clear controller data for T3 controller 1 that is located in chassis 0, for a SIP installed in slot 6 with a SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/RSP0/CPU0:router(config)# controller t3 0/6/2/0/1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller t3, on page 834</td>
<td>Configures a T3 controller and enters T3 configuration mode.</td>
</tr>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
clock source (T1/E1)

To set clocking for individual T1 or E1 links, use the `clock source` command in T1 or E1 configuration mode. To return to the default, use the `no` form of this command.

```
clock source {internal | line}
```

**Syntax Description**

- `internal` Specifies that the clock is generated from the internal clock of the T1 or E1 controller. The default is internal.
- `line` Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).

**Note** When configuring clocking on a serial link, you need to configure one end to be `internal` and the other end to be `line`. If you configure `internal` clocking on both ends of a connection, framing slips occur. If you configure `line` clocking on both ends of a connection, the line does not come up.

**Command Default**
The default clock source is internal.

**Command Modes**

- T1 configuration
- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E1 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following example shows how to set the clocking on the T1 controller in slot 6, subslot 0 to internal:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1e1)# clock source internal
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>controller e1</code>, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>controller t1, on page 832</td>
<td>clock source (T1/E1)</td>
</tr>
</tbody>
</table>
# clock source (T3/E3)

To set clocking for individual T3 or E3 links, use the `clock source` command in T3 or E3 configuration mode. To return to the default, use the `no` form of this command.

```
clock source {internal | line}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Specifies that the clock is generated from the internal clock of the T3 controller. The default is internal.</td>
</tr>
<tr>
<td>line</td>
<td>Specifies that the clock on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).</td>
</tr>
</tbody>
</table>

**Note**

When configuring clocking on a serial link, you need to configure one end to be `internal` and the other end to be `line`. If you configure `internal` clocking on both ends of a connection, framing slips occur. If you configure `line` clocking on both ends of a connection, the line does not come up.

## Command Default

The default clock source is internal.

## Command Modes

- T3 configuration
- E3 configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

If you do not specify the `clock source` command, the default clock source is used.

Configure the `clock source line` command if your telephone company or the remote data service unit provides the master clock of the T3 or E3 connection.

Configure the `clock source internal` command if your router provides the master clock of the T3 or E3 connection.

**Note**

For a back-to-back connection between two T3 network modules, one controller must be configured for internal clocking while the other controller must be configured for line clocking.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to set the clocking to line on the T3 controller 1 that is located in chassis 0, on a SIP installed in slot 6 with a SPA in subslot 0, on port 0 with T3 controller 1:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/RSP0/CPU0:router(config-t3)# clock source line
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller e3, on page 830</td>
<td>Configures an E3 controller and enters E3 configuration mode.</td>
</tr>
<tr>
<td>controller t3, on page 834</td>
<td>Configures a T3 controller and enters T3 configuration mode.</td>
</tr>
</tbody>
</table>
controller e1

To configure an E1 controller and enter E1 configuration mode, use the **controller e1** command in Global Configuration mode. To return to the default state, use the **no** form of this command.

```
controller e1 interface-path-id
```

**Syntax Description**
- `interface-path-id`: Physical interface or virtual interface.

**Note**
- Use the `show controllers` command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
- No default behavior or values

**Command Modes**
- Global Configuration

**Command History**
- **Release** 4.0.0  This command was introduced.

**Usage Guidelines**
For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

The **controller e1** command is used in configurations in which the router is intended to communicate with an E1 fractional data line. The **controller e1** command is available only on channelized interfaces.

Use the **mode** command in T3 configuration mode to specify the mode for the port. The default mode for 2-Port and 4-Port Channelized T3 SPAs is T1.

**Note**
If you do not use the **mode** command to define the port to be E1, you cannot configure the E1 controller.

To view the status of the controllers, use the **show controllers e1** command.
**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter E1 configuration mode for a controller:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/1/0/0
RP/0/RSP0/CPU0:router(config-e1)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode, on page 873</td>
<td>Sets the mode of the T3/E3 or T1/E1 controller.</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
</tbody>
</table>
**controller e3**

To configure an E3 controller and enter E3 configuration mode, use the `controller e3` command in Global Configuration mode. To return to the default state, use the `no` form of this command.

```
controller e3 interface-path-id
```

**Syntax Description**  
`interface-path-id` Physical interface or virtual interface.

**Note**  
Use the `show controllers` command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**  
No default behavior or values

**Command Modes**  
Global Configuration

**Command History**  
```
Release | Modification
---------|------------------
4.0.0     | This command was introduced.
```

**Usage Guidelines**  
For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

To view the status of the controllers, use the `show controllers e3` command.

**Task ID**  
```
Task ID | Operations
--------|-----------
interface | read, write
```

**Examples**  
The following example shows how to enter E3 configuration mode for a controller in slot 6, on the SPA in subslot 2, on E3 controller 0:
RP/0/RSP0/CPU0:router(config)# **controller e3 0/6/2/0**
RP/0/RSP0/CPU0:router(config-e3)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show controllers e3, on page 880</strong></td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
<td></td>
</tr>
</tbody>
</table>
controller t1

To configure a T1 controller and enter T1 configuration mode, use the controller t1 command in Global Configuration mode. To return to the default state, use the no form of this command.

controller t1 interface-path-id

Syntax Description

interface-path-id  Physical interface or virtual interface.

Note  Use the show controllers command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

Global Configuration

Command History

Release 3.9.0  This command was introduced.

Usage Guidelines

When specifying a channelized T1 controller, use the following guidelines for the interface-path-id:

- The naming notation is rack/slot/module/port/T3Num/T1num.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:
  - rack—Chassis number of the rack.
  - slot—Physical slot number of the line card.
  - module—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - port—Physical port number of the interface.
  - T3num—T3 controller number.
  - T1num—T1 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.
- When specifying a virtual tributary group, the naming notation is rack/slot/module/port/vtg/vt. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - rack—Chassis number of the rack.
  - slot—Physical slot number of the line card.
- **module**—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
- **port**—Physical port number of the interface.
- **vrg**—Virtual tributary group.
- **vt**—Virtual tributary instance.

The `controller t1` command is used in configurations in which the router is intended to communicate with a T1 fractional data line. The `controller t1` command is available only on channelized SPAs.

Use the `mode` command in T3 configuration mode to specify the mode for each T3 port.

To view the status of the controllers, use the `show controllers t1` command.

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection as the yellow alarm can be incorrectly detected with SF framing.

Serial interface may flap and eventually, go down if yellow alarm detection is not disabled on its T1 controller configured with SF framing.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enter T1 configuration mode for a controller:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-t1)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mode, on page 873</code></td>
<td>Sets the mode of the T3/E3 or T1/E1 controller.</td>
</tr>
<tr>
<td><code>show controllers t1, on page 887</code></td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
**controller t3**

To configure a T3 controller and enter T3 configuration mode, use the `controller t3` command in Global Configuration mode. To return to the default state, use the `no` form of this command.

```plaintext
controller t3 interface-path-id
```

**Syntax Description**

`interface-path-id` Physical interface or virtual interface.

**Note** Use the `show controllers` command to see a list of all controllers currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is `rack/slot/module/port/T3num`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`—Chassis number of the rack.
  - `slot`—Physical slot number of the line card or SIP.
  - `module`—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - `port`—Physical port number of the interface.
  - `T3num`—T3 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.

To view the status of the controllers, use the `show controllers t3` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to enter T3 configuration mode for T3 controller 1 that is located in chassis 0, for a SIP installed in slot 6 with a SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RSP0/CPU0:router(config-t3)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
delay clear (T1/E1)

To configure the amount of time before a T1 or E1 path delay trigger alarm is cleared, use the delay clear command in T1 or E1 configuration mode. To return the command to its default setting, use the no form of this command.

delay clear value

Syntax Description

value Value, in milliseconds, before a T1 path delay trigger alarm is cleared. The range is from 0 through 180000. The default is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

T1 configuration
E1 configuration

Command History

Release | Modification
--------|-------------------
3.9.0    | This command was introduced.
4.0.0    | Support for E1 configuration mode was added.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to specify that T1 path delay trigger alarms should be cleared after 9000 seconds:

RP/0/RSP0/CPU0:router(config)# controller t1 0/4/2/0/1
RP/0/RSP0/CPU0:router(config-t1)# delay clear 9000

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay trigger (T1/E1), on page 838</td>
<td>Configures a time value for the T1 or E1 path delay trigger.</td>
</tr>
</tbody>
</table>
delay clear (T3/E3)

To configure the amount of time before a T3 or E3 path delay trigger alarm is cleared, use the `delay clear` command in T3 or E3 configuration mode. To return the command to its default setting, use the `no` form of this command.

```
delay clear value
```

**Syntax Description**

- `value`: Value, in milliseconds, before a T3 or E3 path delay trigger alarm is cleared. The range is from 0 through 180000. The default is 10 seconds.

**Command Default**
The default is 10 seconds.

**Command Modes**
- T3 configuration
- E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- `read`, `write`

**Examples**
The following example shows how to specify that T3 path delay trigger alarms should be cleared after 9000 seconds:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/RSP0/CPU0:router(config-t3)# delay clear 9000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay trigger (T3/E3)</code>, on page 839</td>
<td>Configures a time value for the T3 or E3 path delay trigger.</td>
</tr>
</tbody>
</table>
**delay trigger (T1/E1)**

To configure a time value for the T1 or E1 path delay trigger, use the `delay trigger` command in T1 or E1 configuration mode. To return the command to its default setting, use the `no` form of this command.

```
delay trigger value
```

**Syntax Description**

- `value` Sets the T1 path delay trigger value, in milliseconds. The range is from 0 through 60000. The default is 2.5 seconds.

**Command Default**
The default is 2.5 seconds.

**Command Modes**
- T1 configuration
- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E1 configuration was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If the timer for the T1 or E1 path delay trigger expires, an alarm is declared.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set the T1 path delay trigger to 8000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/4/2/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# delay trigger 8000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay clear (T1/E1), on page 836</td>
<td>Configures the amount of time before a T1 or E1 path delay trigger alarm is cleared.</td>
</tr>
</tbody>
</table>
delay trigger (T3/E3)

To configure a time value for the T3 or E3 path delay trigger, use the `delay trigger` command in T3 or E3 configuration mode. To return the command to its default setting, use the `no` form of this command.

```
delay trigger value
```

**Syntax Description**

- `value`: Sets the T3 path delay trigger value, in milliseconds. The range is from 0 through 60000. The default is 2.5 seconds.

**Command Default**

The default is 2.5 seconds.

**Command Modes**

- T3 configuration
- E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 configuration was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the timer for the T3 or E3 path delay trigger expires, an alarm is declared.

**Task ID**

- `sonet-sdh`: read, write

**Examples**

The following example shows how to set the T3 path delay trigger to 8000 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/4/2/0/1
RP/0/RSP0/CPU0:router(config-t3)# delay trigger 8000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay clear (T3/E3)</code>, on page 837</td>
<td>Configures the amount of time before a T3 or E3 path delay trigger alarm is cleared.</td>
</tr>
</tbody>
</table>
description (T1/E1)

To configure a description for a T1 or E1 controller, use the `description` command in T1 or E1 configuration mode. To delete a T1 or E1 controller description, use the `no` form of this command.

```
description  text
```

**Syntax Description**

- `text` A text string comprised of alphanumeric characters.

**Command Default**

No description is configured.

**Command Modes**

- T1 configuration
- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E1 configuration was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a description for a T1 controller:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/2/0
RP/0/RSP0/CPU0:router(config-t1)# description This is a sample description for T1 controller 0/6/2/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
description (T3/E3)

To configure a description for a T3 or E3 controller, use the `description` command in T3 or E3 configuration mode. To delete a T3 controller description, use the `no` form of this command.

**Syntax Description**
```
description text
```
- **text**: A text string comprised of alphanumeric characters.

**Command Default**
No description is configured.

**Command Modes**
- T3 configuration
- E3 configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- **sonet-sdh**: read, write
- **interface**: read, write

**Examples**
The following example shows how to configure a description for a T3 controller:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/RSP0/CPU0:router(config-t3)# description This is a sample description for T3 controller 0/6/2/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show controllers e3</strong>, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td><strong>show controllers t3</strong>, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
down-when-looped (T1/E1)

To configure a T1 or E1 controller to inform the system that it is down when loopback is detected, use the `down-when-looped` command in T1 or E1 configuration mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
By default, a T1 or E1 controller does not inform the system that it is down when loopback is detected.

**Command Modes**
- T1 configuration
- E1 configuration

**Command History**
- Release 3.9.0: This command was introduced.
- Release 4.0.0: Support for E1 configuration mode was added.

**Usage Guidelines**
This command does not have a `no` form.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure a T1 controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/4/2/0/1
RP/0/RSP0/CPU0:router(config-t1)# down-when-looped
```

down-when-looped is a traffic-affecting operation if any loopback is present.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>loopback (T1/E1)</code>, on page 867</td>
<td>Loops individual T1 or E1 channels on the channelized T3 controller.</td>
</tr>
</tbody>
</table>
down-when-looped (T3/E3)

To configure a T3 or E3 controller to inform the system that it is down when loopback is detected, use the `down-when-looped` command in T3 or E3 configuration mode.

```
down-when-looped
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
By default, a T3 or E3 controller does not inform the system that it is down when loopback is detected.

**Command Modes**
T3 configuration  
E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command does not have a `no` form.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure a T3 controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/4/2/0
RP/0/RSP0/CPU0:router(config-t3)# down-when-looped
```

down-when-looped is a traffic-affecting operation if any loopback is present

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback (T3/E3), on page 869</td>
<td>Loops the entire T3 or E3 line on the T3 controller or E3 controller.</td>
</tr>
</tbody>
</table>
dsu bandwidth

To specify the maximum allowable bandwidth used by a T3 or an E3 controller, use the `dsu bandwidth` command in T3 or E3 configuration mode. To return to the default state, use the `no` form of this command.

`dsu bandwidth kbps`

**Syntax Description**

`kbps` Maximum bandwidth, in kilobits per second (kbps). Range is from 75 to 44210. The default is 44210.

**Command Default**

The default bandwidth is 44210.

**Command Modes**

T3 configuration

E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The local interface configuration must match the remote interface configuration. For example, if you reduce the maximum bandwidth to 16,000 on the local port, you must also do the same on the remote port.

The `dsu bandwidth` command reduces the bandwidth by padding the E3 and T3 frame.

To verify the data service unit (DSU) bandwidth configured on the interface, use the `show controllers t3` or `show controllers e3` command in EXEC mode.

When G.751 framing is used on E3 links, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps. Before framing bypass can be used, a DSU bandwidth of 34,010 kbps must be configured.

Although software allows the user to configure a continuous range of bandwidths in subrate modes, vendors support bandwidths only in quantums (for example, in a ADC Kentrox T3 link, bandwidth must be in multiples of 500 kbps). Therefore, the software sets the user-configured bandwidth to the closest vendor-supported bandwidth. Use the `show controllers t3` or `show controllers e3` command to display the actual bandwidth that is configured.

The following table shows DSU modes and vendor-supported bandwidths.

**Table 57: DSU Modes and Vendor-supported Bandwidths**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Bandwidth (in kbps)</th>
<th>Bandwidth Multiples (in kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Link or Cisco</td>
<td>358–34010 for E3300–44210 for T3</td>
<td>358 300.746</td>
</tr>
<tr>
<td>ADC Kentrox T3 IDSU</td>
<td>1000–34010 for E31500–44210 for T3</td>
<td>500 500</td>
</tr>
<tr>
<td>Larscom Access T45</td>
<td>3100–44210 kbps</td>
<td>3158</td>
</tr>
</tbody>
</table>
### Bandwidth Multiples (in kbps)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Bandwidth (in kbps)</th>
<th>Bandwidth Multiples (in kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adtran T3SU 300</td>
<td>75–44210 kbps</td>
<td>75.186</td>
</tr>
<tr>
<td>Verilink HDM 2182</td>
<td>1500–44210 kbps</td>
<td>1579</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set the maximum allowable DSU bandwidth to 16,000 kbps on a SIP in slot 6, on the SPA in subslot 2, for port 0, and T3 controller 1:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RSP0/CPU0:router(config-t3)# dsu bandwidth 16000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers e3, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
dsu mode

To specify the interoperability mode used by a T3 or an E3 controller, use the **dsu mode** command in T3 or E3 configuration mode. To return to the default state, use the **no** form of this command.

**dsu mode mode**

**Syntax Description**

`mode` DSU mode. Valid values are as follows:

- (T3 only) *adtran*
- (E3 only) *cisco*
- digital-link
- kentrox
- (T3 only) *larscom*
- (T3 only) *verilink*

For T3, digital-link is default and for E3 cisco is default.

**Command Default**

For T3, digital-link is default and for E3 cisco is default.

**Command Modes**

T3 configuration

E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default DSU mode Cisco is equivalent to Digilink Mode with Scrambling Enabled. This mode was added to enable scrambling along with Digilink mode on E3 Controllers.

Digilink Mode, by definition does not support scrambling for E3 Controllers though it supports the same for T3 Controllers. For T3 controllers, there is no functional default DSU mode. The DSU Mode Cisco is not applicable for T3 Controller.

For interoperability, it is recommended to always configure the DSU mode command under T3/E3 Controller by matching the DSU type of the remote port.

To enable Scrambling, configure Scramble under the respective Serial Interface for the T3/E3 Controller.

Refer to Table 57: DSU Modes and Vendor-supported Bandwidths, on page 844 for more information regarding the modes.

The local interface configuration must match the remote interface configuration. For example, if you define the data service unit (DSU) interoperability mode as **digital-link** on the local port, you must also do the same on the remote port.

You must know what type of DSU is connected to the remote port to determine if it interoperates with a T3 or an E3 controller. The **dsu mode** command enables and improves interoperability with other DSUs.

To verify the DSU mode configured on the interface, use the **show controllers t3** command in EXEC mode.
### Examples

The following example shows how to set the DSU mode to `digital-link` for T3 controller 1 located in chassis 0, on a SIP in slot 6 and SPA in subslot 2, and port 0 with T3 controller 1:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/2/0/1
RP/0/RSP0/CPU0:router(config-t3)# dsu mode digital-link
```
dsu remote

To control the bandwidth usage with the remote port, use the dsu remote command in T3 or E3 configuration mode. To return to the default state, use the no form of this command.

```
dsuc remote {disable | fullrate}
```

**Syntax Description**
- `disable` Denies incoming remote requests to reset the bandwidth to the full rate.
- `fullrate` Requests that the remote port set its bandwidth to full rate.

**Command Default**
Remote accept is the default.

**Command Modes**
- T3 configuration
- E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced. Release 3.9.0</td>
</tr>
<tr>
<td></td>
<td>Support for E3 configuration mode was added. Release 4.0.0</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To verify the DSU remote settings configured on the interface, use the `show controllers t3` command in EXEC mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to specify that the connected remote port set its bandwidth to full rate:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/2/0
RP/0/RSP0/CPU0:router(config-t3)# dsu remote fullrate
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
To enable or disable the transmission of performance reports through Facility Data Link (FDL) for a T1 channel on the channelized T3 interface, use the `fdl` command in T1 configuration mode. To return to the default state of performance reporting, use the `no` form of this command.

```
fdl {ansi | att} {enable | disable}
```

**Syntax Description**
- **ansi**: Specifies the transmission of ANSI T1.403 once-per-second performance reports.
- **att**: Specifies the transmission of AT&T TR54016 once-per-second performance reports.
- **enable**: Enables transmission of the specified performance reports.
- **disable**: Disables transmission of the specified performance reports. The default is disable.

**Command Default**
The transmission of ANSI T1.403 and AT&T TR54016 performance reports through FDL are disabled.

**Command Modes**
T1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `fdl` command applies only to T1 lines and can be used only if the T1 framing type is Extended Super Frame (ESF).

To display the performance report information, use the `show controllers t1` command.

**Examples**
The following example shows how to enable ANSI T1.403 performance reports for T1 channel 10:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/1/10
RP/0/RSP0/CPU0:router(config-t1e1)# fdl ansi enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers t1</code>, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
framing (E1)

To select the frame type for an E1 data line, use the `framing` command in E1 configuration mode. To disable E1 framing, use the `no` form of this command.

```
framing  {crc4 | no-crc4 | unframed}
```

**Syntax Description**

- `crc4` Specifies framing with CRC-4 error-monitoring capabilities. The default is `crc4`.
- `no-crc4` Specifies framing without CRC-4 error-monitoring capabilities.
- `unframed` Specifies unframed E1.

**Command Default**
The default is `crc4`.

**Command Modes**
E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `framing` command in configurations in which the router or access server is intended to communicate with E1 fractional data lines. The service provider determines the framing type required for your E1 circuit.

**Task ID**

- `sonet-sdh` read, write

**Examples**
The following example shows how to select E1 framing without CRC-4 error-monitoring capabilities:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# framing no-crc4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e1</code>, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
</tbody>
</table>
framing (E3)

To select the frame type for E3 data lines, use the `framing` command in E3 configuration mode. To disable E3 framing, use the `no` form of this command.

```
framing {g751 | g832}
```

**Syntax Description**

- `g751` Specifies that G.751 framing is used as the E3 framing type. The default is G.751.
- `g832` Specifies that G.832 framing is used as the E3 framing type.

**Command Default**

The default is G.751.

**Command Modes**

E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not use the `framing` command, the default is used by the E3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1/E1 channel by using the `framing` command in T1 or E1 configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to select G751 as the E3 frame type:

```
RP/0/RSP0/CPU0:router(config)# controller e3 0/6/0/0
RP/0/RSP0/CPU0:router(config-e3)# framing g751
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e3</code>, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
</tbody>
</table>
framing (T1)

To select the frame type for a T1 data line, use the `framing` command in T1 configuration mode. To disable T1 framing, use the `no` form of this command.

```
framing {esf | sf}
```

**Syntax Description**
- `esf`: Specifies extended super frame as the T1 frame type. The default is `esf`.
- `sf`: Specifies super frame as the T1 frame type.

**Command Default**
The default is `esf`.

**Command Modes**
T1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `framing` command in configurations in which the router or access server is intended to communicate with T1 fractional data lines. The service provider determines the framing type required for your T1 circuit.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to select super frame as the T1 frame type:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1)# framing sf
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers t1</code>, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
framing (T3)

To select the frame type for T3 data lines, use the `framing` command in T3 configuration mode. To disable T3 framing, use the `no` form of this command.

```
framing  {c-bit | m23}
```

**Syntax Description**
- `c-bit` Specifies that C-bit framing is used as the T3 framing type. The default is `c-bit`.
- `m23` Specifies that M23 framing is used as the T3 framing type.

**Command Default**
The default is `c-bit`.

**Command Modes**
T3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If you do not use the `framing` command, the default is used by the T3 controllers to automatically determine the framing type received from the far-end equipment. You can also set the framing for each T1 or E1 channel by using the `framing` command in T1 or E1 configuration mode.

**Task ID**
- `sonet-sdh` read, write

**Examples**
The following example shows how to select M23 as the T3 frame type:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/0/0/1
RP/0/RSP0/CPU0:router(config-t3)# framing m23
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers t3</code>, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
linecode

To select the line-code type for T1 or E1 lines, use the `linecode` command in T1 or E1 configuration mode. To return the line to the default line-code type, use the `no` form of this command.

```
linecode  {ami | b8zs | hdb3}
```

**Syntax Description**
- **ami** (T1 only) Specifies alternate mark inversion (AMI) as the line-code type. This value is the default for E1 lines.
- **b8zs** (T1 only) Specifies B8ZS as the line-code type. This value is the default for T1 lines.
- **hdb3** (E1 only) Specifies high-density bipolar 3 (HDB3) as the line-code type.

**Command Default**
- T1 lines: the default is B8ZS.
- E1 lines: the default is AMI.

**Command Modes**
- T1 configuration
- E1 configuration

**Command History**
- Release 3.9.0  This command was introduced.
- Release 4.0.0  Support for E1 configuration mode was added.

**Usage Guidelines**
Use this command in configurations where the router must communicate with T1 or E1 fractional data lines. The T1 or E1 service provider determines which line-code type is required for your T1 or E1 circuit.

**Examples**
The following example shows how to select AMI as the T1 line-code type:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# linecode ami
```

The following example shows how to select HDB3 as the E1 line-code type:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/4/1/1
RP/0/RSP0/CPU0:router(config-e1)# linecode hdb3
```

**Related Commands**
- `show controllers e1`, on page 877  Displays information about the E1 links and hardware and software drivers for the E1 controller.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
To enable link noise monitoring and specify thresholds for noise errors on T1/E1 links that are used to signal major warning events and recovery from those events, use the `lnm major-warning` command in T1 or E1 controller configuration mode. To disable link noise monitoring major warnings, use the `no` form of this command.

```
lnm major-warning [{clear | set} [line-code-violation lcv-value [path-code-violation pcv-value]] [duration seconds]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear</code></td>
<td>(Optional) Specifies threshold values for Line Code Violation (LCV) and Path Code Violation (PCV) errors that are used to determine when a recovery from a major warning has occurred and a “cleared” event is signalled. The clear threshold values cannot exceed the set threshold values.</td>
</tr>
<tr>
<td><code>set</code></td>
<td>(Optional) Specifies the high threshold values for LCV and PCV that are used to signal a major warning event on the link. When errors on the link are greater than or equal to these values, a major warning occurs and a “crossed” event is signalled.</td>
</tr>
</tbody>
</table>
| `line-code-violation lcv-value` | (Optional) Specifies the threshold value for LCV errors (Bi-Polar Violation [BPV] or Excessive Zeroes [EXZ]), in the following possible ranges:  
  - For T1 links, the range is 5 to 1544. The default is 1544.  
  - For E1 links, the range is 7 to 2048. The default is 2048. |
| `path-code-violation pcv-value` | (Optional) Specifies the threshold value for PCV errors (CRC errors), in the following possible ranges:  
  - For T1 links, the range is 3 to 320. The default is 320.  
  - For E1 links, the range is 5 to 832. The default is 831. |
| `duration seconds` | (Optional) Specifies the period of time (in seconds) during which the number of link noise errors must continuously exceed the set threshold levels to signal a major warning, or remain below the clear threshold levels to signal a cleared event. The range is 4 to 600. The default is 10. |

### Command Default

Link noise monitoring is disabled.

If the `lnm major-warning` command is run without specifying `set` or `clear` options, then `set` is used as the default option with its default values. The `clear` option inherits the same threshold values as the default `set` threshold values.

If the `lnm major-warning` command is run and only the `set` option is configured, the threshold values defined for the `set` option are also used as the `clear` threshold values. Alternatively, if the `lnm major-warning` command is run and only the `clear` option is configured, the threshold values defined for the `clear` option are also used as the `set` threshold values.

### Command Modes

- T1 configuration
- E1 configuration
Command History

Release 4.0.0  This command was introduced.

Usage Guidelines

This command can only be configured on full T1 or E1 channel groups; it is not supported on fractional, or DS0 links.

The `lnm major-warning` command cannot be configured with the `lnm remove` command—they are mutually exclusive.

The major threshold values must be greater than the values configured in the `lnm minor-warning` command.

LNM supports hierarchical level alarm reporting as defined in the Telcordia (Bellcore) GR-253 standard. Hierarchical alarm reporting means that whenever a higher alarm is asserted, the lower alarm state is suppressed. When the high alarm is cleared, the lower alarm will re-assert if the condition still exists.

For LNM, this means that if a major warning threshold is exceeded resulting in a crossed event and alarm state reached, then a minor warning alarm state is suppressed and placed in stable state. The minor crossed event also is removed from the bistate log. Only a single crossed event for major warnings will appear in the bistate log for the controller. When the major warning is cleared, the minor warning alarm is asserted if the condition still exists.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enable link noise monitoring on a T1 channel group using the default values for the set and clear threshold values of 1544 LCVs and 320 PCVs for a duration of 10 seconds:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# lnm major-warning
```

The following example shows how to specify set and clear thresholds on an E1 channel group:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/3/0/0/0/1
RP/0/RSP0/CPU0:router(config-e1)# lnm major-warning set line-code-violation 1500 path-code-violation 100 duration 30
RP/0/RSP0/CPU0:router(config-e1)# lnm major-warning clear line-code-violation 1400 path-code-violation 95 duration 30
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controller lnm</td>
<td>on page 817  Clears link noise monitoring statistics or resets states.</td>
</tr>
<tr>
<td>controller e1</td>
<td>on page 828  Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>controller t1</td>
<td>on page 832</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lnm minor-warning, on page 859</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm syslog, on page 865</td>
<td>Enables logging of link noise monitoring major, remove, and minor events and alarms.</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers lnm, on page 884</td>
<td>Displays information about LNM on T1 or E1 links.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
To enable link noise monitoring and specify thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events, use the `lnm minor-warning` command in T1 or E1 controller configuration mode. To disable link noise monitoring minor warnings, use the `no` form of this command.

```
lnm minor-warning [{clear | set} [line-code-violation lcv-value [path-code-violation pcv-value]] [duration seconds]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>(Optional) Specifies threshold values for Line Code Violation (LCV) and Path Code Violation (PCV) errors that are used to determine when a recovery from a minor warning has occurred and a “cleared” event is signalled. The clear threshold values cannot exceed the set threshold values.</td>
</tr>
<tr>
<td>set</td>
<td>(Optional) Specifies the high threshold values for LCV and PCV that are used to signal a minor warning event on the link. When errors on the link are greater than or equal to these values, a minor warning occurs and a “crossed” event is signalled.</td>
</tr>
<tr>
<td>line-code-violation lcv-value</td>
<td>(Optional) Specifies the threshold value for LCV errors (Bi-Polar Violation [BPV] or Excessive Zeroes [EXZ]), in the following possible ranges:</td>
</tr>
<tr>
<td></td>
<td>- For T1 links, the range is 5 to 1544. The default is 154.</td>
</tr>
<tr>
<td></td>
<td>- For E1 links, the range is 7 to 2048. The default is 205.</td>
</tr>
<tr>
<td>path-code-violation pcv-value</td>
<td>(Optional) Specifies the threshold value for PCV errors (CRC errors), in the following possible ranges:</td>
</tr>
<tr>
<td></td>
<td>- For T1 links, the range is 3 to 320. The default is 145.</td>
</tr>
<tr>
<td></td>
<td>- For E1 links, the range is 5 to 832. The default is 205.</td>
</tr>
<tr>
<td>duration seconds</td>
<td>(Optional) Specifies the period of time (in seconds) during which the number of link noise errors must continuously exceed the set threshold levels to signal a minor warning, or remain below the clear threshold levels to signal a cleared event. The range is 4 to 600. The default is 10.</td>
</tr>
</tbody>
</table>

### Command Default

Link noise monitoring is disabled.

If the `lnm minor-warning` command is run without specifying `set` or `clear` options, then `set` is used as the default option with its default values. The `clear` option inherits the same threshold values as the default `set` threshold values.

If the `lnm minor-warning` command is run and only the `set` option is configured, the threshold values defined for the `set` option are also used as the `clear` threshold values. Alternatively, if the `lnm minor-warning` command is run and only the `clear` option is configured, the threshold values defined for the `clear` option are also used as the `set` threshold values.

### Command Modes

- T1 configuration
- E1 configuration
Command History

Release 4.0.0  This command was introduced.

Usage Guidelines

This command can only be configured on full T1 or E1 channel groups; it is not supported on fractional, or DS0 links.

The minor threshold values cannot be greater than the values configured in the `lnm major-warning` command.

LNM supports hierarchical level alarm reporting as defined in the Telcordia (Bellcore) GR-253 standard. Hierarchical alarm reporting means that whenever a higher alarm is asserted, the lower alarm state is suppressed. When the high alarm is cleared, the lower alarm will re-assert if the condition still exists.

For LNM, this means that if a major warning threshold is exceeded resulting in a crossed event and alarm state reached, then a minor warning alarm state is suppressed and placed in stable state. The minor crossed event also is removed from the bistate log. Only a single crossed event for major warnings will appear in the bistate log for the controller. When the major warning is cleared, the minor warning alarm is asserted if the condition still exists.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enable link noise monitoring on a T1 channel group using the default values for the set and clear threshold values of 154 LCVs and 145 PCVs for a duration of 10 seconds:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# lnm minor-warning
```

The following example shows how to specify set and clear thresholds on an E1 channel group:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/3/0/0/0/1
RP/0/RSP0/CPU0:router(config-e1)# lnm minor-warning set line-code-violation 200 path-code-violation 80 duration 30
RP/0/RSP0/CPU0:router(config-e1)# lnm minor-warning clear line-code-violation 150 path-code-violation 75 duration 30
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controller lnm, on page 817</td>
<td>Clears link noise monitoring statistics or resets states.</td>
</tr>
<tr>
<td>controller e1, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>controller t1, on page 832</td>
<td></td>
</tr>
<tr>
<td>lnm major-warning, on page 856</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal major warning events and recovery from those events.</td>
</tr>
</tbody>
</table>
## Command and Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lnm remove</code>, on page 862</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal the noise attribute to PPP for removal of an MLPPP bundle link.</td>
</tr>
<tr>
<td><code>lnm syslog</code>, on page 865</td>
<td>Enables logging of link noise monitoring major, remove, and minor events and alarms.</td>
</tr>
<tr>
<td><code>show controllers e1</code>, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td><code>show controllers lnm</code>, on page 884</td>
<td>Displays information about LNM on T1 or E1 links.</td>
</tr>
<tr>
<td><code>show controllers t1</code>, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
**Inm remove**

To enable link noise monitoring and specify thresholds for noise errors on T1/E1 links that are used to signal the noise attribute to the Point-to-Point Protocol (PPP) for removal of a Multilink PPP (MLPPP) bundle link, use the `lnm remove` command in T1 or E1 controller configuration mode. To disable link removal signaling based on LNM thresholds, use the `no` form of this command.

```
lnm remove [{clear | set} [line-code-violation lcv-value [path-code-violation pcv-value]] [duration seconds]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear</code></td>
<td>(Optional) Specifies threshold values for Line Code Violation (LCV) and Path Code Violation (PCV) errors that are used to determine when a recovery from a set threshold has occurred and a “cleared” event is signalled. The clear threshold values cannot exceed the set threshold values.</td>
</tr>
<tr>
<td><code>set</code></td>
<td>(Optional) Specifies the high threshold values for LCV and PCV that are used to signal the noise attribute to PPP on the link. When errors on the link are greater than or equal to these values, the noise attribute is set and a “crossed” event is signalled.</td>
</tr>
</tbody>
</table>
| `line-code-violation lcv-value` | (Optional) Specifies the threshold value for LCV errors (Bi-Polar Violation [BPV] or Excessive Zeroes [EXZ]), in the following possible ranges:  
  - For T1 links, the range is 5 to 1544. The default is 1544.  
  - For E1 links, the range is 7 to 2048. The default is 2048. |
| `path-code-violation pcv-value` | (Optional) Specifies the threshold value for PCV errors (CRC errors), in the following possible ranges:  
  - For T1 links, the range is 3 to 320. The default is 320.  
  - For E1 links, the range is 5 to 832. The default is 831. |
| `duration seconds` | (Optional) Specifies the period of time (in seconds) during which the number of link noise errors must continuously exceed the set threshold levels to signal the noise attribute, or remain below the clear threshold levels to signal a cleared event. The range is 4 to 600. The default is 10. |

**Command Default**

Link noise monitoring is disabled.

If the `lnm remove` command is run without specifying `set` or `clear` options, then `set` is used as the default option with its default values. The `clear` option inherits the same threshold values as the default `set` threshold values.

If the `lnm remove` command is run and only the `set` option is configured, the threshold values defined for the `set` option are also used as the `clear` threshold values. Alternatively, if the `lnm remove` command is run and only the `clear` option is configured, the threshold values defined for the `clear` option are also used as the `set` threshold values.

**Command Modes**

- T1 configuration
- E1 configuration
This command can only be configured on full T1 or E1 channel groups; it is not supported on fractional, or DS0 links.

The `lnm remove` command cannot be configured with the `lnm major-warning` command—they are mutually exclusive.

The remove threshold values must be greater than the values configured in the `lnm minor-warning` command.

LNM supports hierarchical level alarm reporting as defined in the Telcordia (Bellcore) GR-253 standard. Hierarchical alarm reporting means that whenever a higher alarm is asserted, the lower alarm state is suppressed. When the high alarm is cleared, the lower alarm will re-assert if the condition still exists.

For LNM, this means that if a remove threshold is exceeded resulting in a crossed event and alarm state reached, then a minor warning alarm state is suppressed and placed in stable state. The minor crossed event also is removed from the bistate log. Only a single crossed event for major warnings will appear in the bistate log for the controller. When the major warning is cleared, the minor warning alarm is asserted if the condition still exists.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable link noise monitoring to signal the noise attribute to PPP for link removal on a T1 channel group using the default values for the set and clear threshold values of 1544 LCVs and 320 PCVs for a duration of 10 seconds:

RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# lnm remove

The following example shows how to specify set and clear thresholds for link noise monitoring on an E1 channel group to signal the noise attribute to PPP for link removal:

RP/0/RSP0/CPU0:router(config)# controller e1 0/3/0/0/0/1
RP/0/RSP0/CPU0:router(config-e1)# lnm remove set line-code-violation 1500 path-code-violation 100 duration 30
RP/0/RSP0/CPU0:router(config-e1)# lnm remove clear line-code-violation 1400 path-code-violation 95 duration 30

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controller lnm, on page 817</td>
<td>Clears link noise monitoring statistics or resets states.</td>
</tr>
<tr>
<td>controller e1, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>controller t1, on page 832</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>lnm minor-warning, on page 859</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm syslog, on page 865</td>
<td>Enables logging of link noise monitoring major, remove, and minor events and alarms.</td>
</tr>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers lnm, on page 884</td>
<td>Displays information about LNM on T1 or E1 links.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
Inm syslog

To enable logging of link noise monitoring major, remove, and minor events and alarms, use the **lnm syslog** command in T1 or E1 controller configuration mode. To disable logging, use the **no** form of this command.

**lnm syslog**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Logging of link noise monitoring messages and events is disabled.

**Command Modes**

T1 configuration

E1 configuration

**Command History**

Release 4.0.0   This command was introduced.

**Usage Guidelines**

---

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling LNM syslog messages can produce large amounts of console messages. If you want to avoid this and disable the LNM syslog, you can use the <strong>show controllers lnm</strong> command to view the most recent event messages and current LNM states.</td>
</tr>
</tbody>
</table>

When you enable syslog messages for LNM events using the **lnm syslog** command, LNM messages will appear in both the system log and in the log events buffer. You can display LNM events in the log events buffer using the **show logging events buffer bistate-alarms-set** command, and also using the **show logging** command, which are described in the  *System Monitoring Command Reference for Cisco ASR 9000 Series Routers*

LNM supports hierarchical level alarm reporting as defined in the Telcordia (Bellcore) GR-253 standard. Hierarchical alarm reporting means that whenever a higher alarm is asserted, the lower alarm state is suppressed. When the high alarm is cleared, the lower alarm will re-assert if the condition still exists.

For LNM, this means that if a major warning threshold is continuously met or exceeded resulting in a crossed event and alarm state, then a minor warning alarm state is suppressed and returned to stable state. The minor crossed event also is removed from the bistate log. When the major warning is cleared, the minor warning alarm is asserted if the condition still exists.

Only a single crossed event for major warnings will appear in the bistate log for the controller. Therefore, you will see only a single log message for a controller if noise exists above configured threshold values.

**Examples**

The following example shows how to enable logging of link noise monitoring events:

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# lnm syslog

Wed May 12 15:42:54.679 PDT
WARNING: Enabling 'lnm syslog' could result in large amount of messages depending on the number of links configured.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller e1, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
<tr>
<td>controller t1, on page 832</td>
<td>Configures a T1 controller and enters T1 configuration mode.</td>
</tr>
<tr>
<td>lnm major-warning, on page 856</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal major warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm minor-warning, on page 859</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the contents of the logging buffer.</td>
</tr>
<tr>
<td>show logging events buffer</td>
<td>Displays messages in the logging events buffer.</td>
</tr>
</tbody>
</table>
loopback (T1/E1)

To loop individual T1 or E1 channels on the channelized T3 controller, use the `loopback` command in T1 or E1 configuration mode. To remove the loop, use the `no` form of this command.

```
loopback {local | network {line | payload} | remote {line {fdl {ansi | bellcore} | inband} | payload fdl ansi}}
```

**Syntax Description**

- **local**
  Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.

- **network {line | payload}**
  T1 loopback with encapsulation HDLC:
  Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload).

- **remote line fdl**
  (T1 only) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (0001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end, requesting that it enter into a network line loopback.

- **remote line inband**
  (T1 only) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.

- **remote payload fdl**
  (T1 only) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end, requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.

- **ansi**
  (T1 only) Enables the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, based on the ANSI T1.403 specification.

- **bellcore**
  (T1 only) Enables the remote SmartJack loopback on the T1 channel, based on the TR-TSY-000312 specification.

**Command Default**
No loops are configured.

**Command Modes**
- T1 configuration
- E1 configuration

**Command History**
- Release 3.9.0 This command was introduced.
- Release 4.0.0 Support for E1 configuration mode was added.
Usage Guidelines

Use the `loopback` command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the `show controllers t1` or `show controllers e1` command in EXEC mode.

For E1 lines, only the `local` and `network` options are valid. For T1 lines, all listed options are valid.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

This example shows how to configure the T1 for a local loopback:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1)# loopback local
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e1</code>, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td><code>show controllers t1</code>, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
loopback (T3/E3)

To loop the entire T3 or E3 line (all 28 T1 channels or all 21 E1 channels) on the T3 controller or E3 controller, use the `loopback` command in T3 or E3 configuration mode. To remove the loop, use the `no` form of this command.

```
loopback {local | {network | remote {line | payload}}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>local</th>
<th>Loops the data back toward the router and sends an alarm indication signal (AIS) out toward the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>network {line</td>
<td>payload}</td>
</tr>
<tr>
<td>remote {line</td>
<td>payload}</td>
</tr>
</tbody>
</table>

**Command Default**

No loops are configured on the T3 line.

**Command Modes**

T3 configuration

E3 configuration

**Command History**

Release 3.9.0  This command was introduced.

Release 4.0.0  Support for E3 configuration was added.

**Usage Guidelines**

Use the `loopback` command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the `show controllers t3` or `show controllers e3` command in EXEC mode. Note that remote loopback is valid only in C-bit parity mode.

You can also loopback each T1 or E1 channel by using the `loopback` command in T1 or E1 configuration mode.

**Examples**

This example shows how to configure the T3 for a local loopback:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/3/0/0
RP/0/RSP0/CPU0:router(config-t3)# loopback local
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e3</code>, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td><code>show controllers t3</code>, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification, use the `mdl` command in T3 configuration mode. To remove the message, use the `no` form of this command.

```
mdl string \{eic | fi | fic | gen-number | lic | port-number | unit\} string | transmit \{idle-signal | path | test-signal\} \{disable | enable\}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>string eic string</code></td>
<td>Specifies the Equipment Identification Code; can be up to 10 characters.</td>
</tr>
<tr>
<td><code>string fi string</code></td>
<td>Specifies the Facility Identification Code sent in the MDL Path message; can be up to 38 characters.</td>
</tr>
<tr>
<td><code>string fic string</code></td>
<td>Specifies the Frame Identification Code; can be up to 10 characters.</td>
</tr>
<tr>
<td><code>string gen-number string</code></td>
<td>Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.</td>
</tr>
<tr>
<td><code>string lic string</code></td>
<td>Specifies the Location Identification Code; can be up to 11 characters.</td>
</tr>
<tr>
<td><code>string port-number string</code></td>
<td>Specifies the Port number string sent in the MDL Idle Signal message; can be up to 10 characters.</td>
</tr>
<tr>
<td><code>string unit string</code></td>
<td>Specifies the Unit Identification Code; can be up to 6 characters.</td>
</tr>
<tr>
<td><code>transmit idle-signal</code></td>
<td>Specifies the transmission of the MDL Idle Signal message.</td>
</tr>
<tr>
<td><code>transmit path</code></td>
<td>Specifies the transmission of the MDL Path message.</td>
</tr>
<tr>
<td><code>transmit test-signal</code></td>
<td>Specifies the transmission of the MDL Test Signal message.</td>
</tr>
<tr>
<td>`disable</td>
<td>enable`</td>
</tr>
</tbody>
</table>

### Command Default
No MDL message is configured.

### Command Modes
T3 configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
Use the `show controllers t3` command to display MDL information (received strings). MDL information is displayed only when framing is set to C-bit.

### Note
MDL is supported only when the DS3 framing is C-bit parity.
The following example shows the `mdl` commands on a T3 controller in slot 1, subslot 2, port 0:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/1/2/0
RP/0/RSP0/CPU0:router(config-t3)# clock source line
RP/0/RSP0/CPU0:router(config-t3)# mdl string eic ID
RP/0/RSP0/CPU0:router(config-t3)# mdl string fic Building B
RP/0/RSP0/CPU0:router(config-t3)# mdl string unit ABC
RP/0/RSP0/CPU0:router(config-t3)# mdl string fi Facility Z
RP/0/RSP0/CPU0:router(config-t3)# mdl string port-number Port 7
RP/0/RSP0/CPU0:router(config-t3)# mdl transmit path enable
RP/0/RSP0/CPU0:router(config-t3)# mdl transmit idle-signal enable
```
**mode**

To set the mode of the T3/E3 or T1/E1 controller, use the **mode** command in T3, E3, T1, or E1 configuration mode. To disable the controller mode, use the **no** form of this command.

```
mode  {e1 | serial | t1}
```

**Syntax Description**

- **e1**  (T3 and E3 only) Specifies the mode of the port to be channelized E1.
- **serial**  (T3 and E3 only) Specifies the mode of the port to be clear channel serial. The default for the 2-Port and 4-Port Clear Channel T3/E3 SPAs is serial.
- **t1**  (T3 and E3 only) Specifies the mode of the port to be channelized T1.

**Command Default**

There is no default for the 2-Port Channelized OC-12/DS0 SPA.

**Command Modes**

- T3 configuration
- E3 configuration
- T1 configuration
- E1 configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 and E1 config modes was added.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

You can change the mode of a controller only when there are no subinterfaces defined for the controller. For example, if you previously defined channelized T1 subinterfaces on a T3 interface and now you want to change this to E1 subinterfaces or a clear channel interface, you must first clear the subinterfaces. To do this, use the **no controller t1** command for all defined T1/E1 subinterfaces. If you have defined serial parameters, you also need to use the **no interface serial** command.

For channelized SPAs, you must use the **mode** command before you can configure any channelized controllers.

**Task ID**

```
Task ID Operations
sonet-sdh  read, write
```

**Examples**

The following example shows how to change the mode of a T3 port to channelized T1:

```
RP/0/RSP0/CP00:router(config)# controller t3 0/6/0/0
RP/0/RSP0/CP00:router(config-t3)# mode t1
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td></td>
<td>show controllers e3, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td></td>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
<tr>
<td></td>
<td>show controllers t3, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
national bits (E1)

To specify the national reserved bits for an E1 port, use the `national bits` command in E1 configuration mode. To revert to the default national bits, use the `no` form of this command.

```
national bits bits
```

**Syntax Description**

- `bits`: Bit pattern. Values can be from 0 to 31. The default is 0.

**Command Default**

The default is 0, which corresponds to 0x1f.

**Command Modes**

- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `sonet-sdh` read, write

**Examples**

The following example shows how to specify the national bits for the E1 controller:

```
RP/0/RSP0/CPU0:router(config)# controller e1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# national bits 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e1</code>, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
</tbody>
</table>
national bits (E3)

To enable or disable the national reserved bit pattern on an E3 port, use the `national bits` command in E3 configuration mode. To revert to the default value, use the `no` form of this command.

```
national bits {disable | enable}
```

**Syntax Description**
- `disable` Disables national reserved bits for an E3 port.
- `enable` Enables national reserved bits for an E3 port. The default is `enable`.

**Command Default**
The default is `enable`.

**Command Modes**
E3 configuration

**Command History**
- **Release** 4.0.0  This command was introduced.

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Examples**
The following example shows how to enable the national bits for an E3 controller:

```
RP/0/RSP0/CPU0:router(config)# controller e3 0/6/2/0
RP/0/RSP0/CPU0:router(config-e3)# national bits enable
```

**Related Commands**
- `show controllers e3`, on page 880  Displays information about the E3 links and hardware and software drivers for the E3 controller.
show controllers e1

To display information about the E1 links and hardware and software drivers for the E1 controller, use the `show controllers e1` command in EXEC mode.

```
show controllers e1  interface-path-id  [{all | bert | brief | internal-state | tabular}]
```

**Syntax Description**

- `interface-path-id` Physical interface or virtual interface.

  **Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- `all` Displays all information for the controllers.

- `bert` Displays internal E1 bit error rate test results.

- `brief` Displays summary information for the E1 controller.

- `internal-state` Displays internal E1 state information.

- `tabular` Displays E1 controller information in tabular format.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.
The following example shows sample output from the `show controllers e1` command for a single E1 channel:

```
RP/0/RSP0/CPU0:router# show controllers e1 0/1/0/0

E1 0/1/0/0 is down
timeslots:
Receiver has no alarms.
Framing is E1 CRC, Clock Source is internal
Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
  0 Unavail Secs, 0 Stuffed Secs
  0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

### Table 58: show controllers e1 Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1 0/1/0/0 is down</td>
<td>E1 channel is not operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).</td>
</tr>
<tr>
<td>timeslots</td>
<td>DS0 time slots assigned to the E1 channel.</td>
</tr>
<tr>
<td>Receiver has no alarms</td>
<td>Any alarms detected by the E1 controller are displayed here. Possible alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>Framing</td>
<td>Framing type on the channelized controller.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Clock source controller. Values are internal and line.</td>
</tr>
<tr>
<td>Line Code Violations</td>
<td>Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.</td>
</tr>
<tr>
<td>P-bit Coding Violation</td>
<td>For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slip Secs</td>
<td>Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.</td>
</tr>
<tr>
<td>Fr Loss Secs</td>
<td>Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.</td>
</tr>
<tr>
<td>Line Err Secs</td>
<td>Line errored seconds (LES) is a second in which one or more line code violation errors are detected.</td>
</tr>
<tr>
<td>Degraded Mins</td>
<td>Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, <em>Definitions of Managed Objects for DS1 and E1 Interface Types</em>.</td>
</tr>
<tr>
<td>Errored Secs</td>
<td>Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.</td>
</tr>
<tr>
<td>Bursty Err Secs</td>
<td>Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.</td>
</tr>
<tr>
<td>Severely Err Secs</td>
<td>Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.</td>
</tr>
<tr>
<td>Unavailable Secs</td>
<td>Number of seconds during which the interface was not available in this interval, referred to as UAS.</td>
</tr>
<tr>
<td>Stuffed Secs</td>
<td>Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.</td>
</tr>
<tr>
<td>Near-end path failures</td>
<td>Path failure (PFC)</td>
</tr>
<tr>
<td>Far-end path failures</td>
<td>(PFCFE)</td>
</tr>
<tr>
<td>SEF/AIS Secs</td>
<td>(SAS)</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller e1, on page 828</td>
<td>Configures an E1 controller and enters E1 configuration mode.</td>
</tr>
</tbody>
</table>
show controllers e3

To display information about the E3 links and hardware and software drivers for the E3 controller, use the `show controllers e3` command in EXEC mode.

```
show controllers e3 interface-path-id [{all | bert | brief | internal-state | tabular}]
```

**Syntax Description**

- `interface-path-id` Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- `all` Displays all information for the controllers.
- `bert` Displays internal E3 bit error rate test results.
- `brief` Displays summary information for the E3 controller.
- `internal-state` Displays internal E3 state information.
- `tabular` Displays E3 controller information in tabular format.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 4.0.0    | This command was introduced on the .

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.
The following example shows sample output from the **show controllers e3** command for a single E3 port:

```
RP/0/RSP0/CPU0:router# show controllers e3 0/2/0/0

E3 0/2/0/0 is down
Transmitter is sending RAI.
Receiver has loss of frame.
Framing is G.751, Line Code is B3ZS, Clock Source is Internal
Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
Remote accept is enabled
Remote fullrate has no request outstanding
Data in current interval (360 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  360 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The following example shows sample output from the **show controllers e3** command using the **tabular** keyword, for a single E3 port:

```
RP/0/RSP0/CPU0:router# show controllers e3 0/2/0/0 tabular

E3 0/2/0/0 is down
Transmitter is sending RAI.
Receiver has loss of frame.
Framing is G.751, Line Code is B3ZS, Clock Source is Internal
Subrate is enabled. Mode: Cisco(default), Bandwidth: 34010 kbps
Remote accept is enabled
Remote fullrate has no request outstanding
INTERVAL | LCV | PCV | CCV | PES | PSES | SEFS | UAS | LES | CES | CSES
-----------|-----|-----|-----|-----|------|------|-----|-----|-----|------
07:49-07:56 | 0   | 0   | 0   | 0   | 0    | 0    | 380 | 0   | 0   | 0

Data in current interval (380 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  380 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```
### Table 59: show controllers e3 Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transmitter is sending RAI                | Any alarms detected by the controller are displayed here. Possible alarms are as follows:  
  - Transmitter is sending remote alarm.  
  - Transmitter is sending AIS.  
  - Receiver has loss of signal.  
  - Receiver is getting AIS.  
  - Receiver has loss of frame.  
  - Receiver has remote alarm.  
  - Receiver has no alarms. |
| Framing                                    | Framing type on the controller. Values are G.751 and G.832. |
| Line Code                                  | Line coding format on the controller. |
| Clock Source                               | Clock source on the channelized controller. Values are internal and line. |
| Data in current interval (seconds elapsed) | Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer. |
| Line Code Violations                       | Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string. |
| P-bit Coding Violation                     | For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code. |
| C-bit Coding Violation                     | For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval. |
| P-bit Err Secs                             | P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted. |
| P-bit Severely Err Secs                    | P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted. |
| Severely Err Framing Secs                  | Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS. |
The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, *DS3 MIB Variables*.

Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.

C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

Shows the last 15-minute accumulation period.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unavailable Secs</td>
<td>The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, <em>DS3 MIB Variables</em>.</td>
</tr>
<tr>
<td>Line Errored Secs</td>
<td>Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.</td>
</tr>
<tr>
<td>C-bit Errored Secs</td>
<td>C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.</td>
</tr>
<tr>
<td>C-bit Severely Errored Secs</td>
<td>C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.</td>
</tr>
<tr>
<td>Total Data (last 24 hours)</td>
<td>Shows the last 15-minute accumulation period.</td>
</tr>
</tbody>
</table>

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller e3, on page 830</td>
<td>Configures an E3 controller and enters E3 configuration mode.</td>
</tr>
</tbody>
</table>
show controllers lnm

To display information about link noise monitoring (LNM) on T1 or E1 links, use the `show controllers lnm` command in EXEC mode.

```
show controllers {t1 | e1} interface-path-id lnm [{all | configuration | event | statistics}]
```

**Syntax Description**

- **t1**
  Displays LNM information for a T1 controller.

- **e1**
  Displays LNM information for an E1 controller.

- **interface-path-id**
  Physical interface or virtual interface.

  **Note**
  Use the `show controllers` command to see a list of all controllers currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **all**
  (Optional) Displays LNM configuration, state, statistics, and event information.

- **configuration**
  (Optional) Displays LNM configuration and state information. This is the default.

- **event**
  (Optional) Displays LNM statistics.

- **statistics**
  (Optional) Displays LNM statistics.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

Release 4.0.0  This command was introduced.

**Usage Guidelines**

When specifying a channelized T1 controller, use the following guidelines for the `interface-path-id`:

- The naming notation is `rack/slot/module/port/T3Num/T1Num`.

- The slash between values is required as part of the notation.

- The following list describes the components of the notation:
  - **rack**—Chassis number of the rack.
  - **slot**—Physical slot number of the line card.
  - **module**—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - **port**—Physical port number of the interface.
  - **T3num**—T3 controller number.
• T1num—T1 controller number.

### Examples

The following example shows sample output from the `show controllers t1 lnm` command with the `all` keyword for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/1/0/1/1 lnm all
Thu May 13 10:28:26.474 PDT
Controller T1 0/1/0/1/1

Syslog Monitoring type State Thresholds (lcv/pcv/duration)
--------------------------------------------------------------------
| enabled | minor-warning | stable | Set( 15/ 15/ 4) Clear( 15/ 15/ 4) |
| major-warning | stable | Set( 154/ 145/ 4) Clear( 154/ 145/ 4) |

Monitoring type Minor-Warn Major-Warn
--------------- ---------------
Create 1 1
Update 0 0
Delete 0 0
Clear 0 0
Noise Crossed 1 1
Noise Cleared 1 1

Last Five Events
--------------------------------------------------------------------
MINWARNCROSS: Noise crossed minor-warn threshold at Thu May 13 09:54:10 2010
MAJWARNCROSS: Noise crossed major-warn threshold at Thu May 13 09:54:11 2010
MAJWARNCLEAR: Noise cleared major-warn threshold at Thu May 13 10:27:25 2010
MINWARNCLEAR: Noise cleared minor-warn threshold at Thu May 13 10:28:14 2010
```

The following example shows sample output from the `show controllers t1 lnm` command with the `configuration` keyword for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/1/0/1/1 lnm configuration
Thu May 13 10:28:26.474 PDT
Controller T1 0/1/0/1/1

Syslog Monitoring type State Thresholds (lcv/pcv/duration)
--------------------------------------------------------------------
| enabled | minor-warning | stable | Set( 15/ 15/ 4) Clear( 15/ 15/ 4) |
| major-warning | stable | Set( 154/ 145/ 4) Clear( 154/ 145/ 4) |
```

This is also the default output that is displayed if you run the `show controllers lnm` command without specifying any keyword options.
The following example shows sample output from the `show controllers t1 lnm` command with the `event` keyword for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/1/1/0/1/1 lnm event
Thu May 13 10:28:26.474 PDT
Controller T1 0/1/1/0/1/1
Last Five Events
--------------------------------------------------------------------
MINWARNCROSS: Noise crossed minor-warn threshold at Thu May 13 09:54:10 2010
MAJWARNCROSS: Noise crossed major-warn threshold at Thu May 13 09:54:11 2010
MAJWARNCLEAR: Noise cleared major-warn threshold at Thu May 13 10:27:25 2010
MINWARNCLEAR: Noise cleared minor-warn threshold at Thu May 13 10:28:14 2010
```

The following example shows sample output from the `show controllers t1 lnm` command with the `statistics` keyword for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/1/1/0/1/1 lnm statistics
Thu May 13 10:28:26.474 PDT
Controller T1 0/1/1/0/1/1

<table>
<thead>
<tr>
<th>Monitoring type</th>
<th>Minor-Warn</th>
<th>Major-Warn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Update</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Delete</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Noise Crossed</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Noise Cleared</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controller lnm, on page 817</td>
<td>Clears link noise monitoring states or statistics.</td>
</tr>
<tr>
<td>lnm major-warning, on page 856</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal major warning events and recovery from those events.</td>
</tr>
<tr>
<td>lnm minor-warning, on page 859</td>
<td>Enables link noise monitoring and specifies thresholds for noise errors on T1/E1 links that are used to signal minor warning events and recovery from those events.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the contents of the logging buffer.</td>
</tr>
<tr>
<td>show logging events buffer</td>
<td>Displays messages in the logging events buffer.</td>
</tr>
</tbody>
</table>
show controllers t1

To display information about the T1 links and hardware and software drivers for the T1 controller, use the `show controllers t1` command in EXEC mode.

```
show controllers t1 interface-path-id { all | bert | brief | internal-state | remote { performance brief | tabular } | tabular }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark ( ? ) online help function.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all information for the controllers.</td>
</tr>
<tr>
<td>bert</td>
<td>Displays internal T1 bit error rate test results.</td>
</tr>
<tr>
<td>brief</td>
<td>Displays summary information for the T1 controller.</td>
</tr>
<tr>
<td>internal-state</td>
<td>Displays internal T1 state information.</td>
</tr>
<tr>
<td>remote { performance brief</td>
<td>tabular }</td>
</tr>
<tr>
<td>tabular</td>
<td>Displays T1 controller information in table format.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When specifying a channelized T1 controller, use the following guidelines for the `interface-path-id`:

- The naming notation is `rack/slot/module/port/T3Num/T1num`.
- The slash between values is required as part of the notation.
- The following list describes the components of the notation:
  - `rack`—Chassis number of the rack.
  - `slot`—Physical slot number of the line card.
  - `module`—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - `port`—Physical port number of the interface.
- **T3num**—T3 controller number.
- **T1num**—T1 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.
- When specifying a virtual tributary group, the naming notation is `rack/slot/module/port/vtg/vt`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**—Chassis number of the rack.
  - **slot**—Physical slot number of the line card.
  - **module**—Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - **port**—Physical port number of the interface.
  - **vtg**—Virtual tributary group.
  - **vt**—Virtual tributary instance.

### Examples

The following example shows sample output from the `show controllers t1` command with the `brief` keyword for a single T1 channel:

```bash
RP/0/RSP0/CPU0:router# show controllers t1 0/4/2/0/1 brief

T1 0/4/2/0/1 is up
mode: ATM
timeslots: 1-24
FDL per AT&T 54016 spec.
Receiver has no alarms.
Framing is ESF, Line Code is B8ZS, Clock Source is internal
Alarm Soaking Interval:
  Alarm Declaring= 2500 msec
  Alarm clearing = 10000 msec

Bert Test on controller port : T1 0/4/2/0/1
BERT test result (not running)
  Test Pattern : Not Configured, Status : not running, Sync Detected : 0
  Interval : 1 minute(s), Time Remain : 0 (ms)
  Bit Errors (since BERT started): 0 bits,
  Bits Received (since BERT started): 0 Kbits
  Bit Errors (since last sync): 0 bits
  Bits Received (since last sync): 0 Kbits
```
### Table 60: show controllers t1 brief Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1 0/4/2/0/1 is up</td>
<td>T1 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).</td>
</tr>
<tr>
<td>mode</td>
<td>Mode of the T1 controller, which can be ATM.</td>
</tr>
<tr>
<td>timeslots</td>
<td>DS0 time slots assigned to the T1 channel.</td>
</tr>
<tr>
<td>FDL per spec-name spec.</td>
<td>Performance monitoring is through Facility Data Link based on ANSI T1.403 specification or AT&amp;T standard specification number 54016.</td>
</tr>
<tr>
<td>Receiver has no alarms.</td>
<td>Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>Framing</td>
<td>Framing type on the channelized controller. Values are ESF and SF.</td>
</tr>
<tr>
<td>Line Code</td>
<td>Line coding format on the channelized controller. Values are AMI or B8ZS.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Clock source on the T1 channel. Values are internal and line.</td>
</tr>
<tr>
<td>Alarm Soaking Interval</td>
<td>Values of the following alarm soaking intervals:</td>
</tr>
<tr>
<td></td>
<td>• Alarm declarings: amount of time, in milliseconds, after which an alarm is declared.</td>
</tr>
<tr>
<td></td>
<td>• Alarm clearing: amount of time, in milliseconds, after which an alarm is cleared.</td>
</tr>
<tr>
<td>Bert Test on controller port</td>
<td>Indicates controller port on which BERT test can be run.</td>
</tr>
<tr>
<td>BERT test result</td>
<td>Indicates the current state of the test. Can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• running—BER test is still in progress.</td>
</tr>
<tr>
<td></td>
<td>• done—BER test is complete.</td>
</tr>
<tr>
<td></td>
<td>• not running—BER test is not running on the controller.</td>
</tr>
<tr>
<td>Test Pattern</td>
<td>Indicates the test pattern you selected for the test.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the current synchronization state (sync).</td>
</tr>
<tr>
<td>Sync Detected</td>
<td>Indicates the number of times synchronization has been detected during this test.</td>
</tr>
<tr>
<td>Interval</td>
<td>Indicates the length of the test.</td>
</tr>
</tbody>
</table>
Indicates the time remaining for the test to run.

Note: If you terminate a BER test, you receive a message similar to the following: Time Remain: 2 minute(s) (unable to complete) "(Unable to complete)" signifies that you interrupted the test.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Remain</td>
<td>Indicates the time remaining for the test to run.</td>
</tr>
<tr>
<td>Bit Errors (since BERT started)</td>
<td>Bit errors that have been detected since the test started.</td>
</tr>
<tr>
<td>Bits Received (since BERT started)</td>
<td>Total number of test bits that have been received since the test started.</td>
</tr>
<tr>
<td>Bit Errors (since last sync)</td>
<td>Bit errors that have been detected since the synchronization started.</td>
</tr>
<tr>
<td>Bits Received (since last sync)</td>
<td>Total number of test bits that have been received since the synchronization started.</td>
</tr>
</tbody>
</table>

The following example shows sample output from the `show controllers t1` command for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/4/2/0/1

T1 0/4/2/0/1 is up
  mode: ATM
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  Receiver has no alarms.
  Framing is ESF, Line Code is B8ZS, Clock Source is internal
  Data in current interval (38 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    0 Unavail Secs, 0 Stuffed Secs
    0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Data in Interval 1:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    0 Unavail Secs, 0 Stuffed Secs
    0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Data in Interval 2:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    0 Unavail Secs, 0 Stuffed Secs
    0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
.  
```

The following example shows sample output from the `show controllers t1` command with the `tabular` keyword for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/4/2/0/1 tabular

T1 0/4/2/0/1 is up
  mode: ATM
```

The following example shows sample output from the `show controllers t1` command for a single T1 channel:

```
RP/0/RSP0/CPU0:router# show controllers t1 0/4/2/0/1

T1 0/4/2/0/1 is up
  mode: ATM
```
timeslots: 1-24
FDL per AT&T 54016 spec.
Receiver has no alarms.
Framing is ESF, Line Code is B8ZS, Clock Source is internal

<table>
<thead>
<tr>
<th>INTERVAL</th>
<th>LCS</th>
<th>CCS</th>
<th>EFS</th>
<th>LSS</th>
<th>DM</th>
<th>ES</th>
<th>BES</th>
<th>SES</th>
<th>UAS</th>
<th>SSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30-08:35</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>08:15-08:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>08:00-08:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>07:45-08:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>07:30-07:45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>07:15-07:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>07:00-07:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>06:45-07:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>06:30-06:45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>06:15-06:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>06:00-06:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>05:45-06:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>05:30-05:45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>05:15-05:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 61: `show controllers t1` and `show controllers t1` tabular Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1 0/4/2/0/1 is up</td>
<td>T1 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Loopied) or (Remotely Loopied).</td>
</tr>
<tr>
<td>mode</td>
<td>Mode of the T1 controller, which can be ATM.</td>
</tr>
<tr>
<td>timeslots</td>
<td>DS0 time slots assigned to the T1 channel.</td>
</tr>
<tr>
<td>FDL per <code>spec-name</code> spec.</td>
<td>Performance monitoring is through Facility Data Link based on ANSI T1.403 specification or AT&amp;T standard specification number 54016.</td>
</tr>
<tr>
<td>Receiver has no alarms.</td>
<td>Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>Framing</td>
<td>Framing type on the channelized controller. Values are ESF and SF.</td>
</tr>
<tr>
<td>Line Code</td>
<td>Line coding format on the channelized controller. Values are AMI or B8ZS.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Clock source on the T1 channel. Values are internal and line.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data in current interval (seconds elapsed)</td>
<td>Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.</td>
</tr>
<tr>
<td>Line Code Violations</td>
<td>Line CodeViolations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.</td>
</tr>
<tr>
<td>Slip Secs</td>
<td>Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.</td>
</tr>
<tr>
<td>Fr Loss Secs</td>
<td>Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.</td>
</tr>
<tr>
<td>Line Err Secs</td>
<td>Line errored seconds (LES) is a second in which one or more line code violation errors are detected.</td>
</tr>
<tr>
<td>Degraded Mins</td>
<td>Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, see RFC 1406, <em>Definitions of Managed Objects for DS1 and E1 Interface Types</em>.</td>
</tr>
<tr>
<td>Errored Secs</td>
<td>Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.</td>
</tr>
<tr>
<td>Bursty Err Secs</td>
<td>Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.</td>
</tr>
<tr>
<td>Severely Err Secs</td>
<td>Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.</td>
</tr>
<tr>
<td>Unavailable Secs</td>
<td>Number of seconds during which the interface was not available in this interval, referred to as UAS.</td>
</tr>
<tr>
<td>Stuffed Secs</td>
<td>Stuffed seconds (SSS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.</td>
</tr>
<tr>
<td>Near-end path failures</td>
<td>Total number of near-end path failures.</td>
</tr>
<tr>
<td>Far-end path failures</td>
<td>Total number of far-end path failures.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SEF/AIS Secs</td>
<td>Total number of Severely Errored Framing (SEF) and Alarm Indication Signal (AIS) errors.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller t1, on page 832</td>
<td></td>
</tr>
</tbody>
</table>
show controllers t3

To display information about the T3 links and hardware and software drivers for the T3 controller, use the **show controllers t3** command in EXEC mode.

```
show controllers t3 interface-path-id [{all | bert | brief | internal-state | tabular}]
```

**Syntax Description**
- **interface-path-id**: Physical interface or virtual interface.

  **Note**: Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

  **all**: Displays all information for the controllers.

  **bert**: Displays internal T3 bit error rate test results.

  **brief**: Displays summary information for the controller.

  **internal-state**: Displays internal T3 state information.

  **tabular**: Displays T3 controller information in tabular format.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- **Release 3.9.0**: This command was introduced.

**Usage Guidelines**
For the **interface-path-id** argument, use the following guidelines:

- When specifying a T3 controller, the naming notation is `rack/slot/module/port/T3num`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - **rack**: Chassis number of the rack.
  - **slot**: Physical slot number of the line card or SIP.
  - **module**: Module number or subslot (for a SPA). A physical layer interface module (PLIM) is always 0.
  - **port**: Physical port number of the interface.
  - **T3num**: T3 controller number.

- If specifying a virtual interface, the number range varies, depending on interface type.
The following example shows sample output from the `show controllers t3` command using the `brief` keyword for a single T3 port:

```
RP/0/RSP0/CPU0:router# show controllers t3 0/4/2/0/1 brief
T3 0/4/2/0 is up
No alarms detected.
mode: serial
MDL transmission is disabled
    EIC: , LIC: , FIC: , UNIT:
    Path FI:
    Idle Signal PORT_NO:
    Test Signal GEN_NO:
FEC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Alarm Soaking Interval:
    Alarm Declaring= 2500 msec
    Alarm clearing = 10000 msec
BERT test result (not running)
    Test Pattern : Not Configured, Status : not running, Sync Detected : 0
    Interval : 1 minute(s), Time Remain : 0 (ms)
    Bit Errors (since BERT started): 0 bits,
    Bits Received (since BERT started): 0 Kbits
    Bit Errors (since last sync): 0 bits
    Bits Received (since last sync): 0 Kbits
```

### Table 62: `show controllers t3 brief` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3 0/4/2/0/1 is up</td>
<td>T3 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).</td>
</tr>
<tr>
<td>No alarms detected</td>
<td>Any alarms detected by the controller are displayed here. Possible alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>mode</td>
<td>Mode of the T3 controller, which can be ATM, serial, or T1 serial or T1.</td>
</tr>
<tr>
<td>MDL transmission</td>
<td>Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EIC</td>
<td>Equipment Identification Code.</td>
</tr>
<tr>
<td>LIC</td>
<td>Location Identification Code.</td>
</tr>
<tr>
<td>FIC</td>
<td>Frame Identification Code.</td>
</tr>
<tr>
<td>UNIT</td>
<td>Unit Identification Code.</td>
</tr>
<tr>
<td>Path FI</td>
<td>Path facility identifier.</td>
</tr>
<tr>
<td>Idle Signal PORT_NO</td>
<td>Identifies the port that initiates the idle signal message.</td>
</tr>
<tr>
<td>Test Signal GEN_NO</td>
<td>Generator number to send in test signal messages.</td>
</tr>
<tr>
<td>FEAC code received</td>
<td>Whether or not a far-end alarm code request is being received. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• DS3 Eqpt. Failure (SA)</td>
</tr>
<tr>
<td></td>
<td>• DS3 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS3 Out-of-Frame</td>
</tr>
<tr>
<td></td>
<td>• DS3 AIS Received</td>
</tr>
<tr>
<td></td>
<td>• DS3 IDLE Received</td>
</tr>
<tr>
<td></td>
<td>• DS3 Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• Common Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• Multiple DS1 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS1 Eqpt. Failure</td>
</tr>
<tr>
<td></td>
<td>• Single DS1 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS1 Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• No code is being received</td>
</tr>
<tr>
<td>Framing</td>
<td>Framing type on the channelized controller. Values are auto-detect, M23,</td>
</tr>
<tr>
<td></td>
<td>and C-Bit.</td>
</tr>
<tr>
<td>Line Code</td>
<td>Line coding format on the channelized controller. Values are AMI and B8ZS.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Clock source on the channelized controller. Values are internal and line.</td>
</tr>
<tr>
<td>Alarm Soaking Interval</td>
<td>Values of the following alarm soaking intervals:</td>
</tr>
<tr>
<td></td>
<td>• Alarm declarings: amount of time, in milliseconds, after which an alarm</td>
</tr>
<tr>
<td></td>
<td>is declared.</td>
</tr>
<tr>
<td></td>
<td>• Alarm clearing: amount of time, in milliseconds, after which an alarm</td>
</tr>
<tr>
<td></td>
<td>is cleared.</td>
</tr>
<tr>
<td>BERT test result</td>
<td>Indicates the current state of the test. Can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• running—BER test is still in progress.</td>
</tr>
<tr>
<td></td>
<td>• done—BER test is complete.</td>
</tr>
<tr>
<td></td>
<td>• not running—BER test is not running on the controller.</td>
</tr>
<tr>
<td>Test Pattern</td>
<td>Indicates the test pattern you selected for the test.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the current synchronization state (sync).</td>
</tr>
<tr>
<td>Sync Detected</td>
<td>Indicates the number of times synchronization has been detected during this test.</td>
</tr>
<tr>
<td>Interval</td>
<td>Indicates the length of the test.</td>
</tr>
<tr>
<td>Time Remain</td>
<td>Indicates the time remaining for the test to run.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you terminate a BER test, you receive a message similar to the following: Time Remain: 2 minute(s) (unable to complete) &quot;(Unable to complete)&quot; signifies that you interrupted the test.</td>
</tr>
<tr>
<td>Bit Errors (since BERT started)</td>
<td>Bit errors that have been detected since the test started.</td>
</tr>
<tr>
<td>Bits Received (since BERT started)</td>
<td>Total number of test bits that have been received since the test started.</td>
</tr>
<tr>
<td>Bit Errors (since last sync)</td>
<td>Bit errors that have been detected since the synchronization started.</td>
</tr>
<tr>
<td>Bits Received (since last sync)</td>
<td>Total number of test bits that have been received since the synchronization started.</td>
</tr>
</tbody>
</table>

The following example shows sample output from the `show controllers t3` command using the `tabular` keyword, for a single T3 port:

```
RP/0/RSP0/CPU0:router# show controllers t3 0/4/2/0/1 tabular
T3 0/4/2/0/1 is up
INTERVAL LCV PCV CCV PES PSES SEFS UAS LES CES CSES
09:00-09:02  0  0  0  0  0  0  0  0  0  0  0 0
08:45-09:00  0  0  0  0  0  0  0  0  0  0  0 0
08:30-08:45  0  0  0  0  0  0  0  0  0  0  0 0
08:15-08:30  0  0  0  0  0  0  0  0  0  0  0 0
08:00-08:15  0  0  0  0  0  0  0  0  0  0  0 0
07:45-08:00  0  0  0  0  0  0  0  0  0  0  0 0
07:30-07:45  0  0  0  0  0  0  0  0  0  0  0 0
.
.
.
```

The following example shows sample output from the `show controllers t3` command for a single T3 port:

```
RP/0/RSP0/CPU0:router# show controllers t3 0/4/2/0/1
T3 0/4/2/0/1 is up
No alarms detected.
mode: serial
MDL transmission is disabled
  EIC: , LIC: , FIC: , UNIT:
  Path FI:
  Idle Signal PORT_NO:
```
Test Signal GEN_NO:
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Data in current interval (695 seconds elapsed):
  0 C-bit Coding Violation, 0 P-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Severely Err Secs
  0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Data in Interval 1:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Data in Interval 2:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Data in Interval 3:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs

Table 63: show controllers t3 and show controllers t3 tabular Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3 0/4/2/0/1 is up</td>
<td>T3 channel is operating. The channel state can be up, down, or administratively down. Loopback conditions are shown by (Locally Loopied) or (Remotely Loopied).</td>
</tr>
<tr>
<td>No alarms detected</td>
<td>Any alarms detected by the controller are displayed here. Possible alarms are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Transmitter is sending AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of signal.</td>
</tr>
<tr>
<td></td>
<td>• Receiver is getting AIS.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has loss of frame.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has remote alarm.</td>
</tr>
<tr>
<td></td>
<td>• Receiver has no alarms.</td>
</tr>
<tr>
<td>mode</td>
<td>Mode of the T3 controller, which can be ATM, serial, T1, or E1 serial or T1 ATM or serial.</td>
</tr>
<tr>
<td>MDL transmission</td>
<td>Status of the Maintenance Data Link (either enabled or disabled) and the values of the MDL message fields.</td>
</tr>
<tr>
<td>EIC</td>
<td>Equipment Identification code.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LIC</td>
<td>Location Identification code.</td>
</tr>
<tr>
<td>FIC</td>
<td>Frame Identification code.</td>
</tr>
<tr>
<td>UNIT</td>
<td>Unit Identification code.</td>
</tr>
<tr>
<td>Path FI</td>
<td>Path facility identifier.</td>
</tr>
<tr>
<td>Idle Signal PORT_NO</td>
<td>Identifies the port that initiates the idle signal message.</td>
</tr>
<tr>
<td>Test Signal GEN_NO</td>
<td>Generator number to send in test signal messages.</td>
</tr>
<tr>
<td>FEAC code received</td>
<td>Whether or not a far-end alarm code request is being received. Possible values</td>
</tr>
<tr>
<td></td>
<td>are as follows:</td>
</tr>
<tr>
<td></td>
<td>• DS3 Eqpt. Failure (SA)</td>
</tr>
<tr>
<td></td>
<td>• DS3 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS3 Out-of-Frame</td>
</tr>
<tr>
<td></td>
<td>• DS3 AIS Received</td>
</tr>
<tr>
<td></td>
<td>• DS3 IDLE Received</td>
</tr>
<tr>
<td></td>
<td>• DS3 Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• Common Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• Multiple DS1 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS1 Eqpt. Failure</td>
</tr>
<tr>
<td></td>
<td>• Single DS1 LOS/HBER</td>
</tr>
<tr>
<td></td>
<td>• DS1 Eqpt. Failure (NSA)</td>
</tr>
<tr>
<td></td>
<td>• No code is being received</td>
</tr>
<tr>
<td>Framing</td>
<td>Framing type on the channelized controller. Values are M23 and C-Bit.</td>
</tr>
<tr>
<td>Line Code</td>
<td>Line coding format on the channelized controller. Values are AMI and B8ZS.</td>
</tr>
<tr>
<td>Clock Source</td>
<td>Clock source on the channelized controller. Values are internal and line.</td>
</tr>
<tr>
<td>Data in current interval</td>
<td>Shows the current accumulation period, which rolls into the 24-hour accumulation</td>
</tr>
<tr>
<td>(seconds elapsed)</td>
<td>every 15 minutes. The accumulation period is from 1 to 900 seconds. The oldest</td>
</tr>
<tr>
<td></td>
<td>15-minute period falls off the back of the 24-hour accumulation buffer.</td>
</tr>
<tr>
<td>Line Code Violations</td>
<td>Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and</td>
</tr>
<tr>
<td></td>
<td>Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments</td>
</tr>
<tr>
<td></td>
<td>the LCV by one regardless of the length of the zero string.</td>
</tr>
<tr>
<td>P-bit Coding Violation</td>
<td>For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit</td>
</tr>
<tr>
<td></td>
<td>parity error event. A P-bit parity error event is the occurrence of a received P-</td>
</tr>
<tr>
<td></td>
<td>bit code on the DS3 M-frame that is not identical to the corresponding locally</td>
</tr>
<tr>
<td></td>
<td>calculated code.</td>
</tr>
</tbody>
</table>

**T3, E3, T1, E1 Controller Commands on the Cisco ASR 9000 Series Router**

**Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers**
For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.

P-bit Err Secs

P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.

P-bit Severely Err Secs

P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.

Severely Err Framing Secs

Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.

Unavailable Secs

The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, DS3 MIB Variables.

Line Errored Secs

Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.

C-bit Errored Secs

C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

C-bit Severely Errored Secs

C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-bit Coding Violation</td>
<td>For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported by the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.</td>
</tr>
<tr>
<td>P-bit Err Secs</td>
<td>P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.</td>
</tr>
<tr>
<td>P-bit Severely Err Secs</td>
<td>P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge does not increment when unavailable seconds are counted.</td>
</tr>
<tr>
<td>Severely Err Framing Secs</td>
<td>Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.</td>
</tr>
<tr>
<td>Unavailable Secs</td>
<td>The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, see RFC 1407, DS3 MIB Variables.</td>
</tr>
<tr>
<td>Line Errored Secs</td>
<td>Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.</td>
</tr>
<tr>
<td>C-bit Errored Secs</td>
<td>C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.</td>
</tr>
<tr>
<td>C-bit Severely Errored Secs</td>
<td>C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller t3, on page 834</td>
<td>Configures a T3 controller and enters T3 configuration mode.</td>
</tr>
</tbody>
</table>
shutdown (T1/E1)

To disable the T1 or E1 controller, use the `shutdown` command in T1 or E1 configuration mode. To restart a disabled T1 or E1 controller, use the `no` form of this command.

```
shutdown
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

- T1 configuration
- E1 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E1 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Shutting down the T1 or E1 controller disables all functions on the interface and sends an AIS alarm to the network. The `shutdown` command marks the interface as unavailable. To check if the controller is disabled, use the `show controllers t1` or `show controllers e1` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to bring up a controller that was previously shut down:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# no shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers e1, on page 877</td>
<td>Displays information about the E1 links and hardware and software drivers for the E1 controller.</td>
</tr>
<tr>
<td>show controllers t1, on page 887</td>
<td>Displays information about the T1 links and hardware and software drivers for the T1 controller.</td>
</tr>
</tbody>
</table>
shutdown (T3/E3)

To disable a T3 or E3 controller, use the `shutdown` command in T3 or E3 configuration mode. To restart a disabled T3 or E3 controller, use the `no` form of this command.

**shutdown**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
T3 configuration

E3 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>Support for E3 configuration mode was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Shutting down the T3 or E3 controller disables all functions on the interface and sends an AIS alarm to the network. The `shutdown` command marks the interface as unavailable. To check if the controller is disabled, use the `show controllers t3` or `show controllers e3` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to bring up a controller that was previously shut down:

```
RP/0/RSP0/CPU0:router(config)# controller t3 0/6/0/0
RP/0/RSP0/CPU0:router(config-t3)# no shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers e3</code>, on page 880</td>
<td>Displays information about the E3 links and hardware and software drivers for the E3 controller.</td>
</tr>
<tr>
<td><code>show controllers t3</code>, on page 894</td>
<td>Displays information about the T3 links and hardware and software drivers for the T3 controller.</td>
</tr>
</tbody>
</table>
speed (DS0)

To specify the speed of the underlying DS0s in a channel group, use the `speed` command in channel group configuration mode. To revert to the default speed, use the `no` form of this command.

```plaintext
Note
This command is not applicable for E1 controllers.
```

```plaintext
speed  kbps
```

**Syntax Description**

- `kbps`  Speed of the underlying DS0s in kilobits per second (kbps). Valid values are 56 and 64. The default is 64 kbps.

**Command Default**

The default speed is 64 kbps.

**Command Modes**

Channel group configuration for T1

**Command History**

- **Release** 3.9.0  This command was introduced.

**Usage Guidelines**

Before the channel group configuration is valid, you must define the associated DS0 time slots using the `timeslots` command.

**Task ID**

- **Task ID**  `sonet-sdh`
  - **Operations**  `read`, `write`

**Examples**

The following example shows how to define the speed for the underlying DS0 to be 56 kbps:

```plaintext
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# channel-group 5
RP/0/RSP0/CPU0:router(config-t1e1-channel_group)# speed 56
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeslots</code>, on page 904</td>
<td>Associates one or more DS0 time slots to a channel group and create an associated serial subinterface.</td>
</tr>
<tr>
<td><code>channel-group</code>, on page 815</td>
<td>Configures a DS0 channel group and enters channel group configuration mode.</td>
</tr>
</tbody>
</table>
timeslots

To associate one or more DS0 time slots to a channel group and create an associated serial subinterface, use the `timeslots` command in channel group configuration mode. To unassign the DS0 time slots and delete the associated serial interface, use the `no` form of this command.

```
timeslots  range
```

**Syntax Description**

```
range
```

**Command Default**

No default behavior or values

**Command Modes**

Channel group configuration for T1 and E1

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The time slot range must match the DS0 time slots assigned to the channel group. The service provider defines the DS0 time slots that compose a channel group.

Before the channel group configuration is valid, you must define the associated DS0 time slots using the `timeslots` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet-sdh</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to associate DS0 time slots 1, 6, 8, 9 and 10 to channel group 5:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# channel-group 5
RP/0/RSP0/CPU0:router(config-t1e1-channel_group)# timeslots 1:6:8-10
```

The following example shows configuration of the full 24 timeslots on the 2-Port Channelized OC-12/DS0 SPA, which is required when configuring link noise monitoring:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# channel-group 5
RP/0/RSP0/CPU0:router(config-t1e1-channel_group)# timeslots 1-24
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>framing (E1), on page 850</td>
<td>Selects the frame type for an E1 data line.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>framing (T1), on page 852</td>
<td>Selects the frame type for a T1 data line.</td>
</tr>
<tr>
<td>speed (DS0), on page 903</td>
<td>Specifies the speed of the underlying DS0s in a channel group.</td>
</tr>
<tr>
<td>channel-group, on page 815</td>
<td>Configures a DS0 channel group and enters channel group configuration mode.</td>
</tr>
</tbody>
</table>
yellow

To enable detection and generation of T1 yellow alarms, use the `yellow` command in T1 configuration mode. To disable detection and generation of T1 yellow alarms, use the `no` form of this command.

```
yellow {detection | generation} {disable | enable}
```

**Syntax Description**
- `detection` Detects yellow alarms.
- `generation` Generates yellow alarms.
- `disable` Disables detection or generation of T1 yellow alarms.
- `enable` Enables detection or generation of T1 yellow alarms. The default is `enable`.

**Command Default**
Yellow alarms are detected and generated on the T1 channel.

**Command Modes**
- `T1 configuration`

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection as the yellow alarm can be incorrectly detected with SF framing.

Serial interface may flap and eventually, go down if yellow alarm detection is not disabled on its T1 controller configured with SF framing.

The default state of the `yellow` command is enabled. If you disable yellow alarm detection and want to reenable it, you can use the `no` form of the command. Alternatively, you can use the `enable` keyword.

The `yellow` command is only applicable to T1 lines.

**Examples**
The following example shows how to disable yellow alarm generation:

```
RP/0/RSP0/CPU0:router(config)# controller t1 0/6/0/0/10
RP/0/RSP0/CPU0:router(config-t1e1)# yellow generation disable
```
Traffic Mirroring Commands

This module describes the commands used to configure and monitor traffic mirroring.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- acl, on page 908
- clear monitor-session counters, on page 909
- destination interface, on page 910
- destination pseudowire, on page 911
- mirror first, on page 912
- mirror interval, on page 913
- monitor-session, on page 914
- monitor-session (interface), on page 915
- show monitor-session status, on page 917
- show monitor-session counters, on page 918
acl

To configure ACL-based traffic mirroring, use the `acl` command in monitor session configuration mode. To stop ACL-based traffic mirroring, use the `no` form of this command.

**acl**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>No default behavior or values</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Monitor session configuration</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong> 4.0.0  This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you use the `acl` command, traffic is mirrored according to the definition of the global interface access list (ACL) defined in one of the following commands: *ipv4 access-list*, *ipv6 access-list*, *ethernet-services access-list*.

Even when the `acl` command is configured on the source mirroring port, if the ACL configuration command does not use the `capture` keyword, no traffic gets mirrored.

If the ACL configuration uses the `capture` keyword, but the `acl` command is not configured on the source port, although traffic is mirrored, no access list configuration is applied.

**Examples**

This example shows how to configure ACL-based traffic mirroring on the interface:

```
RP/0/RSP0/CPU0>monitor-session tm_example
RP/0/RSP0/CPU0>ethernet-services access-list tm_filter
RP/0/RSP0/CPU0>router(config-es-acl)# 10 deny 0000.1234.5678 0000.abcd.abcd any capture
RP/0/RSP0/CPU0>router(config-es-acl)# exit
RP/0/RSP0/CPU0>router(config)# interface GigabitEthernet0/2/0/0
RP/0/RSP0/CPU0>router(config-if)# monitor-session tm_example direction rx-only
RP/0/RSP0/CPU0>router(config-if)# acl
RP/0/RSP0/CPU0>router(config-if)# l2transport
RP/0/RSP0/CPU0>router(config-if)# exit
RP/0/RSP0/CPU0>router(config-if)# ethernet-services access-group tm_filter ingress
RP/0/RSP0/CPU0>router(config-if)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-services access-list</td>
<td>Defines an Ethernet services (Layer 2) access list by name.</td>
</tr>
<tr>
<td>ipv4 access-list</td>
<td>Defines an IPv4 access list by name.</td>
</tr>
</tbody>
</table>
clear monitor-session counters

To clear the traffic mirroring session statistics, use the **clear monitor-session counters** command in EXEC mode.

```
clear monitor-session counters [interface type interface-path-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Identifies the interface for which the counters are to be cleared.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-name</code></td>
<td>Name of the monitor session to clear.</td>
</tr>
</tbody>
</table>

**Command Default**

All stored statistics for all interfaces are cleared.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear the traffic mirroring statistic counters:

```
RP/0/RSP0/CPU0:router>clear monitor-session counters
```
destination interface

To associate a destination interface with a traffic mirroring session, use the destination interface command in monitor session configuration mode. To remove the designated destination, use the no form of this command.

```
destination interface type interface-path-id
```

**Syntax Description**

- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Monitor sessions configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the destination interface command to assign a traffic monitoring session to a specific destination interface. This is the port to which a network analyzer is connected. This is generally called the monitoring port.

A destination port has these characteristics:

- A destination port must reside on the same switch as the source port.
- A destination port can be any Ethernet physical port, nV Satellite ICL port or EFP, but not a bundle interface. Also, the ICL must not be a bundle interface.
- At any one time a destination port can participate in only one traffic mirroring session. A destination port in one traffic mirroring session cannot be a destination port for a second traffic mirroring session. In other words, no two monitor sessions can have the same destination port.
- A destination port cannot also be a source port.

**Examples**

This example shows how to configure a monitoring port for a traffic mirroring session:

```
RP/0/R00/CPU0:router(config)# monitor-session mon1
RP/0/R00/CPU0:router(config-mon)# destination interface gigabitethernet0/0/15
```
destination pseudowire

To direct mirrored traffic to a pseudowire, use the `destination pseudowire` command in monitor session configuration mode. To remove the pseudowire designation, use the `no` form of this command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
Monitor session configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `destination pseudowire` command to direct the mirrored traffic to a pseudowire. A network analyzer in a central location can then be used to monitor the traffic. Use the monitor session command to define the exact pseudowire to which the monitored traffic should be replicated.

**Examples**
This example shows how to configure a monitoring port for a traffic mirroring session:

```
RP/0/RP0/CPU0:router(config)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-mon)# destination pseudowire
```
mirror first

To configure partial traffic mirroring, use the **mirror first** command in monitor session configuration mode. To stop mirroring a portion of the packet, use the **no** form of this command.

```
mirror first bytes
```

**Syntax Description**

- **bytes**: Number of bytes mirrored. The mirrored packet length value can range from 65 to 128.

**Command Default**

The entire packet is mirrored.

**Command Modes**

Monitor session configuration

**Command History**

- **Release**
  - 4.0.0: This command was introduced.

**Usage Guidelines**

Use the **mirror first** command to mirror the first 64 to 128 bytes of the packet. The actual mirrored packet is the configured partial packet monitoring size plus the 4-byte trailing CRC.

**Examples**

This example shows how to mirror the first 100 bytes of the packet:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RSP0/CPU0:router(config-if)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-if-mon)# mirror first 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>monitor-session</strong>, on page 914</td>
<td>Defines a traffic mirroring session and enter monitor session configuration mode.</td>
</tr>
</tbody>
</table>
mirror interval

To configure mirror interval for a specified number of packets in traffic mirroring, use the `mirror interval` command in monitor session configuration mode. To stop mirroring the packet in the interval, use the `no` form of this command.

```
mirror interval {512 | 1k | 2k | 4k | 8k | 16k}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Number of packets per mirror interval. The interval can be configured for every 512, 1k, 2k, 4k, 8k, or 16k packets.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• port-level mirroring is only supported in the ingress direction.</td>
</tr>
<tr>
<td></td>
<td>• port-level mirroring is only supported in sampling mode with a minimal sampling rate of 1:512</td>
</tr>
</tbody>
</table>

**Command Default**
The mirror interval is set as per the specified packet count.

**Command Modes**
Monitor session configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 4.0.0 This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
This example shows how to set the mirror interval for every 512 packets:

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RSP0/CPU0:router(config-if)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-if-mon)# mirror first 100
RP/0/RSP0/CPU0:router(config-if-mon)# mirror interval 512
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor-session, on page 914</code></td>
<td>Defines a traffic mirroring session and enter monitor session configuration mode.</td>
</tr>
</tbody>
</table>


monitor-session

To define a traffic mirroring session and enter monitor session configuration mode, use the `monitor-session` command in global configuration mode. To remove the traffic mirroring session, use the `no` form of this command.

```
monitor-session  session-name
```

**Syntax Description**
- `session-name` Name of the monitor session to configure.

**Command Default**
No default behavior or values

**Command Modes**
Global configuration

**Command History**
- **Release 3.9.1** This command was introduced.

**Usage Guidelines**
Before you can assign a monitor session to a specific interface, you must configure it using the `monitor-session` command. The `session-name` should not be the same as any interface name.

In monitor session configuration mode, you should define the destination interface to be used in the traffic mirroring session using the `destination` command.

For more information about monitoring a session, see Configuring Traffic Monitoring chapter in Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

**Examples**

This example shows how to enter monitor session configuration mode:

```
RP/0/RSP0/CPU0:router(config)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-mon)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>destination interface, on page 910</code></td>
<td>Associates a destination interface with a traffic mirroring session.</td>
</tr>
</tbody>
</table>
monitor-session (interface)

To associate a traffic mirroring session with a specific interface, use the `monitor-session` command in interface configuration mode or dynamic-template configuration mode. To remove the association between a traffic mirroring session and an interface, use the `no` form of this command.

```
monitor-session session-name [direction {rx-only | tx-only}] [port-level]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-name</td>
<td>Name of the monitor session to configure.</td>
</tr>
<tr>
<td>direction</td>
<td>Specifies that traffic replication is in only one direction.</td>
</tr>
<tr>
<td>rx-only</td>
<td>Specifies that only ingress traffic is replicated.</td>
</tr>
<tr>
<td>tx-only</td>
<td>Specifies that only egress traffic is replicated.</td>
</tr>
</tbody>
</table>

**Command Default**

Replicates both ingress and egress traffic.

**Command Modes**

Interface configuration

Dynamic template configuration (for BNG)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.0.0</td>
<td>The <code>acl</code> and <code>mirror first</code> keywords were added.</td>
</tr>
<tr>
<td>5.1</td>
<td>The support for this command under dynamic-template configuration mode was added for BNG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can associate a traffic mirroring session to a specific interface, you must define it using the `monitor-session` global configuration command. After the traffic mirroring session is defined, use the `monitor-session` interface configuration command or dynamic template configuration command to associate this session with a specific source interface. For BNG sessions, the subscriber is attached to the monitor session, only when the dynamic template is applied to the subscriber. When the session is associated, all specified traffic on the interface is then replicated to the destination location defined in the monitor session configuration.

The `monitor-session` interface configuration command also enters monitor session configuration mode for you to configure additional features of the mirroring session.

If a physical interface is configured for Layer 3, then the traffic mirroring session can be associated on physical interfaces. Example:

```
interface TenGigE0/1/0/0
ipv4 address 10.0.0.1 255.255.255.0
```
If a physical interface has sub-interfaces configured for Layer 3, then the traffic mirroring session must be associated on each sub-interface. Example:

```
interface TenGigE0/1/0/1.601
ipv4 address 10.0.1.1 255.255.255.0
encapsulation dot1q 601
```

For more information about monitoring a session, see Configuring Traffic Monitoring chapter in Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enter monitor session configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/0/0/11
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# monitor-session mon1
RP/0/RSP0/CPU0:router(config-if-mon)#
```

This example shows how to configure `monitor-session` command in the dynamic-template configuration mode for BNG:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp ppp_template
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# monitor-session mon1 direction rx-only
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# acl
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# mirror first 100
```
show monitor-session status

To display status information about configured traffic mirroring sessions, use the show monitor-session status command in EXEC mode.

```
show monitor-session [session-name] status [detail] [errors]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-name</td>
<td>Name of the monitor session to configure.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays the full error string for any errors.</td>
</tr>
<tr>
<td>errors</td>
<td>Displays all sessions, but only source interfaces with errors are displayed (if no source interfaces have errors, then 'No errors' is displayed).</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show monitor-sessions status` command displays the following information:

- Destination information for the session (including the name of the interface).
- Destination status (interface state).
- List of source interfaces.
- Any other status information that may be pertinent, such as a software or hardware error that would stop sessions operating correctly. If an error is returned from interactions with another component, then the full error string is only displayed in detail output; standard tabular output reports that there has been an error but refers the user to the detailed output.

**Examples**

This example shows sample output from the `show monitor-session status` command:

```
RP/0/RSP0/CPU0:router# show monitor-session status

Monitor-session foo
Destination interface GigabitEthernet 0/0/0/0

Source Interface Dir Status
--------------------- ---- -----------------------------------------------
G10/1/0/0.10 Both Operational
G10/1/0/0.11 Rx   Operational
G10/1/0/0.12 Tx   Operational
```

Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers
show monitor-session counters

To display statistics regarding traffic mirroring sessions, use the `show monitor-session counters` command in EXEC mode.

```
show monitor-session [session-name] counters
```

**Syntax Description**

- `session-name` Name of the monitor session to configure.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show monitor-sessions counters` command displays a list of all source interfaces, and the replicated packet statistics for each interface. The full set of statistics displayed for each interface is:

- Ingress replicated packets and octets
- Egress replicated packets and octets
- Non-replicated packets and octets

**Examples**

This example shows sample output from the `show monitor-session counters` command:

```
RP/0/RSP0/CPU0:router show monitor-session 2 counters

Monitor session 2
GigabitEthernet 0/3/0/0.100:
   Rx Replicated: 100 Packets 8000 Bytes
   Tx Replicated: 2 Packets 3000 Bytes
   Non Replicated: 0 Packets 0 Bytes
```
VLAN Subinterface Commands

This module provides command line interface (CLI) commands for configuring IEEE 802.1Q VLANs on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

- dot1q vlan, on page 920
- interface (VLAN), on page 922
dot1q vlan

To assign a VLAN ID to a subinterface (or to modify the VLAN ID that is currently assigned to a subinterface), use the `dot1q vlan` command in subinterface configuration mode. To remove the VLAN ID assigned to a subinterface, use the no form of this command.

Note

Effective with Cisco IOS XR Release 3.7.2, the `dot1q vlan` command is replaced by the `encapsulation dot1q` command. See the `encapsulation dot1q` command for more information.

```
dot1q vlan vlan-id [{vlan-id2 | any}]
```

**Syntax Description**

- **vlan-id** (Optional) Identifies the host VLAN of a Q-in-Q VLAN pair. Replace `vlan-id2` with a number that specifies the host VLAN. Range is from 1 to 4094.
- **vlan-id2** (Optional) Identifies the host VLAN of a Q-in-any VLAN pair.
- **any** (Optional) Identifies the host VLAN of a Q-in any VLAN pair.

**Command Default**

No default behavior or values

**Command Modes**

Subinterface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced and was also replaced by the <code>encapsulation dot1q</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The VLAN ID specifies where 802.1Q tagged packets are sent and received on a specified subinterface. An 802.1Q VLAN subinterface must have a configured VLAN ID to send and receive traffic; without a VLAN ID, the subinterface remains in the down state. All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. To change a VLAN ID, the new VLAN must not already be in use on the same physical interface. To exchange VLAN IDs, you must remove the configuration information and reconfigure the ID for each device.

Note

The subinterface does not pass traffic without an assigned VLAN ID.

Note

The `dot1q vlan` command is replaced by the `encapsulation dot1q` command. It is still available for backward-compatibility, but only for Layer 3 interfaces. The `encapsulation dot1q` command must be used going forward.
VLAN Subinterface Commands

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure the VLAN ID and IP address on a subinterface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/RSP0/CPU0:router(config-subif)# dot1q vlan 10
RP/0/RSP0/CPU0:router(config-subif)# ipv4 addr 10.0.0.1/24
```

This example shows how to configure the VLAN IDs for both VLANS in a single Q-in-Q attachment circuit (AC). In this case, incoming traffic must match both of the VLAN IDs before it is accepted by the subinterface:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/RSP0/CPU0:router(config-subif)# dot1q vlan 10 20
```

This example shows how to configure the VLAN IDs for a Q-in-any AC. In this case, all incoming traffic must have two VLAN tags, where the outer VLAN ID matches the configured value, while the inner VLAN ID can be any value.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# dot1q vlan 10 any
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces, on page 440</td>
<td>Displays statistics for all interfaces configured on the router or for a specific node.</td>
</tr>
</tbody>
</table>
interface (VLAN)

To create a VLAN subinterface, use the `interface` command in Global Configuration mode. To delete a subinterface, use the `no` form of this command.

```bash
interface type interface-path-id.subinterface [l2transport]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `type` | Type of Ethernet interface on which you want to create a VLAN. Enter `GigabitEthernet`, `TenGigE`, or `Bundle-Ether`.
| `interface-path-id.subinterface` | Physical interface or virtual interface followed by the subinterface path ID. Naming notation is `interface-path-id.subinterface`. The period in front of the subinterface value is required as part of the notation. For more information about the syntax for the router, use the question mark (?) online help function.
| `l2transport` | Enables Layer 2 transport port mode on the specified VLAN interface and enters Layer 2 transport configuration mode. The `l2transport` keyword creates the Vlan interface in L2 mode so that it can be used for L2VPNs and local switching.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.7.2   | This command was introduced.

**Usage Guidelines**

For the `interface-path-id` argument, use the following guidelines:

- If specifying a physical interface, the naming notation is `rack/slot/module/port`. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0.
  - `port`: Physical port number of the interface.

- If specifying an Ethernet bundle interface, the range is from 1 through 65535.

For the `subinterface` argument, the range is from 0 through 4095.

To configure a large number of subinterfaces, we recommend entering all configuration data before you commit the `interface` command.

To change an interface from Layer 2 to Layer 3 mode and back, you must delete the interface first and then re-configure it in the appropriate mode.
A subinterface does not pass traffic without an assigned VLAN ID.

---

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure a VLAN subinterface on a 10-Gigabit Ethernet interface:

```bash
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/0/0/1.2
RP/0/RSP0/CPU0:router(config-subif)# dot1q vlan 1
RP/0/RSP0/CPU0:router(config-subif)# ipv4 address 50.0.0.1/24
```

This example shows how to create a VLAN subinterface with Layer 2 transport port mode enabled, and enter Layer 2 transport configuration mode under that VLAN:

```bash
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/4/0/1.1
RP/0/RSP0/CPU0:router(config-if-l2)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1q vlan</code>, on page 920</td>
<td>Assigns a VLAN ID to a subinterface (or modifies the VLAN ID that is currently assigned to a subinterface).</td>
</tr>
</tbody>
</table>
interface (VLAN)
10-Gigabit Ethernet WAN PHY Controller Commands

This module describes the commands to configure a 10-Gigabit Ethernet WAN PHY physical controller on the Cisco ASR 9000 Series Router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

For information on 10-Gigabit Ethernet (GE) interface commands see the Ethernet Interface Commandson module.

- clear controller wanphy, on page 926
- clear counters wanphy, on page 927
- controller wanphy, on page 928
- report sd-ber, on page 930
- report sf-ber disable, on page 931
- show controllers wanphy, on page 932
- threshold sd-ber, on page 938
- threshold sf-ber, on page 939
clear controller wanphy

To clear the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller, use the `clear controller wanphy` command in EXEC mode.

clear controller wanphy interface-id stats

**Syntax Description**

- **interface-id**: Physical interface instance. Naming notation is `rack/slot/module/port` and a slash between values is required as part of the notation.
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.
  - `port`: Physical port number of the interface.

For more information about the syntax for the router, use the question mark (?) online help function.

**stats**

Clears alarm counters for the specified 10-Gigabit Ethernet WAN PHY controller.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **interface** read, write, execute

**Examples**

This example shows how to configure a 10-Gigabit Ethernet WAN PHY controller in Slot 6:

```
RP/0/RSP0/CPU0:router # clear controller wanphy 0/6/0/0 stats
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers wanphy, on page 932</code></td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
clear counters wanphy

To clear the alarms counters for a specific 10-Gigabit Ethernet WAN PHY interface, use the `clear counters wanphy` command in EXEC mode.

`clear counters wanphy interface-id stats`

**Syntax Description**

- **interface-id**: Physical interface instance. Naming notation is `rack/slot/module/port` and a slash between values is required as part of the notation.
  - `rack`: Chassis number of the rack.
  - `slot`: Physical slot number of the line card.
  - `module`: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.
  - `port`: Physical port number of the interface.

For more information about the syntax for the router, use the question mark (?) online help function.

- **stats**: Clears alarm counters for the specified 10-Gigabit Ethernet WAN interface.

**Command Default**

No default behavior or values

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **Task ID**
  - Operations
    - interface: read, write, execute

**Examples**

This example shows how to clear the alarms counters for a 10-Gigabit Ethernet WAN interface:

```
RP/0/RSP0/CP00:router # clear counters wanphy 0/6/0/0 stats
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers wanphy, on page 932</td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
<tr>
<td>clear controller wanphy, on page 926</td>
<td>Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
controller wanphy

To enter WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN PHY controller, use the `controller wanphy` command in Global Configuration mode. To return the 10-Gigabit Ethernet WAN PHY controller to its default WAN mode configuration, use the `no` form of this command.

```
controller wanphy interface-id
```

**Syntax Description**

`interface-id` Physical interface instance. Naming notation is `rack/slot/module/port` and a slash between values is required as part of the notation.

- `rack`: Chassis number of the rack.
- `slot`: Physical slot number of the line card.
- `module`: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.
- `port`: Physical port number of the interface.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

After you use the `no controller wanphy` command to return a 10-Gigabit Ethernet WAN PHY controller to its default configuration, you need to cycle the power to the 10-Gigabit Ethernet SPA for the mode configuration changes to take effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enter WAN PHY controller configuration mode:

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# controller wanphy 0/6/0/0
RP/0/RSP0/CPU0:router(config-wanphy)#
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show controllers wanphy, on page 932</td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
report sd-ber

To enable Signal Degraded (SD) Bit Error Rate (BER) reporting, use the `report sd-ber` command in wanphy configuration mode. To disable Signal Degraded (SD) Bit Error Rate (BER) reporting, use the `no` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Signal Degraded (SD) Bit Error Rate (BER) reporting is disabled by default.

**Command Modes**

Wanphy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable Signal Degraded (SD) Bit Error Rate (BER) reporting.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RSP0/CPU0:router(config-wanphy)# report sd-ber
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>report sf-ber disable, on page 931</code></td>
<td>Disables SF BER reporting.</td>
</tr>
<tr>
<td><code>show controllers wanphy, on page 932</code></td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
<tr>
<td><code>threshold sf-ber, on page 939</code></td>
<td>Configures the threshold of the SF BER that is used to trigger a link state change.</td>
</tr>
</tbody>
</table>
report sf-ber disable

To disable Signal Failure (SF) Bit Error Rate (BER) reporting, use the **report sf-ber disable** command in wanphy configuration mode. To enable Signal Failure (SF) Bit Error Rate (BER) reporting, use the no form of this command. In the case of A9K-8X100GE-SE line cards, the commands **report sf-ber** and **no report sf-ber** are used to enable and disable SF BER respectively.

**report sf-ber disable**

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Signal Failure (SF) Bit Error Rate (BER) reporting is enabled by default.

**Command Modes**
Wanphy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
This example shows how to disable Signal Failure (SF) Bit Error Rate (BER) reporting.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RSP0/CPU0:router(config-wanphy)# report sf-ber disable
RP/0/RSP0/CPU0:router(config-wanphy)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>report sd-ber</strong>, on page 930</td>
<td>Enables Signal Degradation (SD) Bit Error Rate (BER) reporting.</td>
</tr>
<tr>
<td><strong>show controllers wanphy</strong>, on page 932</td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
<tr>
<td><strong>threshold sf-ber</strong>, on page 939</td>
<td>Configures the threshold of the SF BER that is used to trigger a link state change.</td>
</tr>
</tbody>
</table>
show controllers wanphy

To display alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller, use the `show controllers wanphy` command in EXEC mode.

```
show controller wanphy interface-id [{alarms | all}]
```

**Syntax Description**

`interface-id` Physical interface instance. Naming notation is `rack/slot/module/port` and a slash between values is required as part of the notation.

- `rack`: Chassis number of the rack.
- `slot`: Physical slot number of the line card.
- `module`: Module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.
- `port`: Physical port number of the interface.

For more information about the syntax for the router, use the question mark (?) online help function.

**alarms** Displays information about any alarms that are detected by the specified 10-Gigabit Ethernet WAN PHY controller.

**all** Displays registers, alarms, and module information for the specified 10-Gigabit Ethernet WAN PHY controller.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

```
Release   Modification
3.9.0      This command was introduced.
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID  Operations
interface  read
```

**Examples**

This example shows sample output from the `show controllers wanphy` command with the `all` keyword:

```
RP/0/RSP0/CP:router# show controllers wanphy 0/3/4/0 all

Interface: wanphy0_3_4_0
Configuration Mode: WAN Mode
SECTION
  LOF = 1, LOS = 1, BIP(B1) = 2912
LINE
```
AIS = 1, RDI = 0, FEBE = 949, BIP(B2) = 48562

PATH
AIS = 1, RDI = 0, FEBE = 0, BIP(B2) = 0
LOP = 0, NEWPTR = 0, PSE = 0, NSE = 0

WIS ALARMS
SER = 9, FEPLMP = 0, FEAISP = 0
WL0S = 1, PLC0 = 0
LFEI0P = 47260, PBEC = 949

Active Alarms[All defects]: lof,
Active Alarms[Highest Alarms]: lof
Rx(K1/K2): N/A, Tx(K1/K2): N/A
S1S0 = N/A, C2 = N/A

PATH TRACE BUFFER
Remote IP addr: 000.000.000.000
BER thresholds: N/A
TCA thresholds: N/A

REGISTERS
P_FEBE : 949
L_FE_BIP: 47260
L_BIP : 48562
P_BEC : 949
S_BIP : 2912
J1-Rx0 : 0x3136
J1-Rx1 : 0x352e
J1-Rx2 : 0x3234
J1-Rx3 : 0x332e
J1-Rx4 : 0x3132
J1-Rx5 : 0x3900
J1-Rx6 : 0x3138
J1-Rx7 : 0x372e

Internal Information
Operational Mode : WAN Mode
Current Alarms: 0x8

Table 64: show controllers wanphy Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Identifies the WAN physical interface, in the format rack/slot/module/port.</td>
</tr>
<tr>
<td></td>
<td>• rack: Chassis number of the rack.</td>
</tr>
<tr>
<td></td>
<td>• slot: Physical slot number of the line card.</td>
</tr>
<tr>
<td></td>
<td>• module: Module number. A physical layer interface module (PLIM) is always 0.</td>
</tr>
<tr>
<td></td>
<td>• port: Physical port number of the interface.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Current configuration mode running on this controller. Can be WAN mode or LAN mode.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **SECTION** | Displays the following section alarms:  
  - **LOF**—Number of Loss of Framing (LOF) errors on this connection section. LOF alarms are critical because they indicate that the link associated with this section is down.  
  - **LOS**—Number of loss of signal (LOS) errors on this connection section. LOS alarms are critical because they indicate that the link associated with this section is down.  
  - **BIP(B1)**—Number of bit interleaved parity (BIP) B1 errors on this section that exceeded the specified threshold. |
| **LINE** | Displays the following line alarms:  
  - **AIS**—Number of AIS errors on this line. AIS alarms are critical because they indicate that the line is down.  
  - **RDI**—Remote defect indication.  
    - Line remote defect indication is reported by the downstream LTE when it detects LOF4, LOS5, or AIS6.  
    - Path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.  
  - **FEBE**—Number of far-end block errors (FEBE) on this line. Line FEBE errors are accumulated from the M0 or M1 byte, and are reported when the downstream LTE detects BIP7 (B2) errors.  
  - **BIP(B2)**—Number of bit interleaved parity (BIP) B2 errors on this line that exceeded the specified threshold. |
| **PATH** | Displays the following path alarms:  
  - **AIS**—Number of AIS errors on this path. AIS alarms are critical because they indicate that the line associated with this path is down.  
  - **RDI**—Number of RDI errors on this path. Path RDI is a legacy alarm and is not supported.  
  - **FEBE**—Number of FEBE errors on this path. Path FEBEs are accumulated from the G1 byte, and are reported when the downstream PTE detects BIP (B3) errors.  
  - **BIP(B2)**—Number of bit interleaved parity (BIP) errors on this path that exceeded the specified threshold.  
  - **LOP**—Number of loss of pointer (LOP) errors on this path. Path LOPs are reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.  
  - **NEWPTR**—Inexact count of the number of times the SONET framer has validated a new SONET pointer value (H1, H2).  
  - **PSE**—Inexact count of the number of times the SONET framer has detected a positive stuff event (PSE) in the received pointer (H1, H2).  
  - **NSE**—Inexact count of the number of times the SONET framer has detected a negative stuff event in the received pointer (H1, H2). |

**Note** For Cisco IOS XR software release 3.5.0, the following fields display no errors: RDIFEBEBIP(B2)NEWPTRPSENSE
### Field | Description
--- | ---
WIS ALARMS | Displays the following WAN Interconnect Sublayer (WIS) layer alarms:
| • SER—Number of Severely Errored Frames (SER) errors
| • FELCDP—Number of Far End - Loss of Code-group Delineation - Path (FELCDP) errors
| • FEAISP—Number of Far End - AIS - Path (FEAISP) errors
| • WLOS—Number of WIS LOS (WLOS) errors.
| • PLCD—Number of Path Loss of Code-group Delineation (PLCD) errors
| • LFEBIP—Number of Line - Far End - BIP (LFEBI) errors
| • PBEC—Number of Path - Block Error Counter (PBEC) errors

**Note** | Alarms are applicable only when the controller is configured in WAN-PHY mode.

Active Alarms[All defects] | Total number of currently active alarms on this interface.

**Note** | Alarms are applicable only when the controller is configured in WAN-PHY mode.

Active Alarms[Highest Alarms] | Total number of the most significant active alarms on this interface. These alarms are likely causing all other alarms on the interface.

**Note** | Alarms are applicable only when the controller is configured in WAN-PHY mode.

Rx(K1/K2) | Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were received by this interface.

Tx(K1/K2) | Total number of errored K1/K2 bytes from the Line OverHead (LOH) of the SONET frame that were transmitted by this interface.

S1S0 | Number of errored payload pointer bytes on this interface.

C2 | Number of errored STS identifier (C1) bytes on this interface.

PATH TRACE BUFFER | Rx J1 trace buffer received from the far end. If the received data is valid it will be shown below the PATH TRACE BUFFER field.

Remote IP addr | Byte string containing the IP address of the remote end of this connection. If the received data is invalid, this field displays no IP address.

BER thresholds | BER threshold values of the specified alarms for a the 10-Gigabit Ethernet controller.

TCA thresholds | TCA threshold values of the specified alarms for a the 10-Gigabit Ethernet controller.
show controllers wanphy

### Field | Description
--- | ---
**REGISTERS** | Displays output from the following registers in hexadecimal format:
- P_FEBE—Total number of Far End Block Errors (FEBEs) that occurred on the path that is associated with this interface.
- L_FE_BIP—Total number of far end BIP errors that occurred on this interface.
- L_BIP—Total number of local BIP errors that occurred on this interface.
- P_BEC—Total BIP error count (BEC) that occurred on the path that is associated with this interface.
- S_BIP—Total number of far end BIP errors that occurred on the current section.
- J1-Rx0—Characters from far end IPV4 address string.
- J1-Rx1—Characters from far end IPV4 address string.
- J1-Rx2—Characters from far end IPV4 address string.
- J1-Rx3—Characters from far end IPV4 address string.
- J1-Rx4—Characters from far end IPV4 address string.
- J1-Rx5—Characters from far end IPV4 address string.
- J1-Rx6—Characters from far end IPV4 address string.
- J1-Rx7—Characters from far end IPV4 address string.
**Note** The following Serdes-WISH HW registers are used to debug counters and can be cleared only by power cycling the hardware:
P_FEBE, FEBE, L_FE_BIP, L_BIP, P_BEC, S_BIP, J1-Rx0 through J1-Rx7

**Internal Information** | Displays the following internal information for the interface:
- Operational Mode—Current operation mode for this controller. Can be WAN mode or LAN mode.
- Current Alarms—Bit map of all currently active alarms on this controller. Use this information for debugging purposes.
**Note** Alarms are applicable only when the controller is configured in WAN-PHY mode.

The following example shows sample output from the `show controllers wanphy` command with the **alarms** keyword:

```
RP/0/RSP0/CPU0:router# show controllers wanphy 0/3/4/0 alarms

Interface: wanphy0_3_4_0
Configuration Mode: WAN Mode
SECTION
  LOF = 1, LOS = 1, BIP(B1) = 2912
LINE
  AIS = 1, RDI = 0, FEBE = 949, BIP(B2) = 48562
PATH
  AIS = 1, RDI = 0, FEBE = 0, BIP(B2) = 0
  LOF = 0, NEWPTR = 0, PSE = 0, NSE = 0
WIS ALARMS
  SER = 9, FELCDP = 0, FEAISP = 0
  WLOS = 1, PLCD = 0
```
LFEBIP = 47260, PBEC = 949

Active Alarms[All defects]:
Active Alarms[Highest Alarms]:
Rx(K1/K2): N/A, Tx(K1/K2): N/A
S1S0 = N/A, C2 = N/A
PATH TRACE BUFFER
Remote IP addr: 981.761.542.321
BER thresholds: N/A
TCA thresholds: N/A

The alarm information displayed in the `show controllers wanphy interface-id alarms` command output are described in Table 64: show controllers wanphy Command Output Fields, on page 933.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear controller wanphy, on page 926</td>
<td>Clears the alarms counters for a specific 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
**threshold sd-ber**

To configure the threshold of the Signal Degrade (SD) Bit Error Rate (BER) that is used to trigger a signal degrade alarm, use the `threshold sd-ber` command in wanphy configuration mode. To return the Signal Degrade (SD) Bit Error Rate (BER) to the default value, use the `no` form of this command.

```
threshold sd-ber exponent
```

**Syntax Description**

- **exponent** Value of 10 raised to the $n$ power, where $n$ is the exponent of 10, as in $10^{-n}$. Valid values are 3 to 9, meaning $10^{-3}$ to $10^{-9}$.

**Command Default**

The default is 6, meaning $(10^{-6})$.

**Command Modes**

Wanphy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

This example shows how to configure sd-ber threshold:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RSP0/CPU0:router(config-wanphy)# threshold sd-ber 9
RP/0/RSP0/CPU0:router(config-wanphy)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report sd-ber, on page 930</td>
<td>Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.</td>
</tr>
<tr>
<td>report sf-ber disable, on page 931</td>
<td>Disables SF BER reporting.</td>
</tr>
<tr>
<td>threshold sf-ber, on page 939</td>
<td>Configures the threshold of the SF BER that is used to trigger a link state change.</td>
</tr>
</tbody>
</table>
threshold sf-ber

To configure the threshold of the Signal Failure (SF) Bit Error Rate (BER) that is used to trigger a link state change, use the `threshold sf-ber` command in wanphy configuration mode. To return the Signal Failure (SF) Bit Error Rate (BER) to the default value, use the `no` form of this command.

```
threshold sf-ber exponent
```

**Syntax Description**

| Value of 10 raised to the `n` power, where `n` is the exponent of 10, as in 10^-n. Valid values are 3 to 9, meaning 10^-3 to 10^-9. |

**Command Default**

The default is 3, meaning (10^-3).

**Command Modes**

Wanphy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure the threshold of the Signal Failure (SF) Bit Error Rate (BER):

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# controller wanphy 0/6/1/0
RP/0/RSP0/CPU0:router(config-wanphy)# threshold sf-ber 9
RP/0/RSP0/CPU0:router(config-wanphy)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report sd-ber, on page 930</td>
<td>Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.</td>
</tr>
<tr>
<td>report sf-ber disable, on page 931</td>
<td>Disables SF BER reporting.</td>
</tr>
<tr>
<td>show controllers wanphy, on page 932</td>
<td>Displays alarms, registers, and module information for a 10-Gigabit Ethernet WAN PHY controller.</td>
</tr>
</tbody>
</table>
threshold sf-ber