



## **Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router, Release 4.3.x**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-28484-01

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.

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: <http://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. (1110R)

© 2012 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface xi

Changes to This Document xi

Obtaining Documentation and Submitting a Service Request xi

---

### CHAPTER 1

#### Alarm Management and Logging Correlation Commands 1

alarm 3

all-alarms 4

all-of-router 5

clear logging correlator delete 6

clear logging events delete 7

clear logging events reset 11

context-correlation 13

logging correlator apply rule 15

logging correlator apply ruleset 18

logging correlator buffer-size 20

logging correlator rule 22

logging correlator ruleset 25

logging events buffer-size 27

logging events display-location 29

logging events level 31

logging events threshold 33

logging suppress apply rule 35

logging suppress rule 37

nonrootcause 39

reissue-nonbistate 41

reparent 43

rootcause 45

[show logging correlator buffer](#) 47  
[show logging correlator info](#) 50  
[show logging correlator rule](#) 52  
[show logging correlator ruleset](#) 55  
[show logging events buffer](#) 57  
[show logging events info](#) 62  
[show logging suppress rule](#) 64  
[show snmp correlator buffer](#) 66  
[show snmp correlator info](#) 68  
[show snmp correlator rule](#) 69  
[show snmp correlator ruleset](#) 70  
[source](#) 71  
[timeout](#) 72  
[timeout-rootcause](#) 74

---

## CHAPTER 2

### Embedded Event Manager Commands 77

[event manager directory user](#) 79  
[event manager environment](#) 81  
[event manager policy](#) 83  
[event manager refresh-time](#) 87  
[event manager run](#) 88  
[event manager scheduler suspend](#) 90  
[show event manager directory user](#) 92  
[show event manager environment](#) 94  
[show event manager metric hardware](#) 96  
[show event manager metric process](#) 98  
[show event manager policy available](#) 102  
[show event manager policy registered](#) 104  
[show event manager refresh-time](#) 107  
[show event manager statistics-table](#) 109

---

## CHAPTER 3

### IP Service Level Agreement Commands 113

[access-list](#) 117  
[action \(IP SLA\)](#) 119  
[ageout](#) 121

- [buckets \(history\) 123](#)
- [buckets \(statistics hourly\) 125](#)
- [buckets \(statistics interval\) 127](#)
- [control disable 128](#)
- [datasize request 130](#)
- [destination address \(IP SLA\) 132](#)
- [destination port 134](#)
- [distribution count 136](#)
- [distribution interval 138](#)
- [exp 140](#)
- [filter 142](#)
- [force explicit-null 144](#)
- [frequency \(IP SLA\) 146](#)
- [history 148](#)
- [interval 150](#)
- [ipsla 152](#)
- [key-chain 154](#)
- [life 156](#)
- [lives 158](#)
- [low-memory 160](#)
- [lsp selector ipv4 162](#)
- [lsr-path 164](#)
- [maximum hops 166](#)
- [maximum paths \(IP SLA\) 168](#)
- [monitor 170](#)
- [mpls discovery vpn 172](#)
- [mpls lsp-monitor 174](#)
- [operation 176](#)
- [output interface 177](#)
- [output nexthop 179](#)
- [packet count 181](#)
- [packet interval 183](#)
- [path discover 185](#)
- [path discover echo 186](#)
- [path discover path 188](#)

- path discover scan 190
- path discover session 192
- react 194
- react lpd 197
- reaction monitor 199
- reaction operation 201
- reaction trigger 203
- responder 205
- recurring 206
- reply dscp 207
- reply mode 209
- responder twamp 211
- scan delete-factor 212
- scan interval 214
- schedule monitor 216
- schedule operation 218
- schedule period 220
- server twamp 222
- show ipsla application 223
- show ipsla history 225
- show ipsla mpls discovery vpn 228
- show ipsla mpls lsp-monitor lpd 230
- show ipsla mpls lsp-monitor scan-queue 232
- show ipsla mpls lsp-monitor summary 234
- show ipsla responder statistics 237
- show ipsla statistics 239
- show ipsla statistics aggregated 242
- show ipsla statistics enhanced aggregated 251
- show ipsla twamp connection 254
- show ipsla twamp session 255
- show ipsla twamp standards 256
- source address 257
- source port 259
- start-time 261
- statistics 264

- tag (IP SLA) 267
- target ipv4 269
- target pseudowire 271
- target traffic-eng 273
- threshold 275
- threshold type average 277
- threshold type consecutive 279
- threshold type immediate 281
- threshold type xofy 283
- timeout (IP SLA) 285
- tos 287
- ttl 289
- type icmp echo 291
- type icmp path-echo 292
- type icmp path-jitter 293
- type mpls lsp ping 294
- type mpls lsp trace 296
- type udp echo 298
- type udp jitter 299
- type udp ipv4 address 300
- verify-data 302
- vrf (IP SLA) 304
- vrf (IP SLA MPLS LSP monitor) 306

---

## CHAPTER 4

### Logging Services Commands 309

- archive-length 311
- archive-size 312
- clear logging 313
- device 315
- file-size 316
- frequency (logging) 317
- logging 318
- logging archive 320
- logging buffered 322
- logging console 324

- logging console disable 326
- logging events link-status 327
- logging events link-status (interface) 329
- logging facility 332
- logging history 335
- logging history size 337
- logging hostnameprefix 339
- logging ipv4/ipv6 341
- logging localfilesize 344
- logging monitor 345
- logging source-interface 347
- logging suppress deprecated 349
- logging suppress duplicates 350
- logging trap 352
- service timestamps 354
- severity 356
- show logging 357
- show logging history 361
- terminal monitor 363

---

## CHAPTER 5

### Onboard Failure Logging Commands 365

- show logging onboard 366
- clear logging onboard 369
- hw-module logging onboard 371

---

## CHAPTER 6

### Performance Management Commands 375

- monitor controller fabric 377
- monitor controller sonet 379
- monitor interface 381
- performance-mgmt apply monitor 386
- performance-mgmt apply statistics 389
- performance-mgmt apply thresholds 392
- performance-mgmt regular-expression 395
- performance-mgmt resources dump local 396
- performance-mgmt resources memory 397



performance-mgmt resources tftp-server 399

performance-mgmt statistics 401

performance-mgmt thresholds 404

show performance-mgmt bgp 416

show performance-mgmt interface 418

show performance-mgmt mpls 421

show performance-mgmt node 423

show performance-mgmt ospf 425

show running performance-mgmt 427

---

## CHAPTER 7

### Statistics Service Commands 429

clear counters 430

load-interval 432

---

## CHAPTER 8

### Diagnostics Commands 433

diagnostic load 434

diagnostic monitor 436

diagnostic monitor interval 438

diagnostic monitor syslog 440

diagnostic monitor threshold 441

diagnostic ondemand action-on-failure 443

diagnostic ondemand iterations 445

diagnostic schedule 446

diagnostic start 448

diagnostic stop 450

diagnostic unload 451

ping (administration EXEC) 453

show diag 458

show diagnostic bootup level 463

show diagnostic content 464

show diagnostic ondemand settings 467

show diagnostic result 468

show diagnostic schedule 471

show diagnostic status 473

show run diagnostic monitor 474





## Preface

The *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router* preface contains these sections:

- [Changes to This Document](#), page xi
- [Obtaining Documentation and Submitting a Service Request](#), page xi

## Changes to This Document

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

**Table 1: Changes to this Document**

Data	Change Summary
January 2015	Initial release of the cumulative command reference document that covers all updates from Rel. 4.3.0 onwards.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). RSS feeds are a free service.





# Alarm Management and Logging Correlation Commands

---

This module describes the commands used to manage alarms and configure logging correlation rules for system monitoring on the 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 detailed information about alarm management and logging correlation concepts, configuration tasks, and examples, see the *Implementing and Monitoring Alarms and Logging Correlation* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

For system logging commands, see the *Logging Services Commands* module.

For system logging concepts, see the *Implementing Logging Services* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [alarm](#), page 3
- [all-alarms](#), page 4
- [all-of-router](#), page 5
- [clear logging correlator delete](#), page 6
- [clear logging events delete](#), page 7
- [clear logging events reset](#), page 11
- [context-correlation](#), page 13
- [logging correlator apply rule](#), page 15
- [logging correlator apply ruleset](#), page 18
- [logging correlator buffer-size](#), page 20
- [logging correlator rule](#), page 22
- [logging correlator ruleset](#), page 25
- [logging events buffer-size](#), page 27
- [logging events display-location](#), page 29

- [logging events level, page 31](#)
- [logging events threshold, page 33](#)
- [logging suppress apply rule, page 35](#)
- [logging suppress rule, page 37](#)
- [nonrootcause, page 39](#)
- [reissue-nonbistate, page 41](#)
- [reparent, page 43](#)
- [rootcause, page 45](#)
- [show logging correlator buffer, page 47](#)
- [show logging correlator info, page 50](#)
- [show logging correlator rule, page 52](#)
- [show logging correlator ruleset, page 55](#)
- [show logging events buffer, page 57](#)
- [show logging events info, page 62](#)
- [show logging suppress rule, page 64](#)
- [show snmp correlator buffer, page 66](#)
- [show snmp correlator info, page 68](#)
- [show snmp correlator rule, page 69](#)
- [show snmp correlator ruleset, page 70](#)
- [source, page 71](#)
- [timeout, page 72](#)
- [timeout-rootcause, page 74](#)

# alarm

To specify a type of alarm to be suppressed by a logging suppression rule, use the **alarm** command in logging suppression rule configuration mode.

**alarm** *msg-category group-name msg-code*

## Syntax Description

<i>msg-category</i>	Message category of the root message.
<i>group-name</i>	Group name of the root message.
<i>msg-code</i>	Message code of the root message.

## Command Default

No alarm types are configured by default.

## Command Modes

Logging suppression rule configuration

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure the logging suppression rule “commit” to suppress alarms whose root message are “MBGL”, with group name “commit” and message code “succeeded”:

```
RP/0/0/CPU0:router(config)# logging suppress rule commit
RP/0/0/CPU0:router(config-suppr-rule)# alarm MBGL COMMIT SUCCEEDED
```

## Related Commands

Command	Description
<a href="#">logging suppress rule, on page 37</a>	Creates a logging suppression rule.

# all-alarms

To configure a logging suppression rule to suppress all types of alarms, use the **all-alarms** command in logging suppression rule configuration mode.

## all-alarms

### Syntax Description

This command has no keywords or arguments.

### Command Default

No alarm types are configured by default.

### Command Modes

Logging suppression rule configuration

### Command History

Release	Modification
Release 3.8.0	This command was introduced.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to configure the logging suppression rule commit to suppress all alarms:

```
RP/0/0/CPU0:router(config)# logging suppress rule commit
RP/0/0/CPU0:router(config-suppr-rule)# all-alarms
```

### Related Commands

Command	Description
<a href="#">logging suppress rule, on page 37</a>	Creates a logging suppression rule.



# all-of-router

To apply a logging suppression rule to alarms originating from all locations on the router, use the **all-of-router** command in logging suppression apply rule configuration mode.

## all-of-router

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

**Command Default** No scope is configured by default.

**Command Modes** Logging suppression apply rule configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

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

Task ID	Task ID	Operations
	logging	execute

**Examples** This example shows how to apply the logging suppression rule “commit” to all locations on the router:

```
RP/0/0/CPU0:router(config)# logging suppress apply rule commit
RP/0/0/CPU0:router(config-suppr-apply-rule)# all-of-router
```

Related Commands	Command	Description
	<a href="#">logging suppress apply rule, on page 35</a>	Applies and activates a logging suppression rule.

# clear logging correlator delete

To delete all messages or messages specified by a correlation ID from the logging correlator buffer, use the **clear logging correlator delete** command in EXEC mode.

**clear logging correlator delete** {**all-in-buffer**| *correlation-id*}

## Syntax Description

<b>all-in-buffer</b>	Clears all messages in the logging correlator buffer.
<i>correlation-id</i>	Correlation event record ID. Up to 14 correlation IDs can be specified, separated by a space. Range is 0 to 4294967294.

## Command Default

No messages are automatically deleted unless buffer capacity is reached.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the [show logging correlator buffer, on page 47](#) command to confirm that records have been cleared.

Use the [logging correlator buffer-size, on page 20](#) command to configure the capacity of the logging correlator buffer.

## Task ID

Task ID	Operations
logging	execute

## Examples

This example shows how to clear all records from the logging correlator buffer:

```
RP/0/0/CPU0:router# clear logging correlator delete all-in-buffer
```

## Related Commands

Command	Description
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.

# clear logging events delete

To delete messages from the logging events buffer, use the **clear logging events delete** command in EXEC mode.

## clear logging events delete

### Syntax Description

<b>admin-level-only</b>	Deletes only events at the administrative level.
<b>all-in-buffer</b>	Deletes all event IDs from the logging events buffer.
<b>bistate-alarms-set</b>	Deletes bi-state alarms in the SET state.
<b>category</b> <i>name</i>	Deletes events from a specified category.
<b>context</b> <i>name</i>	Deletes events from a specified context.
<b>event-hi-limit</b> <i>event-id</i>	Deletes events with an event ID equal to or lower than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>event-lo-limit</b> <i>event-id</i>	Deletes events with an event ID equal to or higher than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>first</b> <i>event-count</i>	Deletes events, beginning with the first event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be deleted.
<b>group</b> <i>message-group</i>	Deletes events from a specified message group.
<b>last</b> <i>event-count</i>	Deletes events, beginning with the last event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be deleted.
<b>location</b> <i>node-id</i>	Deletes messages from the logging events buffer for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>message</b> <i>message-code</i>	Deletes events with the specified message code.
<b>severity-hi-limit</b>	Deletes events with a severity level equal to or lower than the severity level specified with the <i>severity</i> argument.

<b>severity</b>	<p>Severity level. Valid values are:</p> <ul style="list-style-type: none"><li>• <b>alerts</b></li><li>• <b>critical</b></li><li>• <b>emergencies</b></li><li>• <b>errors</b></li><li>• <b>informational</b></li><li>• <b>notifications</b></li><li>• <b>warnings</b></li></ul> <p><b>Note</b> Settings for the severity levels and their respective system conditions are listed under the “Usage Guidelines” section for the <b>logging events level</b> command. Events of lower severity level represent events of higher importance.</p>
<b>severity-lo-limit</b>	Deletes events with a severity level equal to or higher than the severity level specified with the <i>severity</i> argument.
<b>timestamp-hi-limit</b>	Deletes events with a time stamp equal to or lower than the specified time stamp.

*hh : mm : ss [month] [day] [year]* Time stamp for the **timestamp-hi-limit** or **timestamp-lo-limit** keyword. The *month*, *day*, and *year* arguments default to the current month, day, and year, if not specified.

Ranges for the *hh : mm : ss month day year* arguments are as follows:

- *hh* :—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
- *mm* :—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
- *ss*—Seconds. Range is 00 to 59.
- *month*—(Optional) The month of the year. The values for the *month* argument are:
  - january
  - february
  - march
  - april
  - may
  - june
  - july
  - august
  - september
  - october
  - november
  - december
- *day*—(Optional) Day of the month. Range is 01 to 31.
- *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

<b>timestamp-lo-limit</b>	Deletes events with a time stamp equal to or higher than the specified time stamp.
---------------------------	--

**Command Default** No messages are automatically deleted unless buffer capacity is reached.

**Command Modes** EXEC mode

**Command History**

Release	Modification
Release 3.2	This command was introduced.

**Usage Guidelines**

This command is used to delete messages from the logging events buffer that match the keywords and arguments that you specify. The description is matched if all of the conditions are met.

Use the [show logging events buffer, on page 57](#) command to verify that events have been cleared from the logging events buffer.

Use the [logging events buffer-size, on page 27](#) command to configure the capacity of the logging events buffer.

**Task ID**

Task ID	Operations
logging	execute

**Examples**

This example shows how to delete all messages from the logging events buffer:

```
RP/0/0/CPU0:router# clear logging events delete all-in-buffer
```

**Related Commands**

Command	Description
<a href="#">clear logging events reset, on page 11</a>	Resets bi-state alarms.
<a href="#">show logging events buffer, on page 57</a>	Displays messages in the logging events buffer.

# clear logging events reset

To reset bi-state alarms, use the **clear logging events reset** command in EXEC mode.

**clear logging events reset** {**all-in-buffer**| *event-id*}

## Syntax Description

<b>all-in-buffer</b>	Resets all bi-state alarm messages in the event logging buffer.
<i>event-id</i>	Event ID. Resets the bi-state alarm for an event or events. Up to 32 event IDs can be specified, separated by a space. Range is 0 to 4294967294.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

This command clears bi-state alarms messages from the logging events buffer. Bi-state alarms are generated by state changes associated with system hardware, such as a change of interface state from active to inactive, or the online insertion and removal (OIR) of a Modular Service Card (MSC), or a change in component temperature.

Use the [show logging events buffer, on page 57](#) command to display messages in the logging events buffer.

## Task ID

Task ID	Operations
logging	execute

## Examples

This example shows how to reset all bi-alarms in the logging events buffer:

```
RP/0/0/CPU0:router# clear logging events reset all-in-buffer
```

**Related Commands**

Command	Description
<a href="#">clear logging events delete, on page 7</a>	Deletes all bi-state alarm messages, or messages specified by correlation ID, from the logging events buffer.
<a href="#">show logging events buffer, on page 57</a>	Displays messages in the logging events buffer.



## context-correlation

To enable context-specific correlation, use the **context-correlation** command in either stateful or nonstateful correlation rule configuration mode. To disable correlation on context, use the **no** form of this command.

**context-correlation**

**no context-correlation**

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

**Command Default** Correlation on context is not enabled.

**Command Modes** Stateful correlation rule configuration  
Nonstateful correlation rule configuration

Release	Modification
Release 3.6.0	This command was introduced.

**Usage Guidelines** This command enables context-specific correlation for each of the contexts in which a given rule is applied. For example, if the rule is applied to two contexts (context1 and context2), messages that have context “context1” are correlated separately from those messages with context “context2”.

Use the [show logging correlator rule, on page 52](#) command to show the current setting for the context-correlation flag.

Task ID	Operations
logging	read, write

**Examples** This example shows how to enable correlation on context for a stateful correlation rule:

```
RP/0/0/CPU0:router(config)# logging correlator rule stateful_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# context-correlation
```

Command	Description
<a href="#">logging correlator rule, on page 22</a>	Defines the rules for correlating messages.

Command	Description
<a href="#">show logging correlator rule, on page 52</a>	Displays one or more predefined logging correlator rules.

# logging correlator apply rule

To apply and activate a correlation rule and enter correlation apply rule configuration mode, use the **logging correlator apply rule** command in Global Configuration mode. To deactivate a correlation rule, use the **no** form of this command.

**logging correlator apply rule** *correlation-rule* [**all-of-router**| **context** *name*| **location** *node-id*]

**no logging correlator apply rule** *correlation-rule* [**all-of-router**| **context** *name*| **location** *node-id*]

## Syntax Description

<i>correlation-rule</i>	Name of the correlation rule to be applied.
<b>all-of-router</b>	(Optional) Applies the correlation rule to the entire router.
<b>context</b> <i>name</i>	(Optional) Applies the correlation rule to the specified context. Unlimited number of contexts. The <i>name</i> string is limited to 32 characters.
<b>location</b> <i>node-id</i>	(Optional) Applies the correlation rule to the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. Unlimited number of locations.

## Command Default

No correlation rules are applied.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator apply rule** command is used to either add or remove apply settings for a given rule. These settings then determine which messages are correlated for the affected rules.

If the rule is applied to **all-of-router**, then correlation occurs for only those messages that match the configured cause values for the rule to be correlated, regardless of the context or location setting of that message.

If a rule is applied to a specific set of contexts or locations, then correlation occurs for only those messages that match both the configured cause values for the rule and at least one of those contexts or locations.

Use the [show logging correlator rule, on page 52](#) command to show the current apply settings for a given rule.

**Tip**

When a rule is applied (or if a rule set that contains this rule is applied), then the rule definition cannot be modified through the configuration until the rule or rule set is once again unapplied.

**Tip**

It is possible to configure apply settings at the same time for both a rule and zero or more rule sets that contain the rule. In this case, the apply settings for the rule are the union of all the apply configurations.

The **logging correlator apply rule** command allows you to enter submode (config-corr-apply-rule) to apply and activate rules:

```
RP/0/0/CPU0:router(config)# logging correlator apply rule statefull
RP/0/0/CPU0:router(config-corr-apply-rule)#?
```

```
all-of-router  Apply the rule to all of the router
clear          Clear the uncommitted configuration
clear         Clear the configuration
commit        Commit the configuration changes to running
context       Apply rule to specified context
describe      Describe a command without taking real actions
do            Run an exec command
exit          Exit from this submode
location      Apply rule to specified location
no            Negate a command or set its defaults
pwd           Commands used to reach current submode
root          Exit to the global configuration mode
show          Show contents of configuration
```

```
RP/0/0/CPU0:router(config-corr-apply-rule)#
```

While in the submode, you can negate keyword options:

```
RP/0/0/CPU0:router(config-corr-apply-rule)# no all-of-router
RP/0/0/CPU0:router(config-corr-apply-rule)# no context
RP/0/0/CPU0:router(config-corr-apply-rule)# no location
```

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to apply a predefined correlator rule to a location:

```
RP/0/0/CPU0:router(config)# logging correlator apply rule rule1
RP/0/0/CPU0:router(config-corr-apply-rule)# location 0/2/CPU0
```

**Related Commands**

Command	Description
<a href="#">logging correlator rule, on page 22</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator rule, on page 52</a>	Displays one or more predefined logging correlator rules.

Command	Description
<a href="#">show logging correlator ruleset, on page 55</a>	Displays one or more predefined logging correlator rule sets.

# logging correlator apply ruleset

To apply and activate a correlation rule set and enter correlation apply rule set configuration mode, use the **logging correlator apply ruleset** command in Global Configuration mode. To deactivate a correlation rule set, use the **no** form of this command.

**logging correlator apply ruleset** *correlation-ruleset* [**all-of-router**| **context name**| **location node-id**]

**no logging correlator apply ruleset** *correlation-ruleset* [**all-of-router**| **context name**| **location node-id**]

## Syntax Description

<i>correlation-ruleset</i>	Name of the correlation rule set to be applied.
<b>all-of-router</b>	(Optional) Applies the correlation rule set to the entire router.
<b>context name</b>	(Optional) Applies the correlation rule set to the specified context. Unlimited number of contexts. The <i>name</i> string is limited to 32 characters.
<b>location node-id</b>	(Optional) Applies the correlation rule to the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. Unlimited number of locations.

## Command Default

No correlation rule sets are applied.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator apply ruleset** command is used to either add or remove apply settings for a given rule set. These settings then determine which messages are correlated for the affected rules.

If the rule set is applied to **all-of-router**, then correlation occurs for only those messages that match the configured cause values for the rule to be correlated, regardless of the context or location setting of that message.

If a rule set is applied to a specific set of contexts or locations, then correlation occurs for only those messages that match both the configured cause values for the rule and at least one of those contexts or locations.

Use the [show logging correlator ruleset, on page 55](#) command to show the current apply settings for a given rule set.

**Tip**

When a rule is applied (or if a rule set that contains this rule is applied), then the rule definition cannot be modified through the configuration until the rule or rule set is once again unapplied.

**Tip**

It is possible to configure apply settings at the same time for both a rule and zero or more rule sets that contain the rule. In this case, the apply settings for the rule are the union of all the apply configurations.

The **logging correlator apply ruleset** command allows you to enter the submode (config-corr-apply-ruleset) to apply and activate rule sets:

```
RP/0/0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/0/CPU0:router(config-corr-apply-ruleset)#?
  all-of-router  Apply the rule to all of the router
  clear         Clear the uncommitted configuration
  clear         Clear the configuration
  commit        Commit the configuration changes to running
  context       Apply rule to specified context
  describe      Describe a command without taking real actions
  do            Run an exec command
  exit          Exit from this submode
  location      Apply rule to specified location
  no            Negate a command or set its defaults
  pwd          Commands used to reach current submode
  root         Exit to the global configuration mode
  show         Show contents of configuration
RP/0/0/CPU0:router(config-corr-apply-ruleset)#
```

While in the submode, you can negate keyword options:

```
RP/0/0/CPU0:router(config-corr-apply-ruleset)# no all-of-router
RP/0/0/CPU0:router(config-corr-apply-ruleset)# no context
RP/0/0/CPU0:router(config-corr-apply-ruleset)# no location
```

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to apply a predefined correlator rule set to the entire router:

```
RP/0/0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/0/CPU0:router(config-corr-apply-rule)# all-of-router
```

**Related Commands**

Command	Description
<a href="#">show logging correlator ruleset, on page 55</a>	Displays one or more predefined logging correlator rule sets.

# logging correlator buffer-size

To configure the logging correlator buffer size, use the **logging correlator buffer-size** command in Global Configuration mode. To return the buffer size to its default setting, use the **no** form of this command.

**logging correlator buffer-size** *bytes*

**no logging correlator buffer-size** *bytes*

<b>Syntax Description</b>	<i>bytes</i>	The size, in bytes, of the logging correlator buffer. Range is 1024 to 52428800 bytes.
---------------------------	--------------	--

<b>Command Default</b>	<i>bytes</i> : 81920 bytes
------------------------	----------------------------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.2	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>logging correlator buffer-size</b> command configures the size of the correlation buffer. This buffer holds all the correlation records as well as the associated correlated messages. When the size of this buffer is exceeded, older correlations in the buffer are replaced with the newer incoming correlations. The criteria that are used to recycle these buffers are:</p> <ul style="list-style-type: none"> <li>• First, remove the oldest nonstateful correlation records from the buffer.</li> <li>• Then, if there are no more nonstateful correlations present; remove the oldest stateful correlation records.</li> </ul> <p>Use the <a href="#">show logging correlator info, on page 50</a> command to confirm the size of the buffer and the percentage of buffer space that is currently used. The <a href="#">show logging events buffer, on page 57</a> <b>all-in-buffer</b> command can be used to show the details of the buffer contents.</p>
-------------------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	logging	read, write

<b>Examples</b>	This example shows how to set the logging correlator buffer size to 90000 bytes:
-----------------	--

```
RP/0/0/CPU0:router(config)# logging correlator buffer-size 90000
```



**Related Commands**

Command	Description
<a href="#">show logging correlator info, on page 50</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.

# logging correlator rule

To define the rules for correlating messages, use the **logging correlator rule** command in Global Configuration mode. To delete the correlation rule, use the **no** form of this command.

**logging correlator rule** *correlation-rule* **type** {stateful| nonstateful}

**no logging correlator rule** *correlation-rule*

## Syntax Description

<i>correlation-rule</i>	Name of the correlation rule to be applied.
<b>type</b>	Specifies the type of rule.
<b>stateful</b>	Enters stateful correlation rule configuration mode.
<b>nonstateful</b>	Enters nonstateful correlation rule configuration mode.

## Command Default

No rules are defined.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator rule** command defines the correlation rules used by the correlator to store messages in the logging correlator buffer. A rule must, at a minimum, consist of three elements: a root-cause message, one or more non-root-cause messages, and a timeout.

When the root-cause message, or a non-root-cause message is received, the timer is started. Any non-root-cause messages are temporarily held, while the root-cause is sent to syslog. If, after the timer has expired, the root-cause and at least one non-root-cause message was received, a correlation is created and stored in the correlation buffer.

A rule can be of type stateful or nonstateful. Stateful rules allow non-root-cause messages to be sent from the correlation buffer if the bi-state root-cause alarm clears at a later time. Nonstateful rules result in correlations that are fixed and immutable after the correlation occurs.

Below are the rule parameters that are available while in stateful correlation rule configuration mode:

```
RP/0/0/CPU0:router(config-corr-rule-st)# ?
```

```
context-correlation  Specify enable correlation on context
nonrootcause         nonrootcause alarm
reissue-nonbistate    Specify reissue of non-bistate alarms on parent clear
```

```

reparent          Specify reparent of alarm on parent clear
rootcause         Specify root cause alarm: Category/Group/Code combos
timeout           Specify timeout
timeout-rootcause Specify timeout for root-cause

```

```
RP/0/0/CPU0:router(config-corr-rule-st)#
```

Below are the rule parameters that are available while in nonstateful correlation rule configuration mode:

```
RP/0/0/CPU0:router(config-corr-rule-nonst)# ?
```

```

context-correlation Specify enable correlation on context
nonrootcause        nonrootcause alarm
rootcause           Specify root cause alarm: Category/Group/Code combos
timeout             Specify timeout
timeout-rootcause   Specify timeout for root-cause
RP/0/0/CPU0:router(config-corr-rule-nonst)#

```

**Note**

A rule cannot be deleted or modified while it is applied, so the **no logging correlator apply** command must be used to unapply the rule before it can be changed.

**Note**

The name of the correlation rule must be unique across all rule types and is limited to a maximum length of 32 characters.

Use the [show logging correlator buffer](#), on page 47 to display messages stored in the logging correlator buffer.

Use the [show logging correlator rule](#), on page 52 command to verify correlation rule settings.

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to enter stateful correlation rule configuration mode to specify a collection duration period time for correlator messages sent to the logging events buffer:

```

RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# timeout 50000

```

**Related Commands**

Command	Description
<a href="#">logging correlator apply rule</a> , on page 15	Applies and activates correlation rules.
<a href="#">nonrootcause</a> , on page 39	Enters non-root-cause configuration mode and specifies a non-root-cause alarm.
<a href="#">reissue-nonbistate</a> , on page 41	Reissues non-bistate alarm messages (events) from the correlator log after its root-cause alarm clears.

Command	Description
<a href="#">reparent, on page 43</a>	Reparents non-root-cause messages to the next highest active root-cause in a hierarchical correlation when their immediate parent clears.
<a href="#">rootcause, on page 45</a>	Specifies a root-cause message alarm.
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator rule, on page 52</a>	Displays one or more predefined logging correlator rules.
<a href="#">timeout, on page 72</a>	Specifies the collection period duration time for the logging correlator rule message.
<a href="#">timeout-rootcause, on page 74</a>	Specifies an optional parameter for an applied correlation rule.

# logging correlator ruleset

To enter correlation rule set configuration mode and define a correlation rule set, use the **logging correlator ruleset** command in Global Configuration mode. To delete the correlation rule set, use the **no** form of this command.

**logging correlator ruleset** *correlation-ruleset* **rulename** *correlation-rulename*

**no logging correlator ruleset** *correlation-ruleset*

## Syntax Description

<i>correlation-ruleset</i>	Name of the correlation rule set to be applied.
<b>rulename</b>	Specifies the correlation rule name.
<i>correlation-rulename</i>	Name of the correlation rule name to be applied.

## Command Default

No rule sets are defined.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator ruleset** command defines a specific correlation rule set. A rule set name must be unique and is limited to a maximum length of 32 characters.

To apply a logging correlator rule set, use the [logging correlator apply ruleset, on page 18](#) command.

## Examples

This example shows how to specify a logging correlator rule set:

```
RP/0/0/CPU0:router(config)# logging correlator ruleset ruleset_1
RP/0/0/CPU0:router(config-corr-ruleset)# rulename state_rule
RP/0/0/CPU0:router(config-corr-ruleset)# rulename state_rule2
```

## Related Commands

Command	Description
<a href="#">logging correlator apply ruleset, on page 18</a>	Applies and activates a correlation rule set and enters correlation apply rule set configuration mode.

Command	Description
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator ruleset, on page 55</a>	Displays defined correlation rule set names.

# logging events buffer-size

To configure the size of the logging events buffer, use the **logging events buffer-size** command in Global Configuration mode. To restore the buffer size to the default value, use the **no** form of this command.

**logging events buffer-size** *bytes*

**no logging events buffer-size** *bytes*

## Syntax Description

<i>bytes</i>	The size, in bytes, of the logging events buffer. Range is 1024 to 1024000 bytes. The default is 43200 bytes.
--------------	---

## Command Default

*bytes*: 43200

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

### Note

The logging events buffer automatically adjusts to a multiple of the record size that is lower than or equal to the value configured for the *bytes* argument.

Use the [show logging events info](#), on page 62 command to confirm the size of the logging events buffer.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to increase the logging events buffer size to 50000 bytes:

```
RP/0/0/CPU0:router(config)# logging events buffer-size 50000
```

**Related Commands**

Command	Description
<a href="#">logging events level, on page 31</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 33</a>	Specifies the event logging buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging correlator info, on page 50</a>	Displays information about the size of the logging correlator buffer and available capacity.
<a href="#">show logging events buffer, on page 57</a>	Displays messages in the logging events buffer.
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.



# logging events display-location

To enable the alarm source location display field for bistate alarms in the output of the **show logging** and **show logging events buffer** command, use the **logging events display-location** command in Global Configuration mode.

**logging events display-location**

**no logging events display-location**

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

**Command Default** The alarm source location display field in **show logging** output is not enabled.

**Command Modes** Global Configuration mode

Release	Modification
Release 3.8.0	This command was introduced.

**Usage Guidelines** The output of the **show logging** command for bistate alarms has been enhanced. Previously, the alarm source field in the output displayed the location of the process that logged the alarm. Use the **logging events display-location** command to configure the output of the **show logging** command to include an additional source field that displays the actual source of the alarm. The alarm source is displayed in a format that is consistent with alarm source identification in other platforms and equipment. The new alarm source display field aids accurate identification and isolation of the source of a fault.

By default, the output of the **show logging** command does not include the new alarm source identification field. If you enable the alarm source location display field in the **show logging** output, the same naming conventions are also used to display hardware locations in the **show diag** and **show inventory** command output.



**Note** Customer OSS tools may rely on the default output to parse and interpret the alarm output.

Task ID	Operations
logging	read, write

**Examples**

This example shows the **show logging** command output for bistate alarms before and after enabling the alarm source location display field:

```
RP/0/0/CPU0:router# show logging | inc Interface

Wed Aug 13 01:30:58.461 UTC
LC/0/2/CPU0:Aug 12 01:20:54.073 : ifmgr[159]: %PKT_INFRA-LINK-5-CHANGED : Interface
GigabitEthernet0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/2/0/0, changed state to Down
LC/0/2/CPU0:Aug 12 01:20:59.451 : ifmgr[159]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
on Interface GigabitEthernet0/2/0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/5/CPU0/0, changed state to Administratively Down
RP/0/5/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
on Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/5/CPU0/0, changed state to Up
RP/0/5/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
on Interface MgmtEth0/5/CPU0/0, changed state to Up

RP/0/0/CPU0:router# config
Wed Aug 13 01:31:32.517 UTC

RP/0/0/CPU0:router(config)# logging events display-location

RP/0/0/CPU0:router(config)# commit

RP/0/0/CPU0:router(config)# exit

RP/0/0/CPU0:router# show logging | inc Interface

Wed Aug 13 01:31:48.141 UTC
LC/0/2/CPU0:Aug 12 01:20:54.073 : ifmgr[159]: %PKT_INFRA-LINK-5-CHANGED : Interface
GigabitEthernet0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : interface
GigabitEthernet0/2/0/0: Interface GigabitEthernet0/2/0/0, changed state to Down
LC/0/2/CPU0:Aug 12 01:20:59.451 : ifmgr[159]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
GigabitEthernet0/2/0/0: Line protocol on Interface GigabitEthernet0/2/0/0, changed state
to Down
RP/0/5/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/5/CPU0/0, changed state to Administratively Down
RP/0/5/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/5/CPU0/0: Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/5/CPU0/0: Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/5/CPU0/0: Interface MgmtEth0/5/CPU0/0, changed state to Up
RP/0/5/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/5/CPU0/0: Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Up
```

**Related Commands**

Command	Description
<a href="#">show logging events buffer, on page 57</a>	Displays messages in the logging events buffer.

# logging events level

To specify a severity level for logging alarm messages, use the **logging events level** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

**logging events level** *severity*

**no logging events level**

## Syntax Description

*severity* Severity level of events to be logged in the logging events buffer, including events of a higher severity level (numerically lower). [Table 2: Alarm Severity Levels for Event Logging](#), on page 31 lists severity levels and their respective system conditions.

## Command Default

All severity levels (from 0 to 6) are logged.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

This command specifies the event severity necessary for alarm messages to be logged. Severity levels can be specified by the severity level description (for example, **warnings**). When a severity level is specified, events of equal or lower severity level are also written to the logging events buffer.



### Note

Events of lower severity level represent events of higher importance.

This table lists the system severity levels and their corresponding numeric values, and describes the corresponding system condition.

**Table 2: Alarm Severity Levels for Event Logging**

Severity Level Keyword	Numeric Value	Logged System Messages
emergencies	0	System is unusable.
alerts	1	Critical system condition exists requiring immediate action.
critical	2	Critical system condition exists.

Severity Level Keyword	Numeric Value	Logged System Messages
errors	3	Noncritical errors.
warnings	4	Warning conditions.
notifications	5	Notifications of changes to system configuration.
informational	6	Information about changes to system state.

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to set the severity level for notification to warnings (level 4):

```
RP/0/0/CPU0:router(config)# logging events level warnings
```

**Related Commands**

Command	Description
<a href="#">logging events buffer-size, on page 27</a>	Specifies the logging events buffer size.
<a href="#">logging events threshold, on page 33</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.

# logging events threshold

To specify the logging events buffer threshold that, when surpassed, generates an alarm, use the **logging events threshold** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

**logging events threshold** *percent*

**no logging events threshold**

## Syntax Description

<i>percent</i>	Minimum percentage of buffer capacity that must be allocated to messages before an alarm is generated. Range is 10 to 100. The default is 80 percent.
----------------	---

## Command Default

*percent*: 80 percent

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

This command can be configured to generate an alarm when 10 percent or more of the event buffer capacity is available.

The logging events buffer is circular; that is, when full it overwrites the oldest messages in the buffer. Once the logging events buffer reaches full capacity, the next threshold alarm is generated when the number of overwritten events surpasses the percentage of buffer capacity allocated to messages.

Use the [show logging events info, on page 62](#) command to display the current threshold setting.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure the threshold setting to 95 percent of buffer capacity:

```
RP/0/0/CPU0:router(config)# logging events threshold 95
```

**Related Commands**

Command	Description
<a href="#">logging events buffer-size, on page 27</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 31</a>	Specifies a severity level for logging alarm messages.
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.

# logging suppress apply rule

To apply and activate a logging suppression rule, use the **logging suppress apply rule** command in Global Configuration mode. To deactivate a logging suppression rule, use the **no** form of this command.

**logging suppress apply rule** *rule-name* [**all-of-router**| **source location** *node-id*]

**no logging suppress apply rule** *rule-name* [**all-of-router**| **source location** *node-id*]

## Syntax Description

<i>rule-name</i>	Name of the logging suppression rule to activate.
<b>all-of-router</b>	(Optional) Applies the specified logging suppression rule to alarms originating from all locations on the router.
<b>source location</b> <i>node-id</i>	(Optional) Applies the specified logging suppression rule to alarms originating from the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

## Command Default

No logging suppression rules are applied.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to apply a predefined logging suppression rule to the entire router:

```
RP/0/0/CPU0:router(config)#logging suppress apply rule infobistate
RP/0/0/CPU0:router(config-suppr-apply-rule)# all-of-router
```

**Related Commands**

Command	Description
<a href="#">all-of-router</a> , on page 5	Applies a logging suppression rule to suppress alarms originating from all sources on the router.
<a href="#">source</a> , on page 71	Applies a logging suppression rule to alarms originating from a specific node on the router.



# logging suppress rule

To create a logging suppression rule and enter the configuration mode for the rule, use the **logging suppress rule** command in the Global Configuration mode. To remove a logging suppression rule, use the **no** form of this command.

**logging suppress rule** *rule-name* [**alarm** *msg-category group-name msg-code*] **all-alarms**]

**no logging suppress rule** *rule-name*

## Syntax Description

<i>rule-name</i>	Name of the rule.
<b>alarm</b>	(Optional) Specifies a type of alarm to be suppressed by the logging suppression rule.
<i>msg-category</i>	Message category of the root message.
<i>group-name</i>	Group name of the root message.
<i>msg-code</i>	Message code of the root message.
<b>all-alarms</b>	(Optional) Specifies that the logging suppression rule suppresses all types of alarms.

## Command Default

No logging suppression rules exist by default.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

If you use the **logging suppress rule** command without specifying a non-root-cause alarm, you can do so afterwards, by entering the **alarm** keyword at the prompt.

## Task ID

Task ID	Operations
logging	read, write

**Examples**

This example shows how to create a logging suppression rule called infobistate:

```
RP/0/0/CPU0:router(config)# logging suppress rule infobistate
RP/0/0/CPU0:router(config-suppr-rule)#
```

**Related Commands**

Command	Description
<a href="#">alarm, on page 3</a>	Specifies a type of alarm to be suppressed by a logging suppression rule.
<a href="#">all-alarms, on page 4</a>	Configures a logging suppression rule to suppress all types of alarms.

## nonrootcause

To enter the non-root-cause configuration mode and specify a non-root-cause alarm, use the **nonrootcause** command in stateful or nonstateful correlation rule configuration modes.

**nonrootcause alarm** *msg-category group-name msg-code*

**no nonrootcause**

### Syntax Description

<b>alarm</b>	Non-root-cause alarm.
<i>msg-category</i>	(Optional) Message category assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.
<i>group-name</i>	(Optional) Message group assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.
<i>msg-code</i>	(Optional) Message code assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.

### Command Default

Non-root-cause configuration mode and alarm are not specified.

### Command Modes

Stateful correlation rule configuration  
Nonstateful correlation rule configuration

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

### Usage Guidelines

This command is used to enter the non-root-cause configuration mode to configure one or more non-root-cause alarms associated with a particular correlation rule.

Use the [show logging events info](#), on page 62 command to display the current threshold setting.

If you use the **nonrootcause** command without specifying a non-root-cause alarm, you can do so afterwards, by entering the **alarm** keyword at the prompt.

### Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to enter non-root-cause configuration mode and display the commands that are available under this mode:

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# nonrootcause
RP/0/0/CPU0:router(config-corr-rule-st-nonrc)# ?
alarm      Specify non-root cause alarm: Category/Group/Code combos
clear      Clear the uncommitted configuration
clear      Clear the configuration
commit     Commit the configuration changes to running
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
pwd        Commands used to reach current submode
root       Exit to the global configuration mode
show       Show contents of configuration
```

This example shows how to specify a non-root-cause alarm for Layer 2 local SONET messages with an alarm severity of 4. The non-root-cause alarm is associated with the correlation rule named `state_rule`.

```
RP/0/0/CPU0:router(config-corr-rule-st-nonrc)# alarm L2 SONET_LOCAL ALARM
```

## Related Commands

Command	Description
<a href="#">logging events buffer-size, on page 27</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 31</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 33</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.

# reissue-nonbistate

To reissue non-bistate alarm messages (events) from the correlator log after the root-cause alarm of a stateful rule clears, use the **reissue-nonbistate** command in stateful or nonstateful correlation rule configuration modes. To disable the reissue-nonbistate flag, use the **no** form of this command.

**reissue-nonbistate**

**no reissue-nonbistate**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Non-bistate alarm messages are not reissued after their root-cause alarm clears.

## Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

By default, when the root-cause alarm of a stateful correlation is cleared, any non-root-cause, bistate messages being held for that correlation are silently deleted and are not sent to syslog. If the non-bistate messages should be sent, use the **reissue-nonbistate** command for the rules where this behavior is required.

## Task ID

Task ID	Operations
logging	read, write


## Examples

This example shows how to reissue nonbistate alarm messages:

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# reissue-nonbistate
```

## Related Commands

Command	Description
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging events buffer, on page 57</a>	Displays messages in the logging events buffer.

 reissue-nonbistate

# reparent

To reparent non-root-cause messages to the next highest active rootcause in a hierarchical correlation when their immediate parent clears, use the **reparent** command in stateful correlation rule configuration mode. To disable the reparent flag, use the **no** form of this command.

**reparent**

**no reparent**

## Syntax Description

This command has no keywords or arguments.

## Command Default

A non-root-cause alarm is sent to syslog after a root-cause parent clears.

## Command Modes

Stateful correlation rule configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

Use the **reparent** command to specify what happens to non-root-cause alarms in a hierarchical correlation after their root-cause alarm clears. The following scenario illustrates why you may want to set the reparent flag.

Rule 1 with rootcause A and non-rootcause B

Rule 2 with rootcause B and non-rootcause C

(Alarm B is a non-rootcause for Rule 1 and a rootcause for Rule 2. For the purpose of this example, all the messages are bistate alarms.)

If both Rule 1 and Rule 2 each trigger a successful correlation, then a hierarchy is constructed that links these two correlations. When alarm B clears, alarm C would normally be sent to syslog, but the operator may choose to continue suppression of alarm C (hold it in the correlation buffer); because the rootcause that is higher in the hierarchy (alarm A) is still active.

The reparent flag allows you to specify non-root-cause behavior—if the flag is set, then alarm C becomes a child of rootcause alarm A; otherwise, alarm C is sent to syslog.



### Note

Stateful behavior, such as reparenting, is supported only for bistate alarms. Bistate alarms are associated with system hardware, such as a change of interface state from active to inactive.

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to set the reparent flag for a stateful rule:

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# reparent
```

**Related Commands**

Command	Description
<a href="#">logging correlator rule, on page 22</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.



# rootcause

To specify the root-cause alarm message, use the **rootcause** command in stateful or nonstateful correlation rule configuration modes.

**rootcause** *msg-category group-name msg-code*

**no rootcause**

## Syntax Description

<i>msg-category</i>	Message category of the root message.
<i>group-name</i>	Group name of the root message.
<i>msg-code</i>	Message code of the root message.

## Command Default

Root-cause alarm is not specified.

## Command Modes

Stateful correlation rule configuration  
Nonstateful correlation rule configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

This command is used to configure the root-cause message for a particular correlation rule. Messages are identified by their message category, group, and code. The category, group, and code each can contain up to 32 characters. The root-cause message for a stateful correlation rule should be a bi-state alarm.

Use the [show logging events info, on page 62](#) command to display the root-cause and non-root-cause alarms for a correlation rule.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure a root-cause alarm for a stateful correlation rule:

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# rootcause L2 SONET_LOCAL ALARM
```

**Related Commands**

Command	Description
<a href="#">logging events buffer-size, on page 27</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 31</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 33</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">timeout-rootcause, on page 74</a>	Specifies an optional parameter for an applied correlation rule.
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.

## show logging correlator buffer

To display messages in the logging correlator buffer, use the **show logging correlator buffer** command in EXEC mode.

**show logging correlator buffer** {**all-in-buffer** [**ruletype** [**nonstateful**| **stateful**]] [**rulesource** [**internal**| **user**]] [**rule-name** *correlation-rule1* ... *correlation-rule14*] [**correlationID** *correlation-id1* .. *correlation-id14*}

### Syntax Description

<b>all-in-buffer</b>	Displays all messages in the correlation buffer.
<b>ruletype</b>	(Optional) Displays the ruletype filter.
<b>nonstateful</b>	(Optional) Displays the nonstateful rules.
<b>stateful</b>	(Optional) Displays the stateful rules.
<b>rulesource</b>	(Optional) Displays the rulesource filter.
<b>internal</b>	(Optional) Displays the internally defined rules from the rulesource filter.
<b>user</b>	(Optional) Displays the user-defined rules from the rulesource filter.
<b>rule-name</b> <i>correlation-rule1</i> ... <i>correlation-rule14</i>	Displays a messages associated with a correlation rule name. Up to 14 correlation rules can be specified, separated by a space.
<b>correlationID</b> <i>correlation-id1</i> .. <i>correlation-id14</i>	Displays a message identified by correlation ID. Up to 14 correlation IDs can be specified, separated by a space. Range is 0 to 4294967294.

### Command Default

None

### Command Modes

EXEC mode

### Command History

Release	Modification
Release 3.2	This command was introduced.

Release	Modification
Release 3.6.0	<p>The following keywords were added:</p> <ul style="list-style-type: none"> <li>• <b>internal</b></li> <li>• <b>nonstateful</b></li> <li>• <b>rulesource</b></li> <li>• <b>ruletype</b></li> <li>• <b>stateful</b></li> <li>• <b>user</b></li> </ul> <p>Range changed from 32 to 14 for <b>correlationID</b> and <b>rule-name</b> keywords.</p>

**Usage Guidelines**

This command displays messages from the logging correlator buffer that match the correlation ID or correlation rule name specified. When the **all-in-buffer** keyword is entered, all messages in the logging correlator buffer are displayed.

If the ruletype is not specified, then both stateful and nonstateful rules are displayed.

if the rulesource is not specified, then both user and internal rules are displayed.

**Task ID**

Task ID	Operations
logging	read

**Examples**

This is the sample output from the **show logging correlator buffer** command:

```
RP/0/0/CPU0:router# show logging correlator buffer all-in-buffer
```

```
#C_id.id:Rule Name:Source :Context: Time : Text
#14.1 :Rule1:RP/0/5/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]: %PKT_INFRA-LINK-3-UPDOWN :
Interface MgmtEth0/5/CPU0/0, changed state to Down
#14.2 :Rule1:RP/0/5/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]: %PKT_INFRA-LINEPROTO-3-UPDOWN
: Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Down
```

This table describes the significant fields shown in the display.

**Table 3: show logging correlator buffer Field Descriptions**

Field	Description
C_id.	Correlation ID assigned to a event that matches a logging correlation rule.

Field	Description
id	An ID number assigned to each event matching a particular correlation rule. This event number serves as index to identify each individual event that has been matched for a logging correlation rule.
Rule Name	Name of the logging correlation rule that filters messages defined in a logging correlation rule to the logging correlator buffer.
Source	Node from which the event is generated.
Time	Date and time at which the event occurred.
Text	Message string that delineates the event.

### Related Commands

Command	Description
<a href="#">show logging correlator info, on page 50</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
<a href="#">show logging correlator rule, on page 52</a>	Displays one or more predefined logging correlator rules.

# show logging correlator info

To display the logging correlator buffer size and the percentage of the buffer occupied by correlated messages, use the **show correlator info** command in EXEC mode.

**show logging correlator info**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

This command displays the size of the logging correlator buffer and the percentage of the buffer allocated to correlated messages.

Use the [logging correlator buffer-size, on page 20](#) command to set the size of the buffer.

## Task ID

Task ID	Operations
logging	read

## Examples

In this example, the **show logging correlator info** command is used to display remaining buffer size and percentage allocated to correlated messages:

```
RP/0/0/CPU0:router# show logging correlator info

Buffer-Size      Percentage-Occupied
      81920              0.00
```

## Related Commands

Command	Description
<a href="#">logging correlator buffer-size, on page 20</a>	Specifies the logging correlator buffer size.
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.

Command	Description
<a href="#">show logging correlator rule, on page 52</a>	Displays one or more predefined logging correlator rules.

# show logging correlator rule

To display defined correlation rules, use the **show logging correlator rule** command in EXEC mode.

**show logging correlator rule** {**all**|**correlation-rule1...correlation-rule14**} [**context** *context1...context 6*] [**location** *node-id1...node-id6*] [**rulesource** {**internal**|**user**}] [**ruletype** {**nonstateful**|**stateful**}] [**summary**|**detail**]

## Syntax Description

<b>all</b>	Displays all rule sets.
<i>correlation-rule1...correlation-rule14</i>	Rule set name to be displayed. Up to 14 predefined correlation rules can be specified, separated by a space.
<b>context</b> <i>context1...context 6</i>	(Optional) Displays a list of context rules.
<b>location</b> <i>node-id1...node-id6</i>	(Optional) Displays the location of the list of rules filter from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>rulesource</b>	(Optional) Displays the rulesource filter.
<b>internal</b>	(Optional) Displays the internally defined rules from the rulesource filter.
<b>user</b>	(Optional) Displays the user defined rules from the rulesource filter.
<b>ruletype</b>	(Optional) Displays the ruletype filter.
<b>nonstateful</b>	(Optional) Displays the nonstateful rules.
<b>stateful</b>	(Optional) Displays the stateful rules.
<b>summary</b>	(Optional) Displays the summary information.
<b>detail</b>	(Optional) Displays detailed information.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.



Release	Modification
Release 3.6.0	<p>The following keyword and argument pairs were added:</p> <ul style="list-style-type: none"> <li>• <b>context</b> <i>context</i></li> <li>• <b>detail</b></li> <li>• <b>location</b> <i>node-id</i></li> <li>• <b>rulesource</b> { <i>internal</i>   <i>user</i> }</li> <li>• <b>ruletype</b> { <i>nonstateful</i>   <i>stateful</i> }</li> <li>• <b>summary</b></li> </ul>

**Usage Guidelines**

If the ruletype is not specified, then both stateful and nonstateful rules are displayed as the default.

If the rulesource is not specified, then both user and internally defined rules are displayed as the default.

If the summary or detail keywords are not specified, then detailed information is displayed as the default.

**Task ID**

Task ID	Operations
logging	read

**Examples**

This is sample output from the **show logging correlator rule** command:

```
RP/0/0/CPU0:router# show logging correlator rule test
```

```
Rule Name : test
Type : Non Stateful
Source : User
Timeout : 30000 Rule State: RULE_APPLIED_ALL
Rootcause Timeout : None
Context Correlation : disabled
Reissue Non Bistate : N/A
Reparent : N/A
Alarms :
Code Type: Category Group Message
Root: MGBL CONFIG DB_COMMIT
Leaf: L2 SONET ALARM
Apply Locations: None
Apply Contexts: None
Number of buffered alarms : 0
```

This table describes the significant fields shown in the display.

**Table 4: show logging correlator rule Field Descriptions**

Field	Description
Rule Name	Name of defined correlation rule.
Time out	Configured timeout for the correlation rule.

**show logging correlator rule**

Field	Description
Rule State	Indicates whether or not the rule has been applied. If the rule applies to the entire router, this field will display "RULE_APPLIED_ALL."
Code Type	Message category, group, and code.
Root	Message category, group and code of the root message configured in the logging correlation rule.
Leaf	Message category, group and code of a non-root-cause message configured in the logging correlation rule.
Apply Locations	Node or nodes where the rule is applied. If the logging correlation rule applies to the entire router, this field will display "None."
Apply Contexts	Context or contexts to which the rule is applied. If the logging correlation rule is not configured to apply to a context, this field will display "None."

**Related Commands**

Command	Description
<a href="#">logging correlator apply rule, on page 15</a>	Applies and activates correlation rules.
<a href="#">logging correlator rule, on page 22</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator info, on page 50</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages

# show logging correlator ruleset

To display defined correlation rule set names, use the **show logging correlator ruleset** command in EXEC mode.

**show logging correlator ruleset** {**all**| *correlation-ruleset1 ... correlation-ruleset14*} [**detail**| **summary**]

## Syntax Description

<b>all</b>	Displays all rule set names.
<i>correlation-rule1...correlation-rule14</i>	Rule set name to be displayed. Up to 14 predefined rule set names can be specified, separated by a space.
<b>detail</b>	(Optional) Displays detailed information.
<b>summary</b>	(Optional) Displays the summary information.

## Command Default

Detail is the default, if nothing is specified.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

If the ruletype is not specified, then both stateful and nonstateful rules are displayed as the default.  
 If the rulesource is not specified, then both user and internally defined rules are displayed as the default.  
 If the summary or detail options are not specified, then detailed information is displayed as the default.

## Task ID

Task ID	Operations
logging	read

## Examples

This is the sample output from the **show logging correlator ruleset** command:

```
RP/0/0/CPU0:router# show logging correlator RuleSetOne RuleSetTwo

Rule Set Name : RuleSetOne
Rules: Rule1 : Applied
```

**show logging correlator ruleset**

```

Rule2 : Applied
Rule3 : Applied
Rule Set Name : RuleSetTwo
Rules: Rule1 : Applied
Rule5 : Not Applied

```

This is the sample output from the **show logging correlator ruleset** command when the **all** option is specified:

```
RP/0/0/CPU0:router# show logging correlator ruleset all
```

```

Rule Set Name : RuleSetOne
Rules: Rule1 : Applied
Rule2 : Applied
Rule3 : Applied
Rule Set Name : RuleSetTwo
Rules: Rule1 : Applied
Rule5 : Not Applied
Rule Set Name : RuleSetThree
Rules: Rule2 : Applied
Rule3 : Applied

```

This is sample output from the **show logging correlator ruleset** command when the **all** and **summary** options are specified:

```

RP/0/0/CPU0:router# show logging correlator ruleset all summary
RuleSetOne
RuleSetTwo
RuleSetThree

```

This table describes the significant fields shown in the display.

**Table 5: show logging correlator ruleset Field Descriptions**

Field	Description
Rule Set Name	Name of the ruleset.
Rules	All rules contained in the ruleset are listed.
Applied	The rule is applied.
Not Applied	The rule is not applied.

**Related Commands**

Command	Description
<a href="#">logging correlator apply rule, on page 15</a>	Applies and activates correlation rules.
<a href="#">logging correlator rule, on page 22</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 47</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator info, on page 50</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
<a href="#">show logging correlator rule, on page 52</a>	Displays defined correlation rules.

## show logging events buffer

To display messages in the logging events buffer, use the **show logging events buffer** command in EXEC mode.

**show logging events buffer** [**admin-level-only**] [**all-in-buffer**] [**bistate-alarms-set**] [**category name**] [**context name**] [**event-hi-limit event-id**] [**event-lo-limit event-id**] [**first event-count**] [**group message-group**] [**last event-count**] [**location node-id**] [**message message-code**] [**severity-hi-limit severity**] [**severity-lo-limit severity**] [**timestamp-hi-limit hh:mm:ss [month] [day] [year]**] [**timestamp-lo-limit hh:mm:ss [month] [day] [year]**]

### Syntax Description

<b>admin-level-only</b>	Displays only the events that are at the administrative level.
<b>all-in-buffer</b>	Displays all event IDs in the events buffer.
<b>bistate-alarms-set</b>	Displays bi-state alarms in the SET state.
<b>category name</b>	Displays events from a specified category.
<b>context name</b>	Displays events from a specified context.
<b>event-hi-limit event-id</b>	Displays events with an event ID equal to or lower than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>event-lo-limit event-id</b>	Displays events with an event ID equal to or higher than the event ID specified with <i>event-id</i> argument. Range is 0 to 4294967294.
<b>first event-count</b>	Displays events in the logging events buffer, beginning with the first event. For the <i>event-count</i> argument, enter the number of events to be displayed.
<b>group message-group</b>	Displays events from a specified message group.
<b>last event-count</b>	Displays events, beginning with the last event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be displayed.
<b>location node-id</b>	Displays events for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>message message-code</b>	Displays events with the specified message code.
<b>severity-hi-limit</b>	Displays events with a severity level equal to or lower than the specified severity level.

<b>severity</b>	<p>Severity level. Valid values are:</p> <ul style="list-style-type: none"><li>• <b>emergencies</b></li><li>• <b>alerts</b></li><li>• <b>critical</b></li><li>• <b>errors</b></li><li>• <b>warnings</b></li><li>• <b>notifications</b></li><li>• <b>informational</b></li></ul> <p><b>Note</b> Settings for the severity levels and their respective system conditions are listed under the “Usage Guidelines” section for the <b>logging events level</b> command. Events of lower severity level represent events of higher importance.</p>
<b>severity-lo-limit</b>	Displays events with a severity level equal to or higher than the specified severity level.
<b>timestamp-hi-limit</b>	Displays events with a time stamp equal to or lower than the specified time stamp.

*hh : mm : ss [month] [day] [year]* Time stamp for the **timestamp-hi-limit** or **timestamp-lo-limit** keyword. The *month*, *day*, and *year* arguments default to the current month, day, and year if not specified.

Ranges for the *hh : mm : ss month day year* arguments are as follows:

- *hh* :—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
- *mm* :—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
- *ss*—Seconds. Range is 00 to 59.
- *month*—(Optional) The month of the year. The values for the *month* argument are:
  - january
  - february
  - march
  - april
  - may
  - june
  - july
  - august
  - september
  - october
  - november
  - december
- *day*—(Optional) Day of the month. Range is 01 to 31.
- *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

---

<b>timestamp-lo-limit</b>	Displays events with a time stamp equal to or higher than the specified time stamp.
---------------------------	---

---

**Command Default**      None

**Command Modes**      EXEC mode

**Command History**

Release	Modification
Release 3.2	This command was introduced.

**Usage Guidelines**

This command displays messages from the logging events buffer matching the description. The description is matched when all of the conditions are met.

**Task ID**

Task ID	Operations
logging	read

**Examples**

This is the sample output from the **show logging events buffer all-in-buffer** command:

```
RP/0/0/CPU0:router# show logging events buffer all-in-buffer
```

```
#ID      :C_id:Source      :Time                               :%CATEGORY-GROUP-SEVERITY-MESSAGECODE: Text
#1       :      :RP/0/0/CPU0:Jan  9 08:57:54 2004:nvram[66]: %MEDIA-NVRAM_PLATFORM-3-BAD_N
VRAM_VAR : ROMMON variable-value pair: '^['[19~CONFIG_FILE = disk0:config/startup, contains
illegal (non-printable)characters
#2       :      :RP/0/0/CPU0:Jan  9 08:58:21 2004:psarb[238]: %PLATFORM-PSARB-5-GO_BID : Card
is going to bid state.
#3       :      :RP/0/0/CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-5-GO_ACTIVE :
Card is becoming active.
#4       :      :RP/0/0/CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-6-RESET_ALL_LC_
CARDS : RP going active; resetting all linecards in chassis
#5       :      :RP/0/0/CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-GO_ACTIVE : this
card going active
#6       :      :RP/0/0/CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-FAILOVER_ENABLED :
Failover has been enabled by config
```

This table describes the significant fields shown in the display.

**Table 6: show logging correlator buffer Field Descriptions**

Field	Description
#ID	Integer assigned to each event in the logging events buffer.
C_id.	Correlation ID assigned to a event that has matched a logging correlation rule.
Source	Node from which the event is generated.
Time	Date and time at which the event occurred.
%CATEGORY-GROUP-SEVERITY-MESSAGECODE	The category, group name, severity level, and message code associated with the event.



Field	Description
Text	Message string that delineates the event.

**Related Commands**

Command	Description
<a href="#">show logging events info, on page 62</a>	Displays configuration and operational messages about the logging events buffer.

# show logging events info

To display configuration and operational information about the logging events buffer, use the **show logging events info** command in EXEC mode.

**show logging events info**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.2	This command was introduced.

**Usage Guidelines** This command displays information about the size of the logging events buffer, the maximum size of the buffer, the number of records being stored, the maximum allowable number of records threshold for circular filing, and message filtering.

Task ID	Task ID	Operations
	logging	read

**Examples** This is the sample output from the **show logging events info** command:

```
RP/0/0/CPU0:router# show logging events info
```

```
Size (Current/Max)      #Records      Thresh      Filter
16960      /42400      37          90          Not Set
```

This table describes the significant fields shown in the display.

**Table 7: show logging events info Field Descriptions**

Field	Description
Size (Current/Max)	The current and maximum size of the logging events buffer. The maximum size of the buffer is controlled by the <a href="#">logging events buffer-size, on page 27</a> command.

Field	Description
#Records	The number of event records stored in the logging events buffer.
Thresh	The configured logging events threshold value. This field is controlled by the <a href="#">logging events threshold, on page 33</a> command.
Filter	The lowest severity level for events that will be displayed. This field is controlled by the <a href="#">logging events level, on page 31</a> command.

**Related Commands**

Command	Description
<a href="#">logging events buffer-size, on page 27</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 31</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 33</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging events buffer, on page 57</a>	Displays information about messages in the logging events buffer according to type, time, or severity level.

# show logging suppress rule

To display defined logging suppression rules, use the **show logging suppression rule** command in EXEC mode.

**show logging suppress rule** [*rule-name1* [... [*rule-name14*]]] **all** [**detail**] [**summary**] [**source location** *node-id*]

## Syntax Description

<i>rule-name1</i> [... <i>rule-name14</i> ]	Specifies up to 14 logging suppression rules to display.
<b>all</b>	Displays all logging suppression rules.
<b>source location</b> <i>node-id</i>	(Optional) Displays the location of the list of rules filter from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>detail</b>	(Optional) Displays detailed information.
<b>summary</b>	(Optional) Displays the summary information.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
logging	read

## Examples

This example displays information about a logging suppression rule that has been configured but has not been activated:

```
RP/0/0/CPU0:router# show logging suppression rule test_suppression
```

```

Rule Name : test_suppression
Rule State: RULE_UNAPPLIED
Severities : informational, critical
Alarms :
    Category      Group      Message
    CAT_C         GROUP_C   CODE_C
    CAT_D         GROUP_D   CODE_D

Apply Alarm-Locations:  PLIM-0/2, PowerSupply-0/A/A0
Apply Sources:         0/RP0/CPU0, 1/6/SP

```

Number of suppressed alarms : 0

This example displays information about all logging suppression rules applied to a specific source location on the router:

```
RP/0/0/CPU0:router# show logging suppress rule all source location 0/RP0/CPU0
```

```

Rule Name : test_suppression
Rule State: RULE_APPLIED_ALL
Severities : N/A
Alarms :
    Category      Group      Message
    CAT_E         GROUP_F   CODE_G

Apply Alarm-Locations:  None
Apply Sources:         0/RP0/CPU0

```

Number of suppressed alarms : 0

This example shows summary information about all logging suppression rules:

```

RP/0/0/CPU0:router# show logging suppression rule all summary
Rule Name                                     :Number of Suppressed Alarms
Mike1                                         0
Mike2                                         0
Mike3                                         0
Reall                                         4

```

## Related Commands

Command	Description
<a href="#">logging suppress apply rule, on page 35</a>	Applies and activates a logging suppression rule.
<a href="#">logging suppress rule, on page 37</a>	Creates a logging suppression rule.

# show snmp correlator buffer

To display messages in SNMP correlator buffer, use the **show snmp correlator buffer** in EXEC mode.

**show snmp correlator buffer** [**all** | **correlation ID** | **rule-name name**]

## Syntax Description

<b>all</b>	Displays all messages in the correlator buffer.
<b>correlation id</b>	Displays a message identified by correlation ID. Range is 0 to 4294967294. Up to 14 correlation rules can be specified, separated by a space.
<b>rule-name name</b>	Displays a messages associated with a SNMP correlation rule name. Up to 14 correlation rules can be specified, separated by a space.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
snmp	read

## Examples

The sample shows an output from the **show snmp correlator buffer** command:

```
RP/0/0/CPU0:router# show snmp correlator buffer correlationID 10
Correlation ID : 10
Rule : ospf-trap-rule
Rootcause: 1.3.6.1.6.3.1.1.5.3
Time : Dec 14 02:32:05
Varbind(s):
  ifIndex.17 = 17
  ifDescr.17 = POS0/7/0/0
  ifType.17 = other(1)
  cieIfStateChangeReason.17 = down

  Nonroot : 1.3.6.1.2.1.14.16.2.2
```

```
Time: Dec 14 02:32:04
Varbind(s):
  ospfRouterId = 1.1.1.1
  ospfNbrIpAddress = 30.0.28.2
  ospfNbrAddressLessIndex = 0
  ospfNbrRtrId = 3.3.3.3
  ospfNbrState = down(1)
```

# show snmp correlator info

To display the SNMP correlator buffer size and the percentage of the buffer occupied by correlated messages, use the **show snmp correlator info** command in EXEC mode.

**show snmp correlator info**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
snmp	read

## Examples

The sample shows an output that contains remaining buffer size and percentage allocated to correlated messages from the **show snmp correlator info** command:

```
RP/0/0/CPU0:router# show snmp correlator info
      Buffer-Size      Percentage-Occupied
      85720             0.00
```



# show snmp correlator rule

To display defined SNMP correlation rules, use the **show snmp correlator rule** command in EXEC mode.

**show snmp correlator rule** [**all**| *rule-name*]

## Syntax Description

<b>all</b>	Displays all rule sets.
<i>rule-name</i>	Specifies the name of a rule. Up to 14 predefined SNMP correlation rules can be specified, separated by a space.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
snmp	read

## Examples

This sample shows an output from the **show snmp correlator rule** command:

```
RP/0/0/CPU0:router# show snmp correlator rule rule_1
Rule Name : rule_1
  Time out : 888                               Rule State: RULE_APPLIED_ALL
    Root:   OID    : 1.3.6.1.2.1.11.0.2
            vbind  : 1.3.6.1.2.1.2.2.1.2 value /3\.3\.d{1,3}\.d{1,3}/
            vbind  : 1.3.6.1.2.1.5.8.3   index val
    Nonroot: OID    : 1.3.6.1.2.1.11.3.3
```

# show snmp correlator ruleset

To display defined SNMP correlation rule set names, use the **show snmp correlator ruleset** command in EXEC mode.

**show snmp correlator ruleset** [**all**| *ruleset-name*]

## Syntax Description

<b>all</b>	Displays all rule set names.
<i>ruleset-name</i>	Specifies the name of a rule set. Up to 14 predefined rule set names can be specified, separated by a space.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
snmp	read

## Examples

This sample shows an output from the **show snmp correlator ruleset** command:

```
RP/0/0/CPU0:router# show snmp correlator ruleset test
Rule Set Name : test
Rules: chris1           : Not Applied
      chris2           : Applied
```

## source

To apply a logging suppression rule to alarms originating from a specific node on the router, use the **source** command in logging suppression apply rule configuration mode.

**source location** *node-id*

**no source location** *node-id*

### Syntax Description

<b>location</b> <i>node-id</i>	Specifies a node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
--------------------------------	---

### Command Default

No scope is configured by default.

### Command Modes

Logging suppression apply rule configuration

### Command History

Release	Modification
Release 3.8.0	This command was introduced.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

Task ID	Operations
logging	execute

### Examples

This example shows how to configure the logging suppression rule infobistate to suppress alarms from 0/RP0/CPU0:

```
RP/0/0/CPU0:router(config)# logging suppress apply rule infobistate
RP/0/0/CPU0:router(config-suppr-apply-rule)# source location 0/RP0/CPU0
```

### Related Commands

Command	Description
<a href="#">logging suppress apply rule, on page 35</a>	Applies and activates a logging suppression rule.

# timeout

To specify the collection period duration time for the logging correlator rule message, use the **timeout** command in stateful or nonstateful correlation rule configuration modes. To remove the timeout period, use the **no** form of this command.

**timeout** [ *milliseconds* ]

**no timeout**

## Syntax Description

*milliseconds* Range is 1 to 600000 milliseconds.

## Command Default

Timeout period is not specified.

## Command Modes

Stateful correlation rule configuration  
Nonstateful correlation rule configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

Each correlation rule that is applied must have a timeout value, and only those messages captured within this timeout period can be correlated together.

The timeout begins when the first matching message for a correlation rule is received. If the root-cause message is received, it is immediately sent to syslog, while any non-root-cause messages are held.

When the timeout expires and the rootcause message has not been received, then all the non-root-cause messages captured during the timeout period are reported to syslog. If the root-cause message was received during the timeout period, then a correlation is created and placed in the correlation buffer.



### Note

The root-cause alarm does not have to appear first. It can appear at any time within the correlation time period.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to define a logging correlation rule with a timeout period of 60,000 milliseconds (one minute):

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# timeout 60000
```

## Related Commands

Command	Description
<a href="#">logging correlator rule</a> , on page 22	Defines the rules by which the correlator logs messages to the logging events buffer.
<a href="#">timeout-rootcause</a> , on page 74	Specifies an optional parameter for an applied correlation rule.

# timeout-rootcause

To specify an optional parameter for an applied correlation rule, use the **timeout-rootcause** command in stateful or nonstateful correlation rule configuration modes. To remove the timeout period, use the **no** form of this command.

**timeout-rootcause** [ *milliseconds* ]

**no timeout-rootcause**

Syntax Description	<i>milliseconds</i> Range is 1 to 600000 milliseconds.					
Command Default	Root-cause alarm timeout period is not specified.					
Command Modes	Stateful correlation rule configuration Nonstateful correlation rule configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.6.0</td><td>This command was introduced.</td></tr></table>		Release	Modification	Release 3.6.0	This command was introduced.
Release	Modification					
Release 3.6.0	This command was introduced.					
Usage Guidelines	<p>When a root-cause timeout is configured and a non-root-cause message is received first, the following occurs:</p> <ul style="list-style-type: none"><li>When a root-cause timeout is configured and a non-root-cause message is received first, the following occurs: When the root-cause message arrives before the root-cause timeout expires, then the correlation continues as normal using the remainder of the main rule timeout.</li><li>When the root-cause message is not received before the root-cause timeout expires, then all the non-root-cause messages held during the root-cause timeout period are sent to syslog and the correlation is terminated.</li></ul>					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>logging</td><td>read, write</td></tr></table>		Task ID	Operations	logging	read, write
Task ID	Operations					
logging	read, write					


## Examples

This example shows how to configure a timeout period for a root cause alarm:

```
RP/0/0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/0/CPU0:router(config-corr-rule-st)# timeout-rootcause 50000
```

## Related Commands

Command	Description
<a href="#">logging correlator rule</a> , on page 22	Defines the rules by which the correlator logs messages to the logging events buffer.

 `timeout-rootcause`





## Embedded Event Manager Commands

---

This module describes the commands that are used to set the Embedded Event Manager (EEM) operational attributes and monitor EEM operations.

The Cisco IOS XR software EEM functions as the central clearing house for the events detected by any portion of Cisco IOS XR software High Availability Services. The EEM is responsible for fault detection, fault recovery, and process the reliability statistics in a system. The EEM is policy driven and enables you to configure the high-availability monitoring features of the system to fit your needs.

The EEM monitors the reliability rates achieved by each process in the system. You can use these metrics during testing to identify the components that do not meet their reliability or availability goals, which in turn enables you to take corrective action.

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 detailed information about the EEM concepts, configuration tasks, and examples, see the *Configuring and Managing Embedded Event Manager Policies* module in *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [event manager directory user](#), page 79
- [event manager environment](#), page 81
- [event manager policy](#), page 83
- [event manager refresh-time](#), page 87
- [event manager run](#), page 88
- [event manager scheduler suspend](#), page 90
- [show event manager directory user](#), page 92
- [show event manager environment](#), page 94
- [show event manager metric hardware](#), page 96
- [show event manager metric process](#), page 98
- [show event manager policy available](#), page 102
- [show event manager policy registered](#), page 104
- [show event manager refresh-time](#), page 107

- [show event manager statistics-table](#), page 109

## event manager directory user

To specify a directory name for storing user library files or user-defined Embedded Event Manager (EEM) policies, use the **event manager directory user** command in Global Configuration mode. To disable the use of a directory for storing user library files or user-defined EEM policies, use the **no** form of this command.

**event manager directory user** {*library path*|*policy path*}

**no event manager directory user** {*library path*|*policy path*}

### Syntax Description

<b>library</b>	Specifies a directory name for storing user library files.
<i>path</i>	Absolute pathname to the user directory on the flash device.
<b>policy</b>	Specifies a directory name for storing user-defined EEM policies.

### Command Default

No directory name is specified for storing user library files or user-defined EEM policies.

### Command Modes

Global Configuration mode

### Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>fault manager userlibdirectory</b> and <b>fault manager userpolicydirectory</b> commands were replaced with the <b>event manager directory user</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

### Usage Guidelines

Cisco IOS XR software supports only the policy files that are created by using the Tool Command Language (TCL) scripting language. The TCL software is provided in the Cisco IOS XR software image when the EEM is installed on the network device. Files with the .tcl extension can be EEM policies, TCL library files, or a special TCL library index file named tclindex. The tclindex file contains a list of user function names and library files that contain the user functions (procedures). The EEM searches the user library directory when the TCL starts to process the tclindex file.

#### User Library

A user library directory is needed to store user library files associated with authoring EEM policies. If you do not plan to write EEM policies, you do not have to create a user library directory.

To create user library directory before identifying it to the EEM, use the **mkdir** command in EXEC mode. After creating the user library directory, use the **copy** command to copy the .tcl library files into the user library directory.

### User Policy

A user policy directory is essential to store the user-defined policy files. If you do not plan to write EEM policies, you do not have to create a user policy directory. The EEM searches the user policy directory when you enter the **event manager policy *policy-name* user** command.

To create a user policy directory before identifying it to the EEM, use the **mkdir** command in EXEC mode. After creating the user policy directory, use the **copy** command to copy the policy files into the user policy directory.

### Task ID

Task ID	Operations
eem	read, write

### Examples

This example shows how to set the pathname for a user library directory to /usr/lib/tcl on disk0:

```
RP/0/0/CPU0:router(config)# event manager directory user library disk0:/usr/lib/tcl
```

This example shows how to set the location of the EEM user policy directory to /usr/fm\_policies on disk0:

```
RP/0/0/CPU0:router(config)# event manager directory user policy disk0:/usr/fm_policies
```

### Related Commands

Command	Description
<a href="#">event manager policy, on page 83</a>	Registers an EEM policy with the EEM.
<a href="#">show event manager directory user, on page 92</a>	Displays the directory name for storing user library and policy files.

# event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

**event manager environment** *var-name* [ *var-value* ]

**no event manager environment** *var-name*

## Syntax Description

<i>var-name</i>	Name assigned to the EEM environment configuration variable.
<i>var-value</i>	(Optional) Series of characters, including embedded spaces, to be placed in the environment variable <i>var-name</i> .

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>fault manager environment</b> command was replaced with the <b>event manager environment</b> command. The <i>var-value</i> argument was changed from required to optional.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

## Usage Guidelines

Environment variables are available to EEM policies when you set the variables using the **event manager environment** command. They become unavailable when you remove them with the **no** form of this command.

By convention, the names of all the environment variables defined by Cisco begin with an underscore character (\_) to set them apart, for example, `_show_cmd`.

Spaces can be used in the *var-value* argument. This command interprets everything after the *var-name* argument until the end of the line in order to be a part of the *var-value* argument.

Use the [show event manager environment](#), on page 94 command to display the name and value of all EEM environment variables before and after they have been set using the **event manager environment** command.

**Task ID**

Task ID	Operations
eem	read, write

**Examples**

This example shows how to define a set of EEM environment variables:

```
RP/0/0/CPU0:router(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
RP/0/0/CPU0:router(config)# event manager environment _show_cmd show eem manager policy
registered
RP/0/0/CPU0:router(config)# event manager environment _email_server alpha@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_from beta@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_to beta@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_cc
```

**Related Commands**

Command	Description
<a href="#">show event manager environment, on page 94</a>	Displays the name and value for all the EEM environment variables.

# event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in Global Configuration mode. To unregister an EEM policy from the EEM, use the **no** form of this command.

**event manager policy** *policy-name* **username** *username* [**persist-time** [*seconds*] **infinite**]] **type** {**system** | **user**}]

**no event manager policy** *policy-name* [**username** *username*]

**event manager policy** <*name of policy file*> **username** <*val*> [**persist-time** <*val*> {**system** | **user**}] [**checksum** {**md5** | **sha-1**} | <*checksum\_val*>]] [**secure-mode** {**trust** | **cisco rsa-2048**}]

## Syntax Description

<i>policy-name</i>	Name of the policy file.
<b>username</b> <i>username</i>	Specifies the username used to run the script. This name can be different from that of the user who is currently logged in, but the registering user must have permissions that are a superset of the username that runs the script. Otherwise, the script is not registered, and the command is rejected.  In addition, the username that runs the script must have access privileges to the commands issued by the EEM policy being registered.
<b>persist-time</b> [ <i>seconds</i>   <b>infinite</b> ]	(Optional) The length of the username authentication validity, in seconds. The default time is 3600 seconds (1 hour). The <i>seconds</i> range is 0 to 4294967294. Enter 0 to stop the username authentication from being cached. Enter the <b>infinite</b> keyword to stop the username from being marked as invalid.
<b>type</b>	(Optional) Specifies the type of policy.
<b>system</b>	(Optional) Registers a system policy defined by Cisco.
<b>user</b>	(Optional) Registers a user-defined policy.
<b>checksum</b> { <b>md5</b>   <b>sha-1</b> }	Specifies a script that is verified against checksum policies.
<b>secure-mode</b> { <b>trust</b>   <b>cisco rsa-2048</b> }	Specifies a script that is verified against Cisco signing server in secure mode.

## Command Default

The default persist time is 3600 seconds (1 hour).

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

Release	Modification
Release 3.3.0	Support was added for the required keyword and argument <b>username</b> <i>username</i> .  Support was added for the optional keyword and argument <b>persist-time</b> [ <i>seconds</i>   <b>infinite</b> ].
Release 3.6.0	The <b>fault manager policy</b> command was replaced with the <b>event manager policy</b> command.  The <b>type</b> keyword was added.
Release 3.7.0	Task ID was changed from fault-mgr to eem.
Release 5.2.0	Support added for verifying scripts against digital signatures, checksum, third party scripts and Cisco signing server.

### Usage Guidelines

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the EEM examines the policy and registers it to be run when the specified event occurs. An EEM script is available to be scheduled by the EEM until the **no** form of this command is entered.



#### Note

AAA authorization (such as the **aaa authorization** command with the **eventmanager** and **default** keywords) must be configured before the EEM policies can be registered. The **eventmanager** and **default** keywords must be configured for policy registration. See the *Configuring AAA Services on the Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco XR 12000 Series Router* for more information on AAA authorization configuration.

#### Username

Enter the username that should execute the script with the **username** *username* keyword and argument. This name can be different from the user who is currently logged in, but the registering user must have permissions that are a superset of the username that runs the script. Otherwise, the script will not be registered, and the command will be rejected. In addition, the username that runs the script must have access privileges to the commands issued by the EEM policy being registered.

#### Persist-time

When a script is first registered, the configured **username** for the script is authenticated. If authentication fails, or if the AAA server is down, the script registration fails.

After the script is registered, the username is authenticated each time a script is run.

If the AAA server is down, the username authentication can be read from memory. The **persist-time** determines the number of seconds this username authentication is held in memory.

- If the AAA server is down and the **persist-time** has not expired, the username is authenticated from memory, and the script runs.
- If the AAA server is down, and the **persist-time** has expired, user authentication fails, and the script does not run.



**Note**

EEM attempts to contact the AAA server and refresh the username reauthenticate whenever the configured **refresh-time** expires. See the [event manager refresh-time](#), [on page 87](#) command for more information.

These values can be used for the **persist-time**:

- The default **persist-time** is 3600 seconds (1 hour). Enter the **event manager policy** command without the **persist-time** keyword to set the **persist-time** to 1 hour.
- Enter zero to stop the username authentication from being cached. If the AAA server is down, the username is not authenticated and the script does not run.
- Enter **infinite** to stop the username from being marked as invalid. The username authentication held in the cache will not expire. If the AAA server is down, the username is authenticated from the cache.

**Type**

If you enter the **event manager policy** command without specifying the **type** keyword, the EEM first tries to locate the specified policy file in the system policy directory. If the EEM finds the file in the system policy directory, it registers the policy as a system policy. If the EEM does not find the specified policy file in the system policy directory, it looks in the user policy directory. If the EEM locates the specified file in the user policy directory, it registers the policy file as a user policy. If the EEM finds policy files with the same name in both the system policy directory and the user policy directory, the policy file in the system policy directory takes precedence, and the policy file is registered as a system policy.

**Task ID**

Task ID	Operations
eem	read, write

**Examples**

This example shows how to register a user-defined policy named cron.tcl located in the user policy directory:

```
RP/0/0/CPU0:router(config)# event manager policy cron.tcl username joe
```

**Related Commands**

Command	Description
<a href="#">event manager environment</a> , <a href="#">on page 81</a>	Specifies a directory for storing user library files.
<a href="#">event manager refresh-time</a> , <a href="#">on page 87</a>	Specifies the time between the system attempts to contact the AAA server and refresh the username reauthentication.
<a href="#">show event manager environment</a> , <a href="#">on page 94</a>	Displays the name and value for all EEM environment variables.
<a href="#">show event manager policy available</a> , <a href="#">on page 102</a>	Displays EEM policies that are available to be registered.
<a href="#">show event manager policy registered</a> , <a href="#">on page 104</a>	Displays the EEM policies that are already registered.



## event manager refresh-time

To define the time between user authentication refreshes in Embedded Event Manager (EEM), use the **event manager refresh-time** command in Global Configuration mode. To restore the system to its default condition, use the **no** form of this command.

**event manager refresh-time** *seconds*

**no event manager refresh-time** *seconds*

### Syntax Description

<i>seconds</i>	Number of seconds between user authentication refreshes, in seconds. Range is 10 to 4294967295.
----------------	---

### Command Default

The default refresh time is 1800 seconds (30 minutes).

### Command Modes

Global Configuration mode

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The <b>fault manager refresh-time</b> command was replaced with the <b>event manager refresh-time</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

### Usage Guidelines

EEM attempts to contact the AAA server and refresh the username reauthentication whenever the configured **refresh-time** expires.

### Task ID

Task ID	Operations
eem	read, write

### Examples

This example shows how to set the refresh time:

```
RP/0/0/CPU0:router(config)# event manager refresh-time 1900
```

## event manager run

To manually run an Embedded Event Manager (EEM) policy, use the **event manager run** command in EXEC mode.

**event manager run** *policy* [*argument* [... [*argument15* ]]]

### Syntax Description

<i>policy</i>	Name of the policy file.
[ <i>argument</i> [...[ <i>argument15</i> ]]]	Argument that you want to pass to the policy. The maximum number of arguments is 15.

### Command Default

No registered EEM policies are run.

### Command Modes

EXEC mode

### Command History

Release	Modification
Release 3.6.0	This command was introduced.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

### Usage Guidelines

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event manager run** command allows policies to be run manually.

You can query the arguments in the policy file by using the **TCL** command *event\_reqinfo*, as shown in this example:

```
array set arr_einfo [event_reqinfo] set argc $arr_einfo(argc) set arg1
    $arr_einfo(arg1)
```

Use the [event manager policy, on page 83](#) command to register the policy before using the **event manager run** command to run the policy. The policy can be registered with none as the event type.

### Task ID

Task ID	Operations
eem	read

## Examples

This example of the **event manager run** command shows how to manually run an EEM policy named `policy-manual.tcl`:

```
RP/0/0/CPU0:router# event manager run policy-manual.tcl parameter1 parameter2 parameter3
RP/0/0/CPU0:Sep 20 10:26:31.169 : user-plocy.tcl[65724]: The reqinfo of arg2 is parameter2.

RP/0/0/CPU0:Sep 20 10:26:31.170 : user-plocy.tcl[65724]: The reqinfo of argc is 3.
RP/0/0/CPU0:Sep 20 10:26:31.171 : user-plocy.tcl[65724]: The reqinfo of arg3 is parameter3.

RP/0/0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_type_string
is none.
RP/0/0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_pub_sec is
1190283990.
RP/0/0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_pub_time is
1190283990.
RP/0/0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_id is 3.
RP/0/0/CPU0:Sep 20 10:26:31.174 : user-plocy.tcl[65724]: The reqinfo of arg1 is parameter1.

RP/0/0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_type is 16.
RP/0/0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_pub_msec is
830
```

## Related Commands

Command	Description
<a href="#">event manager policy, on page 83</a>	Registers an EEM policy with the EEM.

# event manager scheduler suspend

To suspend the Embedded Event Manager (EEM) policy scheduling execution immediately, use the **event manager scheduler suspend** command in Global Configuration mode. To restore a system to its default condition, use the **no** form of this command.

**event manager scheduler suspend**

**no event manager scheduler suspend**

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

**Command Default** Policy scheduling is active by default.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.2	This command was introduced.
	Release 3.6.0	The <b>fault manager schedule-policy suspend</b> command was replaced with the <b>event manager scheduler suspend</b> command.
	Release 3.7.0	Task ID was changed from fault-mgr to eem.

**Usage Guidelines** Use the **event manager scheduler suspend** command to suspend all the policy scheduling requests, and do not perform scheduling until you enter the **no** form of this command. The **no** form of this command resumes policy scheduling and runs pending policies, if any.

It is recommended that you suspend policy execution immediately instead of unregistering policies one by one, for the following reasons:

- Security—If you suspect that the security of your system has been compromised.
- Performance—If you want to suspend policy execution temporarily to make more CPU cycles available for other functions.

Task ID	Task ID	Operations
	eem	read, write

## Examples

This example shows how to disable policy scheduling:

```
RP/0/0/CPU0:router(config)# event manager scheduler suspend
```

This example shows how to enable policy scheduling:

```
RP/0/0/CPU0:router(config)# no event manager scheduler suspend
```

## Related Commands

Command	Description
<a href="#">event manager policy</a> , on page 83	Registers an EEM policy with the EEM.

# show event manager directory user

To display the current value of the EEM user library files or user-defined Embedded Event Manager (EEM) policies, use the **show event manager directory user** command in EXEC mode.

**show event manager directory user** {library| policy}

## Syntax Description

<b>library</b>	Specifies the user library files.
<b>policy</b>	Specifies the user-defined EEM policies.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager userlibdirectory</b> and <b>show fault manager userpolicydirectory</b> commands were replaced with the <b>show event manager directory user</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

## Usage Guidelines

Use the **show event manager directory user** command to display the current value of the EEM user library or policy directory.

## Task ID

Task ID	Operations
eem	read

## Examples

This is a sample output of the **show event manager directory user** command:

```
RP/0/0/CPU0:router# show event manager directory user library
disk0:/fm_user_lib_dir
```

```
RP/0/0/CPU0:router# show event manager directory user policy
disk0:/fm_user_pol_dir
```



**Related Commands**

Command	Description
<a href="#">event manager directory user</a> , on page 79	Specifies the name of a directory that is to be used for storing either the user library or the policy files.

# show event manager environment

To display the names and values of the Embedded Event Manager (EEM) environment variables, use the **show event manager environment** command in EXEC mode.

**show event manager environment** [**all**| *environment-name*]

## Syntax Description

<b>all</b>	(Optional) Specifies all the environment variables.
<i>environment-name</i>	(Optional) Environment variable for which data is displayed.

## Command Default

All environment variables are displayed.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager environment</b> command was replaced with the <b>show event manager environment</b> command.

## Usage Guidelines

Use the **show event manager environment** command to display the names and values of the EEM environment variables.

## Task ID

Task ID	Operations
eem	read

## Examples

This is a sample output of the **show event manager environment** command:

```
RP/0/0/CPU0:router# show event manager environment
```

```

No.   Name                               Value
1     _email_cc                           mosnerd@cisco.com
2     _email_to                           mosnerd@cisco.com
3     _show_cmd                           show event manager policy registered
4     _cron_entry                         0-59/2 0-23/1 * * 0-7
5     _email_from                         mosnerd@cisco.com
6     _email_server                       zeta@cisco.com
```

This table describes the significant fields in the display.

**Table 8: show event manager environment Field Descriptions**

Field	Description
No.	Number of the EEM environment variable.
Name	Name of the EEM environment variable.
Value	Value of the EEM environment variable.

#### Related Commands

Command	Description
<a href="#">event manager environment</a> , on page 81	Specifies a directory to use for storing user library files.

# show event manager metric hardware

To display the Embedded Event Manager (EEM) reliability data for the processes running on a particular node, use the **show event manager metric hardware** command in EXEC mode.

**show event manager metric hardware location** {*node-id*| **all**}

## Syntax Description

<b>location</b>	Specifies the location of the node.
<i>node-id</i>	EEM reliability data for the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>all</b>	Specifies all the nodes.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager metric hardware</b> command was replaced with the <b>show event manager metric environment</b> command.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
eem	read

## Examples

This is a sample output of the **show event manager metric hardware** command:

```
RP/0/0/CPU0:router# show event manager metric hardware location 0/0/CPU0
=====
node: 0/0/CPU0
Most recent online: Mon Sep 10 21:45:02 2007
```

```
Number of times online: 1
Cumulative time online: 0 days, 09:01:07

Most recent offline: n/a
Number of times offline: 0
Cumulative time offline: 0 days, 00:00:00
```

This table describes the significant fields shown in the display.

**Table 9: show event manager metric hardware location Field Descriptions**

Field	Description
node	Node with processes running.
Most recent online	The last time the node was started.
Number of times online	Total number of times the node was started.
Cumulative time online	Total amount of time the node was available.
Most recent offline	The last time the process was terminated abnormally.
Number of times offline	Total number of times the node was terminated.
Cumulative time offline	Total amount of time the node was terminated.

#### Related Commands

Command	Description
show processes	Displays information about active processes.

# show event manager metric process

To display the Embedded Event Manager (EEM) reliability metric data for processes, use the **show event manager metric process** command in EXEC mode.

**show event manager metric process** {**all**|*job-id*|*process-name*} **location** {**all**|*node-id*}

Syntax Description

<b>all</b>	Specifies all the processes.
<i>job-id</i>	Process associated with this job identifier. The value ranges from 0-4294967295.
<i>process-name</i>	Process associated with this name.
<b>location</b>	Specifies the location of the node.
<b>all</b>	Displays hardware reliability metric data for all the nodes.
<i>node-id</i>	Hardware reliability metric data for a specified node. Displays detailed Cisco Express Forwarding information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager metric process</b> command was replaced with the <b>show event manager metric process</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

Usage Guidelines

The system maintains a record of when processes start and end. This data is used as the basis for reliability analysis.

Use the **show event manager metric process** command to obtain availability information for a process or group of processes. A process is considered available when it is running.

**Task ID**

Task ID	Operations
eeem	read

**Examples**

This is sample output from the **show event manager metric process** command:

```
RP/0/0/CPU0:router# show event manager metric process all location all

=====
job id: 88, node name: 0/4/CPU0
process name: wd-critical-mon, instance: 1
-----
last event type: process start
recent start time: Wed Sep 19 13:31:07 2007
recent normal end time: n/a
recent abnormal end time: n/a
number of times started: 1
number of times ended normally: 0
number of times ended abnormally: 0
most recent 10 process start times:
-----
Wed Sep 19 13:31:07 2007
-----

most recent 10 process end times and types:

cumulative process available time: 21 hours 1 minutes 31 seconds 46 milliseconds
cumulative process unavailable time: 0 hours 0 minutes 0 seconds 0 milliseconds
process availability: 1.000000000
number of abnormal ends within the past 60 minutes (since reload): 0
number of abnormal ends within the past 24 hours (since reload): 0
number of abnormal ends within the past 30 days (since reload): 0
=====
job id: 54, node name: 0/4/CPU0
process name: dllmgr, instance: 1
-----
last event type: process start
recent start time: Wed Sep 19 13:31:07 2007
recent normal end time: n/a
recent abnormal end time: n/a
number of times started: 1
number of times ended normally: 0
number of times ended abnormally: 0
most recent 10 process start times:
-----
Wed Sep 19 13:31:07 2007
-----

most recent 10 process end times and types:

cumulative process available time: 21 hours 1 minutes 31 seconds 41 milliseconds
cumulative process unavailable time: 0 hours 0 minutes 0 seconds 0 milliseconds
process availability: 1.000000000
number of abnormal ends within the past 60 minutes (since reload): 0
number of abnormal ends within the past 24 hours (since reload): 0
number of abnormal ends within the past 30 days (since reload): 0
This table describes the significant fields shown in the display.
```

**Table 10: show event manager metric process Field Descriptions**

Field	Description
job id	Number assigned as the job identifier.
node name	Node with the process running.
process name	Name of the process running on the node.
instance	Instance or thread of a multithreaded process.
comp id	Component of which the process is a member.
version	Specific software version or release of which the process is a member.
last event type	Last event type on the node.
recent end type	Most recent end type.
recent start time	Last time the process was started.
recent normal end time	Last time the process was stopped normally.
recent abnormal end time	Last time the process was terminated abnormally.
recent abnormal end type	Reason for the last abnormal process termination. For example, the process was aborted or crashed.
number of times started	Number of times the process has been started.
number of times ended normally	Number of times the process has been stopped normally.
number of times ended abnormally	Number of times the process has stopped abnormally.
most recent 10 process start times	Times of the last ten process starts.
cumulative process available time	Total time the process has been available.
cumulative process unavailable time	Total time the process has been out of service due to a restart, abort, communication problems, and so on.
process availability	Uptime percentage of the process (time running—the duration of any outage).
number of abnormal ends within the past 60 minutes	Number of times the process has stopped abnormally within the last 60 minutes.



Field	Description
number of abnormal ends within the past 24 hours	Number of times the process has stopped abnormally within the last 24 hours.
number of abnormal ends within the past 30 days	Number of times the process has stopped abnormally within the last 30 days.

**Related Commands**

Command	Description
show processes	Displays information about active processes.

# show event manager policy available

To display Embedded Event Manager (EEM) policies that are available to be registered, use the **show event manager policy available** command in EXEC mode.

**show event manager policy available** [system| user]

## Syntax Description

<b>system</b>	(Optional) Displays all the available system policies.
<b>user</b>	(Optional) Displays all the available user policies.

## Command Default

If this command is invoked with no optional keywords, it displays information for all available system and user policies.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager policy available</b> command was replaced with the <b>show event manager policy available</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

## Usage Guidelines

Use the **show event manager policy available** command to find out what policies are available to be registered just prior to using the **event manager policy** command to register policies.

This command is also useful if you forget the exact name of a policy that is required for the **event manager policy** command.

## Task ID

Task ID	Operations
eem	read

## Examples

This is a sample output of the **show event manager policy available** command:

```
RP/0/0/CPU0:router# show event manager policy available
```

No.	Type	Time Created	Name
1	system	Tue Jan 12 09:41:32 2004	pr_sample_cdp_abort.tcl
2	system	Tue Jan 12 09:41:32 2004	pr_sample_cdp_revert.tcl
3	system	Tue Jan 12 09:41:32 2004	sl_sample_intf_down.tcl
4	system	Tue Jan 12 09:41:32 2004	tm_sample_cli_cmd.tcl
5	system	Tue Jan 12 09:41:32 2004	tm_sample_crash_hist.tcl
6	system	Tue Jan 12 09:41:32 2004	wd_sample_proc_mem_used.tcl
7	system	Tue Jan 12 09:41:32 2004	wd_sample_sys_mem_used.tcl

This table describes the significant fields shown in the display.

**Table 11: show event manager policy available Field Descriptions**

Field	Description
No.	Number of the policy.
Type	Type of policy.
Time Created	Time the policy was created.
Name	Name of the policy.

#### Related Commands

Command	Description
<a href="#">event manager policy, on page 83</a>	Registers an EEM policy with the EEM.
<a href="#">show event manager policy registered, on page 104</a>	Displays the EEM policies that are already registered.

# show event manager policy registered

To display the Embedded Event Manager (EEM) policies that are already registered, use the **show event manager policy registered** command in EXEC mode.

**show event manager policy registered**[*event-type type*] [*system*| *user*] [*time-ordered*| *name-ordered*]

Syntax Description

<b>event-type <i>type</i></b>	(Optional) Displays the registered policies for a specific event type, where the valid <i>type</i> options are as follows: <ul style="list-style-type: none"> <li>• <b>application</b>—Application event type</li> <li>• <b>counter</b>—Counter event type</li> <li>• <b>hardware</b>—Hardware event type</li> <li>• <b>oir</b>—Online insertion and removal (OIR) event type</li> <li>• <b>process-abort</b>—Process abort event type</li> <li>• <b>process-start</b>—Process start event type</li> <li>• <b>process-term</b>—Process termination event type</li> <li>• <b>process-user-restart</b>—Process user restart event type</li> <li>• <b>process-user-shutdown</b>—Process user shutdown event type</li> <li>• <b>statistics</b>—Statistics event type</li> <li>• <b>syslog</b>—Syslog event type</li> <li>• <b>timer-absolute</b>—Absolute timer event type</li> <li>• <b>timer-countdown</b>—Countdown timer event type</li> <li>• <b>timer-cron</b>—Clock daemon (cron) timer event type</li> <li>• <b>timer-watchdog</b>—Watchdog timer event type</li> <li>• <b>wdsysmon</b>—Watchdog system monitor event type</li> </ul>
<b>system</b>	(Optional) Displays the registered system policies.
<b>user</b>	(Optional) Displays the registered user policies.
<b>time-ordered</b>	(Optional) Displays the policies according to registration time.
<b>name-ordered</b>	(Optional) Displays the policies in alphabetical order according to policy name.

Command Default

If this command is invoked with no optional keywords or arguments, it displays the registered EEM policies for all the event types. The policies are displayed according to the registration time.

**Command Modes**

EXEC mode

**Command History**

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager policy registered</b> command was replaced with the <b>show event manager policy registered</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

**Usage Guidelines**

The output of the **show event manager policy registered** command is most beneficial if you are writing and monitoring the EEM policies. The output displays registered policy information in two parts. The first line in each policy description lists the index number assigned to the policy, policy type (system or user), type of event registered, time at which the policy was registered, and name of the policy file. The remaining lines of each policy description display information about the registered event and how the event is to be handled, and come directly from the Tool Command Language (TCL) command arguments that make up the policy file.

Registered policy information is documented in the Cisco publication *Writing Embedded Event Manager Policies Using Tcl*.

**Task ID**

Task ID	Operations
eem	read

**Examples**

This is a sample output of the **show event manager policy registered** command:

```
RP/0/0/CPU0:router# show event manager policy registered

No.      Type      Event Type      Time Registered      Name
1        system    proc abort      Wed Jan 16 23:44:56 2004  test1.tcl
  version 00.00.0000 instance 1 path {cdp}
  priority normal maxrun_sec 20 maxrun_nsec 0
2        system    timer cron      Wed Jan 16 23:44:58 2004  test2.tcl
  name {crontimer1}
  priority normal maxrun_sec 20 maxrun_nsec 0
3        system    proc abort      Wed Jan 16 23:45:02 2004  test3.tcl
  path {cdp}
  priority normal maxrun_sec 20 maxrun_nsec 0
4        system    syslog          Wed Jan 16 23:45:41 2004  test4.tcl
  occurs 1 pattern {test_pattern}
  priority normal maxrun_sec 90 maxrun_nsec 0
5        system    timer cron      Wed Jan 16 23:45:12 2004  test5.tcl
  name {crontimer2}
  priority normal maxrun_sec 30 maxrun_nsec 0
6        system    wdsysmon        Wed Jan 16 23:45:15 2004  test6.tcl
  timewin_sec 120 timewin_nsec 0 sub1 mem_tot_used {node {localhost} op gt
  val 23000}
```

**show event manager policy registered**

```

priority normal maxrun_sec 40 maxrun_nsec 0
7      system wdsysmon      Wed Jan 16 23:45:19 2004      test7.tcl
timewin_sec 120 timewin_nsec 0 sub1 mem_proc {node {localhost} procname
{wdsysmon} op gt val 80 is_percent FALSE}
priority normal maxrun_sec 40 maxrun_nsec 0

```

This is the sample of a script that is signed by Cisco:

```

script      system timer watchdog      Off      Fri Apr 23 14:03:27 2010      script_signed_cisco.tcl

      name {clistimer} time 30.000
      nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu 2048 Dsig Cisco

```

This is the sample of a script that is signed by third party:

```

script      system timer watchdog      Off      Fri Apr 23 14:03:27 2010      script_signed.tcl
      name {clistimer} time 30.000
      nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu Trust Dsig
Tcl_trustpoint

```

This is the sample of a script that is verified against a configured checksum:

```

script      user timer watchdog      Off      Fri Apr 23 14:03:27 2010      test3_3rd_signed.tcl
      name {clistimer} time 30.000
      nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu none Cksm MD5

```

This is the sample of a script that is signed by a combination of security levels. If a SHA-1 or MD5 script is verified and registered, the checksum information displays as Cksm sha1 or Cksm md5. The following example shows a SHA-1 checksum signed by Tcl\_trustpoint:

```

script      user timer watchdog      Off      Fri Apr 23 14:03:27 2010      test3_3rd_signed.tcl
      name {clistimer} time 30.000
      nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Cksm sha1 Dsig Tcl_trustpoint

```

This table describes the significant fields displayed in the example.

**Table 12: show event manager policy registered Field Descriptions**

Field	Description
No.	Number of the policy.
Type	Type of policy.
Event Type	Type of the EEM event for which the policy is registered.
Time Registered	Time at which the policy was registered.
Name	Name of the policy.

**Related Commands**

Command	Description
<a href="#">event manager policy</a> , on page 83	Registers an EEM policy with the EEM.

# show event manager refresh-time

To display the time between the user authentication refreshes in the Embedded Event Manager (EEM), use the **show event manager refresh-time** command in EXEC mode.

**show event manager refresh-time**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.3.0	This command was introduced.
	Release 3.6.0	The <b>show fault manager refresh-time</b> command was replaced with the <b>show event manager refresh-time</b> command.
	Release 3.7.0	Task ID was changed from fault-mgr to eem.


**Usage Guidelines** The output of the **show event manager refresh-time** command is the refresh time, in seconds.

Task ID	Task ID	Operations
	eem	read

**Examples** This is a sample output of the **show event manager refresh-time** command:

```
RP/0/0/CPU0:router# show event manager refresh-time
Output:
1800 seconds
```

Related Commands	Command	Description
	<a href="#">event manager refresh-time, on page 87</a>	Specifies the time between the system attempts to contact the AAA server, and refreshes the username reauthentication.

 **show event manager refresh-time**



# show event manager statistics-table

To display the currently supported statistic counters maintained by the Statistic Event Detector, use the **show event manager statistics-table** command in EXEC mode.

**show event manager statistics-table** *{stats-name| all}*

## Syntax Description

<i>stats-name</i>	Specific statistics type to be displayed. There are three statistics types: <ul style="list-style-type: none"><li>• generic (ifstats-generic)</li><li>• interface table (ifstats-iftable)</li><li>• data rate (ifstats-datarate)</li></ul>
<b>all</b>	Displays the possible values for the <i>stats-name</i> argument. Displays the output for all the statistics types.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.6.0	The <b>show fault manager statistics-table</b> command was replaced with the <b>show event manager statistics-table</b> command.
Release 3.7.0	Task ID was changed from fault-mgr to eem.

## Usage Guidelines

Use the **show event manager statistics-table all** command to display the output for all the statistics types.

## Task ID

Task ID	Operations
eem	read

**Examples**

This is a sample output of the **show event manager statistics-table all** command:

```
RP/0/0/CPU0:router# show event manager statistics-table all
```

Name	Type	Description
ifstats-generic	bag	Interface generic stats
ifstats-iftable	bag	Interface iftable stats
ifstats-datarate	bag	Interface datarate stats

This is a sample output providing more detailed information on the ifstats-iftable interface statistics table:

```
RP/0/0/CPU0:router# show event manager statistics-table ifstats-iftable
```

Name	Type	Description
PacketsReceived	uint64	Packets rcvd
BytesReceived	uint64	Bytes rcvd
PacketsSent	uint64	Packets sent
BytesSent	uint64	Bytes sent
MulticastPacketsReceived	uint64	Multicast pkts rcvd
BroadcastPacketsReceived	uint64	Broadcast pkts rcvd
MulticastPacketsSent	uint64	Multicast pkts sent
BroadcastPacketsSent	uint64	Broadcast pkts sent
OutputDropsCount	uint32	Total output drops
InputDropsCount	uint32	Total input drops
InputQueueDrops	uint32	Input queue drops
RuntPacketsReceived	uint32	Received runt packets
GiantPacketsReceived	uint32	Received giant packets
ThrottledPacketsReceived	uint32	Received throttled packets
ParityPacketsReceived	uint32	Received parity packets
UnknownProtocolPacketsReceived	uint32	Unknown protocol pkts rcvd
InputErrorsCount	uint32	Total input errors
CRCErrorCount	uint32	Input crc errors
InputOverruns	uint32	Input overruns
FramingErrorsReceived	uint32	Framing-errors rcvd
InputIgnoredPackets	uint32	Input ignored packets
InputAborts	uint32	Input aborts
OutputErrorsCount	uint32	Total output errors
OutputUnderruns	uint32	Output underruns
OutputBufferFailures	uint32	Output buffer failures
OutputBuffersSwappedOut	uint32	Output buffers swapped out
Applique	uint32	Applique
ResetCount	uint32	Number of board resets
CarrierTransitions	uint32	Carrier transitions
AvailabilityFlag	uint32	Availability bit mask
NumberOfSecondsSinceLastClearCounters	uint32	Seconds since last clear counters
LastClearTime	uint32	SysUpTime when counters were last cleared (in seconds)

This table describes the significant fields displayed in the example.

**Table 13: show event manager statistics-table Field Descriptions**

Field	Description
Name	<p>Name of the statistic.</p> <p>When the <b>all</b> keyword is specified, there are three types of statistics displayed:</p> <ul style="list-style-type: none"><li>• ifstats-generic</li><li>• ifstats-itable</li><li>• ifstats-datarate</li></ul> <p>When a statistics type is specified, the statistics for the statistic type are displayed.</p>
Type	Type of statistic.
Description	Description of the statistic.

**Related Commands**

Command	Description
<a href="#">event manager policy, on page 83</a>	Registers an EEM policy with the EEM.

show event manager statistics-table



## IP Service Level Agreement Commands

---

This module describes the Cisco IOS XR software commands to configure IP Service Level Agreements (IP SLAs) 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.

For detailed information about IP SLA concepts, configuration tasks, and examples, see the *Implementing IP Service Level Agreements* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [access-list](#), page 117
- [action \(IP SLA\)](#), page 119
- [ageout](#), page 121
- [buckets \(history\)](#), page 123
- [buckets \(statistics hourly\)](#), page 125
- [buckets \(statistics interval\)](#), page 127
- [control disable](#), page 128
- [datasize request](#), page 130
- [destination address \(IP SLA\)](#), page 132
- [destination port](#), page 134
- [distribution count](#), page 136
- [distribution interval](#), page 138
- [exp](#), page 140
- [filter](#), page 142
- [force explicit-null](#), page 144
- [frequency \(IP SLA\)](#), page 146
- [history](#), page 148
- [interval](#), page 150

- [ipsla, page 152](#)
- [key-chain, page 154](#)
- [life, page 156](#)
- [lives, page 158](#)
- [low-memory, page 160](#)
- [lsp selector ipv4, page 162](#)
- [lsr-path, page 164](#)
- [maximum hops, page 166](#)
- [maximum paths \(IP SLA\), page 168](#)
- [monitor, page 170](#)
- [mpls discovery vpn, page 172](#)
- [mpls lsp-monitor, page 174](#)
- [operation, page 176](#)
- [output interface, page 177](#)
- [output nexthop, page 179](#)
- [packet count, page 181](#)
- [packet interval, page 183](#)
- [path discover, page 185](#)
- [path discover echo, page 186](#)
- [path discover path, page 188](#)
- [path discover scan, page 190](#)
- [path discover session, page 192](#)
- [react, page 194](#)
- [react lpd, page 197](#)
- [reaction monitor, page 199](#)
- [reaction operation, page 201](#)
- [reaction trigger, page 203](#)
- [responder, page 205](#)
- [recurring, page 206](#)
- [reply dscp, page 207](#)
- [reply mode, page 209](#)
- [responder twamp, page 211](#)
- [scan delete-factor, page 212](#)

- [scan interval, page 214](#)
- [schedule monitor, page 216](#)
- [schedule operation, page 218](#)
- [schedule period, page 220](#)
- [server twamp, page 222](#)
- [show ipsla application, page 223](#)
- [show ipsla history, page 225](#)
- [show ipsla mpls discovery vpn, page 228](#)
- [show ipsla mpls lsp-monitor lpd, page 230](#)
- [show ipsla mpls lsp-monitor scan-queue, page 232](#)
- [show ipsla mpls lsp-monitor summary, page 234](#)
- [show ipsla responder statistics, page 237](#)
- [show ipsla statistics, page 239](#)
- [show ipsla statistics aggregated, page 242](#)
- [show ipsla statistics enhanced aggregated, page 251](#)
- [show ipsla twamp connection, page 254](#)
- [show ipsla twamp session, page 255](#)
- [show ipsla twamp standards, page 256](#)
- [source address , page 257](#)
- [source port , page 259](#)
- [start-time , page 261](#)
- [statistics, page 264](#)
- [tag \(IP SLA\), page 267](#)
- [target ipv4, page 269](#)
- [target pseudowire, page 271](#)
- [target traffic-eng , page 273](#)
- [threshold, page 275](#)
- [threshold type average, page 277](#)
- [threshold type consecutive, page 279](#)
- [threshold type immediate, page 281](#)
- [threshold type xofy, page 283](#)
- [timeout \(IP SLA\), page 285](#)
- [tos, page 287](#)

- [ttl](#), page 289
- [type icmp echo](#), page 291
- [type icmp path-echo](#), page 292
- [type icmp path-jitter](#), page 293
- [type mpls lsp ping](#), page 294
- [type mpls lsp trace](#), page 296
- [type udp echo](#), page 298
- [type udp jitter](#), page 299
- [type udp ipv4 address](#), page 300
- [verify-data](#), page 302
- [vrf \(IP SLA\)](#), page 304
- [vrf \(IP SLA MPLS LSP monitor\)](#), page 306



# access-list

To specify an access-list name to filter provider edge (PE) addresses to restrict operations that are automatically created by MPLS LSP monitor (MPLSLM) instance, use the **access-list** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**access-list** *acl-name*

**no access-list**

## Syntax Description

<i>acl-name</i>	Filters an access-list name.
-----------------	------------------------------

## Command Default

No access list is configured by default.

## Command Modes

IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

Access-list changes are processed before the scan interval expires to display a planned list of changes in the scan-queue.



### Note

There is no verification check between the access list and the IPSLA configuration.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **access-list** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
```

```
RP/0/0/CPU0:router(config-ipsla-mpls-lm-def)# type mpls lsp ping  
RP/0/0/CPU0:router(config-ipsla-mpls-lm-lsp-ping)# access-list ipsla
```

**Related Commands**

Command	Description
<a href="#">scan interval, on page 214</a>	Specifies the frequency at which the MPLS LSP monitor instance checks the scan queue for updates.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

## action (IP SLA)

To specify what action or combination of actions the operation performs when you configure the **react** command or when threshold events occur, use the **action** command in the appropriate configuration mode. To clear action or combination of actions (no action can happen), use the **no** form of this command.

**action** {**logging**| **trigger**}

**no action** {**logging**| **trigger**}

### Syntax Description

<b>logging</b>	Sends a logging message when the specified violation type occurs for the monitored element. The IP SLA agent generates a syslog and informs SNMP. Then, it is up to the SNMP agent to generate a trap or not.
<b>trigger</b>	Determines that the operation state of one or more target operations makes the transition from pending to active when the violation conditions are met. The target operations to be triggered are specified using the <b>ipsla reaction trigger</b> command. A target operation continues until its life expires, as specified by the lifetime value of the target operation. A triggered target operation must finish its life before it can be triggered again.

### Command Default

None

### Command Modes

IP SLA reaction condition configuration  
IP SLA MPLS LSP monitor reaction configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor reaction configuration mode.

### Usage Guidelines

For the **action** command to occur for threshold events, the threshold type must be defined. Absence of threshold type configuration is considered if the threshold check is not activated.

When the **action** command is used from IP SLA MPLS LSP monitor reaction configuration mode, only the **logging** keyword is available.

If the **action** command is used in IP SLA operation mode, the action defined applies to the specific operation being configured. If the **action** command is used in IP SLA MPLS LSP monitor mode, the action defined applies to all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **action** command with the **logging** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/0/CPU0:router(config-ipsla-react-cond)# action logging
```

The following example shows how to use the **action** command from the IP SLA MPLS LSP monitor reaction configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# reaction monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-react)# react connection-loss
RP/0/0/CPU0:router(config-ipsla-mplslm-react-cond)# action logging
```

**Related Commands**

Command	Description
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction monitor, on page 199</a>	Configures MPLS LSP monitoring reactions.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.

# ageout

To specify the number of seconds to keep the operation in memory when it is not actively collecting information, use the **ageout** command in IP SLA schedule configuration mode. To use the default value so that the operation will never age out, use the **no** form of this command.

**ageout** *seconds*

**no ageout**

## Syntax Description

<i>seconds</i>	Age-out interval in seconds. The value 0 seconds means that the collected data is not aged out. Range is 0 to 2073600.
----------------	--

## Command Default

The default value is 0 seconds (never aged out).

## Command Modes

IP SLA schedule configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **ageout** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/0/CPU0:router(config-ipsla-sched)# ageout 3600
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.

Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## buckets (history)

To set the number of history buckets that are kept during the lifetime of the IP SLA operation, use the **buckets** command in IP SLA operation history configuration mode. To use the default value, use the **no** form of this command.

**buckets** *buckets*

**no buckets**

### Syntax Description

<i>buckets</i>	Number of history buckets that are kept during the lifetime of an IP SLA operation. Range is 1 to 60.
----------------	---

### Command Default

The default value is 15 buckets.

### Command Modes

IP SLA operation history configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

The **buckets** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo
- IP SLA UDP echo

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **buckets** command in IP SLA UDP echo configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/0/CPU0:router(config-ipsla-op-hist)# buckets 30
```

**Related Commands**

Command	Description
<a href="#">history, on page 148</a>	Configures the history parameters for the IP SLA operation.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# buckets (statistics hourly)

To set the number of hours for which statistics are kept, use the **bucket** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**buckets** *hours*

**no buckets**

## Syntax Description

<i>hours</i>	Number of hours for which statistics are maintained for the IP SLA operations. Range is 0 to 25 in IP SLA operation statistics configuration mode, and 0 to 2 in IP SLA MPLS LSP monitor statistics configuration mode.
--------------	---

## Command Default

The default value is 2.

## Command Modes

IP SLA operation statistics configuration  
IP SLA MPLS LSP monitor statistics configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor statistics configuration mode.

## Usage Guidelines

The **buckets** command with the *hours* argument is valid only for the **statistics** command with the **hourly** keyword.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA UDP jitter operation for the **buckets** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
```

```
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly  
RP/0/0/CPU0:router(config-ipsla-op-stats)# buckets 10
```

**Related Commands**

Command	Description
<a href="#">statistics</a> , <a href="#">on page 264</a>	Sets the statistics collection parameters for the operation.

## buckets (statistics interval)

To specify the maximum number of buckets in which the enhanced history statistics are kept, use the **buckets** command in IP SLA operation statistics configuration mode. To remove the statistics collection of the specified interval, use the **no** form of this command.

**buckets** *bucket-size*

**no buckets**

### Syntax Description

*bucket-size*

The bucket size is when the configured bucket limit is reached. Therefore, statistics gathering for the operation ends. Range is 1 to 100. Default is 100.

### Command Default

The default value is 100.

### Command Modes

IP SLA operation statistics configuration

### Command History

#### Release

#### Modification

Release 3.3.0

This command was introduced.

### Usage Guidelines

The **buckets** command with the *bucket-size* argument is valid only for the **statistics** command with the **interval** keyword.

### Examples

The following example shows how to collect statistics for a given time interval for the IP SLA UDP jitter operation for the **buckets** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/0/CPU0:router(config-ipsla-op-stats)# buckets 50
```

### Related Commands

Command	Description
<a href="#">statistics</a> , <a href="#">on page 264</a>	Sets the statistics collection parameters for the operation.

# control disable

To disable the control packets, use the **control disable** command in the appropriate configuration mode. To use the control packets again, use the **no** form of this command.

**control disable**

**no control disable**

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

**Command Default** Control packets are enabled by default.

**Command Modes** IP SLA UDP echo configuration  
IP SLA UDP jitter configuration

Release	Modification
Release 3.3.0	This command was introduced.

**Usage Guidelines** When you configure the **control disable** command on the agent side, you need to configure a permanent port on the responder side or the operation returns a timeout error. If you configure the **control disable** command, a permanent port of the IP SLA Responder or some other functionality, such as the UDP echo server, is required on the remote device.

The **control disable** command is valid for operations that require a responder.

The IP SLA control protocol is disabled, which is used to send a control message to the IP SLA Responder prior to sending an operation packet. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA Responder.

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to use the **control disable** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
```

```
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter  
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# control disable
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## datasize request

To set the protocol data size in the request packet in the payload of an operation, use the **datasize request** command in the appropriate configuration mode. To reset the default data size, use the **no** form of this command.

**datasize request** *size*

**no datasize request**

### Syntax Description

<i>size</i>	Specifies the following ranges and default values that are protocol dependent: <ul style="list-style-type: none"> <li>• For a UDP jitter operation, range is 16 to 1500 B.</li> <li>• For a UDP echo operation, range is 4 to 1500 B.</li> <li>• For an ICMP echo operation, range is 0 to 16384 B.</li> <li>• For an ICMP path-echo operation, range is 0 to 16384 B.</li> <li>• For an ICMP path-jitter operation, range is 0 to 16384 B.</li> <li>• For an MPLS LSP ping operation, range is 100 to 17986 B.</li> </ul>
-------------	--

### Command Default

For a UDP jitter operation, the default value is 32 B.  
 For a UDP echo operation, the default value is 16 B.  
 For an ICMP echo operation, the default value is 36 B.  
 For an ICMP path-echo operation, the default value is 36 B.  
 For an ICMP path-jitter operation, the default value is 36 B.  
 For an MPLS LSP ping operation, the default value is 100 B.

### Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA MPLS LSP ping configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

Release	Modification
Release 3.4.0	Support was added for IP SLA MPLS LSP ping configuration mode.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping configuration mode.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **datasize request** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# datasize request 512
```

**Related Commands**

Command	Description
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type icmp echo, on page 291</a>	Configures an IP SLA ICMP echo operation.
<a href="#">type icmp path-echo, on page 292</a>	Configures an IP SLA ICMP path-echo operation.
<a href="#">type icmp echo, on page 291</a>	Configures an IP SLA ICMP echo operation.
<a href="#">type icmp path-echo, on page 292</a>	Configures an IP SLA ICMP path-echo operation.
<a href="#">type icmp path-jitter, on page 293</a>	Configures an IP SLA ICMP path-jitter operation.
<a href="#">type udp jitter, on page 299</a>	Configures an IP SLA UDP jitter operation.

## destination address (IP SLA)

To identify the address of the target device, use the **destination address** command in the appropriate configuration mode. To unset the destination address, use the **no** form of this command.

**destination address** *ipv4-address*

**no destination address**

### Syntax Description

<i>ipv4-address</i>	IP address of the target device.
---------------------	----------------------------------

### Command Default

None

### Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

You must specify the address of the target device. The configuration for the **destination address** command is mandatory for all operations.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to designate an IP address for the **destination address** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# destination address 192.0.2.12
```



**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## destination port

To identify the port of the target device, use the **destination port** command in the appropriate configuration mode. To unset the destination port, use the **no** form of this command.

**destination port** *port*

**no destination port**

### Syntax Description

<i>port</i>	Port number of the target device. Range is 1 to 65535.
-------------	--

### Command Default

None

### Command Modes

IP SLA UDP echo configuration  
IP SLA UDP jitter configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

The **destination port** command is not supported when you configure an ICMP operation; it is supported only to configure UDP operations.

You must specify the port of the target device. The configuration for the **destination port** command is mandatory for both IP SLA UDP echo and IP SLA UDP jitter configurations.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to designate a port for the **destination port** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# destination port 11111
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## distribution count

To set the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation, use the **distribution count** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

**distribution count** *slot*

**no distribution count**

### Syntax Description

slot	Number of statistics distributions that are kept. Range is 1 to 20. Default is 1.
------	---

### Command Default

The default value is 1.

### Command Modes

IP SLA operation statistics configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the statistics distributions interval, use the **distribution interval** command in IP SLA operation statistics configuration mode. The total number of statistics distributions captured is the value set by the **distribution count** command times the value set by the **maximum hops** command times the value set by the **maximum path** command times the value set by the **buckets** command.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to set the number of statistics distribution for the **distribution count** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-op-stats)# distribution count 15
```

**Related Commands**

Command	Description
<a href="#">buckets (statistics hourly), on page 125</a>	Sets the number of hours in which statistics are kept.
<a href="#">distribution interval, on page 138</a>	Sets the time interval (in milliseconds) for each statistical distribution.
<a href="#">maximum hops, on page 166</a>	Sets the number of hops in which statistics are maintained for each path for the IP SLA operation.
<a href="#">maximum paths (IP SLA), on page 168</a>	Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation.
<a href="#">statistics, on page 264</a>	Sets the statistics collection parameters for the operation.

# distribution interval

To set the time interval (in milliseconds) for each statistical distribution, use the **distribution interval** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

**distribution interval** *interval*

**no distribution interval**

## Syntax Description

<i>interval</i>	Number of milliseconds used for each statistics distribution that is kept. Range is 1 to 100. Default is 20.
-----------------	--

## Command Default

The default value is 20.

## Command Modes

IP SLA operation statistics configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the statistics distributions count, use the **distribution count** command in IP SLA operation statistics configuration mode. The total number of statistics distributions captured is the value set by the **distribution count** command times the value set by the **maximum hops** command times the value set by the **maximum path** command times the value set by the **buckets** command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to set the time interval for the **distribution interval** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-op-stats)# distribution interval 50
```

**Related Commands**

Command	Description
<a href="#">buckets (statistics hourly), on page 125</a>	Sets the number of hours in which statistics are kept.
<a href="#">distribution count, on page 136</a>	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
<a href="#">maximum hops, on page 166</a>	Sets the number of hops in which statistics are maintained for each path for the IP SLA operation.
<a href="#">maximum paths (IP SLA), on page 168</a>	Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation.
<a href="#">statistics, on page 264</a>	Sets the statistics collection parameters for the operation.

## exp

To specify the MPLS experimental field (EXP) value in the header of echo request packets, use the **exp** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**exp** *exp-bits*

**no exp**

### Syntax Description

<i>exp-bits</i>	Experimental field value in the header of an echo request packet. Valid values are from 0 to 7. Default is 0.
-----------------	---

### Command Default

The experimental field value is set to 0.

### Command Modes

IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

### Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to the IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

### Usage Guidelines

Use the **exp** command to set the MPLS experimental field in the headers of echo request packets in an MPLS LSP ping or MPLS LSP trace operation. The experimental (EXP) field allows for eight different quality-of-service (QoS) markings that determine the treatment (per-hop behavior) that a transit LSR node gives to a request packet. You can configure different MPLS EXP levels for different operations to create differentiated levels of response.

If the **exp** command is used in IP SLA operation mode, it acts on the headers of echo request packets for the specific operation being configured. If the **exp** command is used in IP SLA MPLS LSP monitor mode, it acts on the headers of echo request packets for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.



**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **exp** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# exp 5
```

The following example shows how to use the **exp** command in MPLS LSP monitor mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-trace)# exp 5
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# filter

To define the type of information that are kept in the history table for the IP SLA operation, use the **filter** command in IP SLA operation history configuration mode. To unset the history filter, use the **no** form of this command.

**filter** {**all**| **failures**}

**no filter**

## Syntax Description

<b>all</b>	Stores history data for all operations, if set.
<b>failures</b>	Stores data for operations that failed, if set.

## Command Default

The default is not to collect the history unless the **filter** command is enabled.

## Command Modes

IP SLA operation history configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **filter** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo
- IP SLA UDP echo

If you use the **no** form of the **filter** command, the history statistics are not collected.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **filter** command in IP SLA UDP echo configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
```

```
RP/0/0/CPU0:router(config-ipsla)# operation 1  
RP/0/0/CPU0:router(config-ipsla-op)# type udp echo  
RP/0/0/CPU0:router(config-ipsla-udp-echo)# history  
RP/0/0/CPU0:router(config-ipsla-op-hist)# filter all
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# force explicit-null

To add an explicit null label to the label stack of an LSP when an echo request is sent, use the **force explicit-null** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**force explicit-null**

**no force explicit-null**

## Syntax Description

This command has no keywords or arguments.

## Command Default

An explicit null label is not added.

## Command Modes

IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

## Usage Guidelines

Use the **force explicit-null** command to force an unsolicited explicit null label to be added to the MPLS label stack of the LSP when an echo request packet is sent in an MPLS LSP ping or MPLS LSP trace operation.

If the **force explicit-null** command is used in IP SLA operation mode, it acts on the label stack of the LSP for the specific operation being configured. If the **force explicit-null** command is used in IP SLA MPLS LSP monitor mode, it acts on the label stack of all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

You cannot use the **force explicit-null** command if pseudowire is specified as the target to be used in an MPLS LSP ping operation.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **force explicit-null** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# force explicit-null
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

## frequency (IP SLA)

To set the frequency for probing, use the **frequency** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**frequency** *seconds*

**no frequency**

### Syntax Description

<i>seconds</i>	Rate at which the specific IP SLA operation is sent into the network. Range is 1 to 604800.
----------------	---

### Command Default

If the **frequency** command is not used, the default value is 60 seconds.

In IP SLA MPLS LSP monitor schedule configuration mode, the default value is equal to the schedule period that is set using the **schedule period** command.

### Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor schedule configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	Support was added for IP SLA MPLS ping and IP SLA MPLS trace configuration modes.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor schedule configuration mode.

### Usage Guidelines

If this command is used in IP SLA MPLS LSP monitor schedule configuration mode, it represents the frequency for the schedule period. In other words, if the frequency is set to 1000 seconds and the schedule period is set to 600 seconds, every 1000 seconds the LSP operations are run. Each run takes 600 seconds. Use the **schedule period** command to specify the schedule period.

The frequency value must be greater than or equal to the schedule period.

This configuration is inherited automatically by all LSP operations that are created.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **frequency** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# frequency 300
```

The following example shows how to use the **frequency** command in IP SLA MPLS LSP monitor schedule configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# schedule monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-sched)# frequency 1200
RP/0/0/CPU0:router(config-ipsla-mplslm-sched)# schedule period 600
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">schedule period, on page 220</a>	Configures the amount of time during which all LSP operations are scheduled to start or run.

# history

To configure the history parameters for the IP SLA operation, use the **history** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**history** [**buckets** *buckets* | **filter** {**all** | **failures**} | **lives** *lives*]

**no history**

## Syntax Description

<b>buckets</b>	Sets the number of history buckets that are kept during the lifetime of the IP SLA operation.
<i>buckets</i>	Number of history buckets that are kept during the lifetime of an IP SLA operation. Range is 1 to 60.
<b>filter</b>	Defines the type of information that is kept in the history table for the IP SLA operation.
<b>all</b>	Stores history data for all operations, if set.
<b>failures</b>	Stores data for operations that failed, if set.
<b>lives</b>	Sets the number of lives that are maintained in the history table for an IP SLA operation.
<i>lives</i>	Number of lives that are maintained in the history table for an IP SLA operation. Range is 0 to 2.

## Command Default

None

## Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.



Release	Modification
Release 3.4.0	Support was added for IP SLA MPLS LSP ping and IP SLA MPLS LSP trace configuration modes.

**Usage Guidelines**

The **history** command enters IP SLA operation history configuration mode in which you can configure more history configuration parameters.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **history** command in IP SLA UDP echo configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/0/CPU0:router(config-ipsla-op-hist)#
```

**Related Commands**

Command	Description
<a href="#">buckets (history), on page 123</a>	Sets the number of history buckets that are kept during the lifetime of the IP SLA operation.
<a href="#">filter, on page 142</a>	Defines the type of information that are kept in the history table for the IP SLA operation.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">lives, on page 158</a>	Sets the number of lives that are maintained in the history table for an IP SLA operation.

# interval

To configure the refresh interval for MPLS label switched path (LSP) monitoring, use the **interval** command in IP SLA MPLS discovery VPN configuration mode. To use the default value, use the **no** form of this command.

**interval** *refresh-interval*

**no interval**

## Syntax Description

<i>refresh-interval</i>	Specifies the time interval, in minutes, after which routing entries that are no longer valid are removed from the Layer 3 VPN discovery database. Range is 30 to 70560.
-------------------------	--

## Command Default

The default refresh interval is 60 minutes.

## Command Modes

IP SLA MPLS discovery VPN configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

### Note

If the total number of routes is large, there is a negative impact on the performance during the refresh of the discovery database. Therefore, the value of the *refresh-interval* argument should be large enough that router performance is not affected. If there are a very large number of routes, we recommend that you set the value of the *refresh-interval* argument to be several hours.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **interval** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
```

```
RP/0/0/CPU0:router(config-ipsla)# mpls discovery vpn  
RP/0/0/CPU0:router(config-ipsla-mpls-discovery-vpn)# interval 120
```

**Related Commands**

Command	Description
<a href="#">mpls discovery vpn, on page 172</a>	Configures MPLS label switched path (LSP) provider edge (PE) router discovery.
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.

# ipsla

To enter IP SLA configuration mode and configure IP Service Level Agreements, use the **ipsla** command in Global Configuration mode. To return to the default setting, use the **no** form of this command.

**ipsla**

**no ipsla**

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

**Command Default** None

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

**Usage Guidelines** The **ipsla** command enters IP SLA configuration mode where you can configure the various IP service level agreement options.

Task ID	Task ID	Operations
	monitor	read, write

**Examples** The following example shows how to enter IP SLA configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)#
```

## Related Commands

Command	Description
<a href="#">key-chain, on page 154</a>	Configures MD5 authentication for IP SLA control messages.
<a href="#">low-memory, on page 160</a>	Configures a low-water memory mark.

Command	Description
<a href="#">mpls discovery vpn, on page 172</a>	Configures MPLS label switched path (LSP) provider edge (PE) router discovery.
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">reaction trigger, on page 203</a>	Defines a second IP SLA operation to make the transition from a pending state to an active state when one of the trigger-type options is defined with the <b>reaction operation</b> command.
<a href="#">responder, on page 205</a>	Enables the IP SLA responder for UDP echo or jitter operations.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# key-chain

To configure the MD5 authentication for the IP SLA control message, use the **key-chain** command in IP SLA configuration mode. To unset the keychain name and not use MD5 authentication, use the **no** form of this command.

**key-chain** *key-chain-name*

**no key-chain**

## Syntax Description

<i>key-chain-name</i>	Name of the keychain.
-----------------------	-----------------------

## Command Default

No default values are defined. No authentication is used.

## Command Modes

IP SLA configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

When you configure the **key-chain** command, you must also configure the **key chain** command in global configuration mode to provide MD5 authentication.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **ipsla key-chain** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# key-chain ipsla-keys
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# life

To specify the length of time to execute, use the **life** command in IP SLA schedule configuration mode. To use the default value, use the **no** form of this command.

**life** {**forever**| *seconds*}

**no life**

## Syntax Description

<b>forever</b>	Schedules the operation to run indefinitely.
<i>seconds</i>	Determines the number of seconds the operation actively collects information. Range is 1 to 2147483647. Default value is 3600 seconds (one hour).

## Command Default

The default value is 3600 seconds.

## Command Modes

IP SLA schedule configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **life** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/0/CPU0:router(config-ipsla-sched)# life forever
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.



Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# lives

To set the number of lives that are maintained in the history table for an IP SLA operation, use the **lives** command in IP SLA operation history configuration mode. To use the default value, use the **no** form of this command.

**lives** *lives*

**no** lives

## Syntax Description

<i>lives</i>	Number of lives that are maintained in the history table for an IP SLA operation. Range is 0 to 2.
--------------	--

## Command Default

The default value is 0 lives.

## Command Modes

IP SLA operation history configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **lives** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo
- IP SLA UDP echo

If you use the **no** form of the **lives** command, the history statistics are not collected.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **lives** command in IP SLA UDP echo configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp echo
```

```
RP/0/0/CPU0:router(config-ipsla-udp-echo)# history  
RP/0/0/CPU0:router(config-ipsla-op-hist)# lives 2
```

**Related Commands**

Command	Description
<a href="#">buckets (history), on page 123</a>	Sets the number of history buckets that are kept during the lifetime of the IP SLA operation.
<a href="#">filter, on page 142</a>	Defines the type of information that are kept in the history table for the IP SLA operation.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# low-memory

**low-memory** *value*

**no low-memory**

## Syntax Description

<i>value</i>	Low-memory watermark value. Range is 0 to 4294967295.
--------------	---

## Command Default

The default value is 20 MB (free memory).

## Command Modes

IP SLA configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

IP SLA ensures that the system provides the specified memory before adding new operations or scheduling the pending operation.

When the 0 value is used, no memory limitation is enforced.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **low-memory** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# low-memory 102400
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">show ipsla application</a> , on page 223	Displays the information for the IP SLA application.



# lsp selector ipv4

To specify the local host IPv4 address used to select an LSP, use the **lsp selector ipv4** command in the appropriate configuration mode. To clear the host address, use the **no** form of this command.

**lsp selector ipv4** *ip-address*

**no lsp selector ipv4**

## Syntax Description

<i>ip-address</i>	A local host IPv4 address used to select the LSP.
-------------------	---

## Command Default

The local host IP address used to select the LSP is 127.0.0.1.

## Command Modes

IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

## Usage Guidelines

Use the **lsp selector ipv4** command to force an MPLS LSP ping or MPLS LSP trace operation to use a specific LSP when there are multiple equal cost paths between provider edge (PE) routers. This situation occurs when transit label switching routers (LSRs) use the destination address in IP packet headers for load balancing.

The IPv4 address configured with the **lsp selector ipv4** command is the destination address in the User Datagram Protocol (UDP) packet sent as the MPLS echo request. Valid IPv4 addresses are defined in the subnet 127.0.0.0/8 and used to:

- Force the packet to be consumed by the router where an LSP breakage occurs.
- Force processing of the packet at the terminal point of the LSP if the LSP is intact.
- Influence load balancing during forwarding when the transit routers use the destination address in the IP header for load balancing.

If the **lsp selector ipv4** command is used in IP SLA operation mode, it acts on the MPLS echo requests for the specific operation being configured. If the **lsp selector ipv4** command is used in IP SLA MPLS LSP

monitor mode, it acts on the MPLS echo requests for all operations associated with the monitored provider edge (PE) routers.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **lsp selector ipv4** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# lsp selector ipv4 127.10.10.1
```

### Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# lsr-path

To specify a loose source routing path in which to measure the ICMP, use the **lsr-path** command in the appropriate configuration mode. To use a path other than the specified one, use the **no** form of this command.

**lsr-path** *ipaddress1* [*ipaddress2* [... [*ipaddress8*]]]

**no** lsr-path

## Syntax Description

<i>ip address</i>	IPv4 address of the intermediate node. Up to eight addresses can be entered.
-------------------	--

## Command Default

No path is configured.

## Command Modes

IP SLA ICMP path-jitter configuration  
IP SLA ICMP path-echo configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **lsr-path** command applies only to ICMP path-echo and ICMP path-jitter operation types. You can configure up to a maximum of eight hop addresses by using the **lsr-path** command, as shown in the following example:

```
lsr-path ipaddress1 [ipaddress2 [... [ipaddress8]]]
```

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **lsr-path** command in IP SLA ICMP Path-echo configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/0/CPU0:router(config-ipsla-icmp-path-echo)# lsr-path 192.0.2.40
```



**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# maximum hops

To set the number of hops in which statistics are maintained for each path for the IP SLA operation, use the **maximum hops** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

**maximum hops** *hops*

**no maximum hops**

## Syntax Description

<i>hops</i>	Number of hops for which statistics are maintained for each path. Range is 1 to 30. Default value is 16 for path operations; for example, <i>pathecho</i> .
-------------	---

## Command Default

The default value is 16 hops.

## Command Modes

IP SLA operation statistics configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced

## Usage Guidelines

The **maximum hops** command is supported only when you configure path operations and the IP SLA ICMP path-echo operation.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to set the number of hops for the statistics for the **maximum** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/0/CPU0:router(config-ipsla-icmp-path-echo)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-op-stats)# maximum hops 20
```

**Related Commands**

Command	Description
<a href="#">buckets (statistics hourly), on page 125</a>	Sets the number of hours in which statistics are kept.
<a href="#">distribution count, on page 136</a>	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
<a href="#">distribution interval, on page 138</a>	Sets the time interval (in milliseconds) for each statistical distribution.
<a href="#">maximum paths (IP SLA), on page 168</a>	Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation.
<a href="#">statistics, on page 264</a>	Sets the statistics collection parameters for the operation.

## maximum paths (IP SLA)

To set the number of paths in which statistics are maintained for each hour for an IP SLA operation, use the **maximum paths** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

**maximum paths** *paths*

**no maximum paths**

### Syntax Description

<i>paths</i>	Number of paths for which statistics are maintained for each hour. Range is 1 to 128. Default value is 5 for path operations; for example, <i>pathecho</i> .
--------------	--

### Command Default

The default value is 5 paths.

### Command Modes

IP SLA operation statistics configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

The **maximum paths** command is supported only when you configure path operations and the IP SLA ICMP path-echo operation.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to set the number of paths for the statistics for the **maximum paths** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/0/CPU0:router(config-ipsla-icmp-path-echo)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-op-stats)# maximum paths 20
```

**Related Commands**

Command	Description
<a href="#">buckets (statistics hourly), on page 125</a>	Sets the number of hours in which statistics are kept.
<a href="#">distribution count, on page 136</a>	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
<a href="#">distribution interval, on page 138</a>	Sets the time interval (in milliseconds) for each statistical distribution.
<a href="#">maximum hops, on page 166</a>	Sets the number of hops in which statistics are maintained for each path for the IP SLA operation.
<a href="#">statistics, on page 264</a>	Sets the statistics collection parameters for the operation.

# monitor

To configure an MPLS LSP monitor instance, use the **monitor** command in IP SLA LSP monitor configuration mode. To remove the monitor instance, use the **no** form of this command.

**monitor** *monitor-id*

**no monitor** [ *monitor-id* ]

Syntax Description	
<i>monitor-id</i>	Number of the IP SLA LSP monitor instance to be configured. Range is 1 to 2048.

**Command Default** No monitor instance is configured.

**Command Modes** IP SLA LSP monitor configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced.

**Usage Guidelines** The **monitor** command enters IP SLA MPLS LSP monitor configuration mode so that you can set the desired monitor type for all operations associated with the monitored provider edge (PE) routers.

To remove all monitor instances, use the **no monitor** command with no argument.

Task ID	Task ID	Operations
	monitor	read, write

**Examples** The following example shows how to use the **monitor** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)#
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## mpls discovery vpn

To configure MPLS label switched path (LSP) provider edge (PE) router discovery, use the **mpls discovery vpn** command in IP SLA configuration mode. To use the default value, use the **no** form of this command.

**mpls discovery vpn** [*interval interval*]

**no mpls discovery vpn**

Syntax Description	<table><tr><td>interval</td><td>Configures the refresh interval for MPLS label switched path (LSP) monitoring.</td></tr></table>		interval	Configures the refresh interval for MPLS label switched path (LSP) monitoring.		
interval	Configures the refresh interval for MPLS label switched path (LSP) monitoring.					
Command Default	None					
Command Modes	IP SLA configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.5.0</td><td>This command was introduced.</td></tr></table>		Release	Modification	Release 3.5.0	This command was introduced.
Release	Modification					
Release 3.5.0	This command was introduced.					
Usage Guidelines	Use the <b>mpls discovery vpn</b> command to configure provider edge (PE) router discovery. PE Discovery discovers the LSPs used to reach every routing next hop. Routing entities are stored in a Layer 3 VPN discover database.					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>monitor</td><td>read, write</td></tr></table>		Task ID	Operations	monitor	read, write
Task ID	Operations					
monitor	read, write					
Examples	The following example shows how to enter IP SLA MPLS discovery VPN mode:  RP/0/0/CPU0:router# <b>configure</b> RP/0/0/CPU0:router(config)# <b>ipsla</b> RP/0/0/CPU0:router(config-ipsla)# <b>mpls discovery vpn</b> RP/0/0/CPU0:router(config-ipsla-mpls-discovery-vpn)#					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td><a href="#">interval</a>, <a href="#">on page 150</a></td><td>Configures the refresh interval for MPLS label switched path (LSP) monitoring.</td></tr></table>		Command	Description	<a href="#">interval</a> , <a href="#">on page 150</a>	Configures the refresh interval for MPLS label switched path (LSP) monitoring.
Command	Description					
<a href="#">interval</a> , <a href="#">on page 150</a>	Configures the refresh interval for MPLS label switched path (LSP) monitoring.					



Command	Description
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.

# mpls lsp-monitor

To configure MPLS label switched path (LSP) monitoring, use the **mpls lsp-monitor** command in IP SLA configuration mode. To use the default value, use the **no** form of this command.

**mpls lsp-monitor**

**no mpls lsp-monitor**

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

**Command Default** None

**Command Modes** IP SLA configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced.

**Usage Guidelines** Use the **mpls lsp-monitor** command to configure MPLS LSP PE monitoring on the router. This provides a means to configure all operations associated with the monitored provider edge (PE) routers. The configuration is inherited by all LSP operations that are created automatically by the PE discovery.

Task ID	Task ID	Operations
	monitor	read, write

**Examples** The following example shows how to enter IP SLA MPLS LSP monitor mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)#
```

Related Commands	Command	Description
	<a href="#">monitor</a> , on page 170	Configures an IP SLA MPLS LSP monitor instance.
	<a href="#">mpls discovery vpn</a> , on page 172	Configures MPLS label switched path (LSP) provider edge (PE) router discovery.

Command	Description
<a href="#">reaction monitor</a> , on page 199	Configures MPLS LSP monitoring reactions.
<a href="#">schedule monitor</a> , on page 216	Schedules an IP SLA MPLS LSP monitor instance.

# operation

To configure an IP SLA operation, use the **operation** command in IP SLA configuration mode. To remove the operation, use the **no** form of this command.

**operation** *operation-number*

**no operation** *operation-number*

## Syntax Description

<i>operation-number</i>	Operation number. Range is 1 to 2048.
-------------------------	---------------------------------------

## Command Default

None

## Command Modes

IP SLA configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the IP SLA **operation** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)#
```

## Related Commands

Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# output interface

To specify the echo request output interface to be used for LSP ping or LSP trace operations, use the **output interface** command in IP SLA MPLS LSP ping or IP SLA MPLS LSP trace configuration mode. To return the output interface to the default, use the **no** form of this command.

**output interface** *type interface-path-id*

**no output interface**

## Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration  
IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

Use the **output interface** command to help monitor path-to-target over the path if there are some ECMP routes in a topology.

You cannot use the **output interface** command if pseudowire is specified as the target to be used in an MPLS LSP ping operation.

## Task ID

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **output interface** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls ls output interface pos 0/1/0/0
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">output nexthop, on page 179</a>	Configures the next-hop address to be used for LSP ping or LSP trace operations.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# output nexthop

To specify the next-hop address to be used for a Label Switched Path (LSP) ping or LSP trace operations, use the **output nexthop** command in the appropriate configuration mode. To return the output next hop to the default, use the **no** form of this command.

**output nexthop** *ip-address*

**no output nexthop**

## Syntax Description

<i>ip-address</i>	IP address of the next hop.
-------------------	-----------------------------

## Command Default

No default behavior or values

## Command Modes

IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

When LSP Path Discovery (LPD) is enabled, the next-hop IP address is also used to filter out the paths that are not associated with the specified next-hop address.



### Note

After you configure the output next hop, you must also configure the output interface.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **output nexthop** command:

```
RP/0/0/CPU0:router# configure
```

```

RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# output nexthop 10.1.1.1

```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">output interface, on page 177</a>	Configures the echo request output interface to be used for LSP ping or LSP trace operations.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.



# packet count

To specify the number of packets that are to be transmitted during a probe, such as a sequence of packets being transmitted for a jitter probe, use the **packet count** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**packet count** *count*

**no packet count**

## Syntax Description

<i>count</i>	Number of packets to be transmitted in each operation. Range for a UDP jitter operation is 1 to 60000. Range for an ICMP path-jitter operation is 1 to 100.
--------------	---

## Command Default

The default packet count is 10.

## Command Modes

IP SLA UDP jitter configuration  
IP SLA ICMP path-jitter configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **packet count** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# packet count 30
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">packet interval, on page 183</a>	Specifies the interval between packets.

# packet interval

To specify the interval between packets, use the **packet interval** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**packet interval** *interval*

**no packet interval**

## Syntax Description

<i>interval</i>	Interpacket interval in milliseconds. Range is 1 to 60000 (in milliseconds).
-----------------	--

## Command Default

The default packet interval is 20 ms.

## Command Modes

IP SLA UDP jitter configuration  
IP SLA ICMP path-jitter configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **packet interval** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# packet interval 30
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.

Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">packet count, on page 181</a>	Specifies the number of packets that are to be transmitted during a probe.

# path discover

To enable path discovery and enter MPLS LSP monitor (MPLSLM) LPD submode, use the **path discover** command in IP SLA MPLS LSP monitor ping configuration mode. To use the default value, use the **no** form of this command.

**path discover**  
**no path discover**

## Syntax Description

None

## Command Default

No default behavior or values

## Command Modes

IP SLA MPLS LSP monitor ping configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to enter path discover submode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/0/CPU0:router(config-ipsla-mplslm-lpd)#
```

## path discover echo

To configure MPLS LSP echo parameters, use the **path discover** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**path discover echo** {*interval time*| **maximum lsp selector ipv4** *host address*| **multipath bitmap size** *size*| **retry count**| **timeout value**}

**no path discover echo** {*interval time*| **maximum lsp selector ipv4** *host address*| **multipath bitmap size** *size*| **retry count**| **timeout value**}

### Syntax Description

<b>interval</b> <i>time</i>	Configures the interval (in milliseconds) between MPLS LSP echo requests sent during path discovery. Range is 0 to 3600000. Default is 0.
<b>maximum lsp selector ipv4</b> <i>host-address</i>	Configures a local host IP address (127.x.x.x) that is the maximum selector value to be used during path discovery. Default is 127.255.255.255.
<b>multipath bitmap size</b> <i>size</i>	Configures the maximum number of selectors sent in the downstream mapping of an MPLS LSP echo request during path discovery. Range is 1 to 256. Default is 32.
<b>retry</b> <i>count</i>	Configures the number of timeout retry attempts for MPLS LSP echo requests sent during path discovery. Range is 0 to 10. Default is 3.
<b>timeout</b> <i>value</i>	Configures the timeout value (in seconds) for MPLS LSP echo requests sent during path discovery. Range is 1 to 3600. Default is 5.

### Command Default

**interval** *time*: 0  
**maximum lsp selector ipv4** *host address*: 127.255.255.255  
**multipath bitmap size** *size* : 32  
**retry** *count*: 3  
**timeout** *value*: 5

### Command Modes

Path discover configuration  
MPLS LSP ping configuration

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

**Usage Guidelines**

A retry occurs when either an echo reply was not received on time for an outstanding echo request, or when no selectors are found for a given path by a transit router.

When a selector value is configured in MPLSLM configuration mode, the maximum selector specified must be larger than that value. In such a scenario, the range of selectors used for path discovery is set by the two values.

When the **interval** *time* is zero, a new echo request is sent after the previous echo retry was received.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to configure the path discover echo interval:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# echo interval 777
```

**Related Commands**

Command	Description
<a href="#">path discover path, on page 188</a>	Configures MPLS LSP path parameters.
<a href="#">path discover scan, on page 190</a>	Configures MPLS LSP scan parameters.
<a href="#">path discover session, on page 192</a>	Configures MPLS LSP session parameters.

## path discover path

To configure MPLS LSP path parameters, use the **path discover path** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

**path discover path** {**retry** *range*| **secondary frequency** {**both**| **connection-loss**| **timeout**} *value*}

**no path-discover path**

### Syntax Description

<b>retry</b> <i>range</i>	Configures the number of attempts to be performed before declaring a path as down. Default is 1 (LSP group will not retry to perform the echo request if the previous attempt fails). Range is 1 to 16.
<b>secondary frequency</b>	Configures a secondary frequency to use after a failure condition (that is, a connection-loss or timeout) occurs.
<b>both</b>	Enable secondary frequency for a timeout and connection loss.
<b>connection-loss</b>	Enable secondary frequency for only a connection loss.
<b>timeout</b>	Enable secondary frequency for only a timeout.
<i>value</i>	Frequency value range is 1 to 604800.

### Command Default

None

### Command Modes

MPLSLM LPD configuration

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

### Usage Guidelines

In the event of a path failure, the secondary frequency value is used instead of the normal frequency value. The normal frequency value is determined by a frequency value or schedule period value, and the LSP operations are scheduled to start periodically at this interval. By default, the secondary frequency value is disabled. When failure condition disappears, probing resumes at the regular frequency.



#### Note

*The **secondary** command works in tandem with the **retry** keyword. Both must be configured.*



**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to configure MPLS LSP path parameters:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplsml-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplsml-lsp-ping)# path discover
RP/0/0/CPU0:router(config-ipsla-mplsml-lsp-lpd)# path retry 12
RP/0/0/CPU0:router(config-ipsla-mplsml-lsp-lpd)# path secondary frequency both 10
```

**Related Commands**

Command	Description
<a href="#">path discover echo, on page 186</a>	Configures MPLS LSP echo parameters.
<a href="#">path discover scan, on page 190</a>	Configures MPLS LSP scan parameters.
<a href="#">path discover session, on page 192</a>	Configures MPLS LSP session parameters.

## path discover scan

To configure MPLS LSP scan parameters, use the **path discover scan** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

**path discover scan period** *value*

**no path discover scan period** *value*

### Syntax Description

<b>period</b> <i>value</i>	Configures the time (in minutes) between consecutive cycles of path discovery requests per MPLSLM instance. Range is 0 to 7200. Default is 5.
----------------------------	---

### Command Default

**period** *value* : 5

### Command Modes

MPLSLM LPD configuration submode

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

### Usage Guidelines

MPLSLM instances periodically trigger path discovery requests for LSP groups. At certain intervals, an MPLSLM instance begins triggering path discovery requests for each group in ascending order (determined by group ID). By default, the path discovery requests are triggered sequentially, although some concurrency may occur if the session limit value is greater than 1. The cycle concludes when the last LSP group finishes path discovery.

If the duration of the discovery cycle is larger than the scan period, a new cycle starts as soon as the previous one completes.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to configure the path discovery scan period value:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
```

```
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# path discover  
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-lpd)# scan period 2
```

**Related Commands**

Command	Description
<a href="#">path discover echo, on page 186</a>	Configures MPLS LSP echo parameters.
<a href="#">path discover path, on page 188</a>	Configures MPLS LSP path parameters.
<a href="#">path discover session, on page 192</a>	Configures MPLS LSP session parameters.

## path discover session

To configure MPLS LSP session parameters, use the **path discover session** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

**path discover session** {*limit value*| *timeout value*}

**no path discover session** {*limit value*| *timeout value*}

### Syntax Description

<b>limit</b> <i>value</i>	Configures the number of concurrent active path discovery requests the MPLSLM instance submits to the LSPV server. Range is 1 to 15. Default is 1.
<b>timeout</b> <i>value</i>	Configures the time (in seconds) the MPLSLM instance will wait for the result of a path discovery request submitted to the LSPV server. Range is 1 to 900. Default is 120.

### Command Default

**limit** *value* : 1

**timeout** *value* : 120

### Command Modes

MPLSLM LPD configuration submode

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

### Usage Guidelines

An MPLSLM instance considers the path discovery as a failure when it receives no response within the configured timeout configuration value.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to configure the path discovery session timeout value:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
```

```
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# path discover
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-lpd)# session timeout 22
```

**Related Commands**

Command	Description
<a href="#">path discover echo, on page 186</a>	Configures MPLS LSP echo parameters.
<a href="#">path discover path, on page 188</a>	Configures MPLS LSP path parameters.
<a href="#">path discover scan, on page 190</a>	Configures MPLS LSP scan parameters.

## react

To specify an element to be monitored for a reaction, use the **react** command in the appropriate configuration mode. To remove the specified reaction type, use the **no** form of this command.

**react** {**connection-loss**| **jitter-average** [**dest-to-source**| **source-to-dest**]| **packet-loss** {**dest-to-source**| **source-to-dest**}| **rtt**| **timeout**| **verify-error**}

**no react** {**connection-loss**| **jitter-average** [**dest-to-source**| **source-to-dest**]| **packet-loss** {**dest-to-source**| **source-to-dest**}| **rtt**| **timeout**| **verify-error**}

### Syntax Description

<b>connection-loss</b>	Specifies that a reaction occurs if there is a connection-loss for the monitored operation.
<b>jitter-average</b> [ <b>dest-to-source</b>   <b>source-to-dest</b> ]	Specifies that a reaction occurs if the average round-trip jitter value violates the upper threshold or lower threshold. The following options are listed for the <b>jitter-average</b> keyword: <ul style="list-style-type: none"> <li>• <b>dest-to-source</b>—(Optional) Specifies the jitter average destination to source (DS).</li> <li>• <b>source-to-dest</b>—(Optional) Specifies the jitter average source to destination (SD).</li> </ul>
<b>packet-loss</b> { <b>dest-to-source</b>   <b>source-to-dest</b> }	Specifies the reaction on packet loss value violation. The following options are listed for the <b>packet-loss</b> keyword: <ul style="list-style-type: none"> <li>• <b>dest-to-source</b>—(Optional) Specifies the packet loss destination to source (DS) violation.</li> <li>• <b>source-to-dest</b>—(Optional) Specifies the packet loss source to destination (SD) violation.</li> </ul>
<b>rtt</b>	Specifies that a reaction occurs if the round-trip value violates the upper threshold or lower threshold.
<b>timeout</b>	Specifies that a reaction occurs if there is a timeout for the monitored operation.
<b>verify-error</b>	Specifies that a reaction occurs if there is an error verification violation.

### Command Default

If there is no default value, no reaction is configured.

### Command Modes

IP SLA reaction configuration  
IP SLA MPLS LSP monitor reaction configuration

**Command History**

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor reaction configuration mode.

**Usage Guidelines**

For the **connection-loss** keyword, **jitter-average** keyword, and **rtt** keyword, the reaction does not occur when the value violates the upper or the lower threshold. The reaction condition is set when the upper threshold is passed, and it is cleared when values go below the lower threshold.

For the **connection-loss** keyword and **verify-error** keyword, thresholds do not apply to the monitored element.

For the **jitter-average** keyword, **packet-loss** keyword, and **rtt** keyword, if the upper threshold for react threshold type average 3 is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average is  $6000 + 6000 + 5000 = 17000 / 3 = 5667$ —therefore violating the 5000-ms upper threshold. The threshold type average must be configured when setting the type. These keywords are not available if connection-loss, timeout, or verify-error is specified as the monitored element, because upper and lower thresholds do not apply to these options.

In IP SLA MPLS LSP monitor reaction configuration mode, only the **connection-loss** and **timeout** keywords are available. If the **react** command is used in IP SLA MPLS LSP monitor reaction configuration mode, it configures all operations associated with the monitored provider edge (PE) routers. The configuration is inherited by all LSP operations that are created automatically by the PE discovery.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **react** command with the **connection-loss** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **jitter-average** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **packet-loss** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
```

```
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **rtt** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react rtt
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **timeout** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react timeout
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **verify-error** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react verify-error
RP/0/0/CPU0:router(config-ipsla-react-cond)#
```

## Related Commands

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs when you configure the <b>react</b> command or when threshold events occur.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.



# react lpd

To specify that a reaction should occur if there is an LSP Path Discovery (LPD) violation, use the **react lpd** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**react lpd {lpd-group| tree-trace} action logging**

**no react lpd {lpd-group| tree-trace}**

## Syntax Description

<b>lpd-group</b>	Specifies that a reaction should occur if there is a status violation for the monitored LPD group.
<b>tree-trace</b>	Specifies that a reaction should occur if there is a path discovery violation for the monitored LPD group.
<b>action</b>	Configures the action to be taken on threshold violation.
<b>logging</b>	Specifies the generation of a syslog alarm on threshold violation.

## Command Default

None

## Command Modes

IP SLA MPLS LSP monitor configuration

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

A status violation for a monitored LPD group happens when the Label Switched Path (LSP) group status changes (with the exception of the status change from the initial state).

A path discovery violation for the monitored LPD group happens when path discovery to the target PE fails, or successful path discovery clears such a failure condition.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to specify that a reaction should occur if there is a status violation for the monitored LPD group:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# reaction monitor 1
RP/0/0/CPU0:router(config-ipsla-mplsml-react)# react lpd lpd-group action logging
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# reaction monitor

To configure MPLS label switched path (LSP) monitoring reactions, use the **reaction monitor** command in IP SLA MPLS LSP monitor configuration mode. To remove the reaction so that no reaction occurs, use the **no** form of this command.

**reaction monitor** *monitor-id*

**no reaction monitor** [*monitor-id*]

## Syntax Description

<i>monitor-id</i>	Number of the IP SLA MPLS LSP monitor instance for the reactions to be configured. Range is 1 to 2048.
-------------------	--

## Command Default

No reaction is configured.

## Command Modes

IP SLA MPLS LSP monitor configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

The **reaction monitor** command enters IP SLA LSP monitor reaction configuration mode so that you can set the desired threshold and action in the event of a connection loss or timeout.

To remove all reactions, use the **no reaction monitor** command with no *monitor-id* argument.

The **reaction monitor** command configures reactions for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **reaction operation** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# reaction monitor 1
RP/0/0/CPU0:router(config-ipsla-mplsml-react)#
```

**Related Commands**

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs when you configure the <b>react</b> command or when threshold events occur
<a href="#">monitor, on page 170</a>	Configures an IP SLA MPLS LSP monitor instance.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">schedule monitor, on page 216</a>	Schedules an IP SLA MPLS LSP monitor instance.
<a href="#">threshold type consecutive, on page 279</a>	Specifies to take action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Specifies to take action immediately upon a threshold violation.

# reaction operation

To configure certain actions that are based on events under the control of the IP SLA agent, use the **reaction operation** command in IP SLA configuration mode. To remove the reaction so that no reaction occurs, use the **no** form of this command.

**reaction operation** *operation-id*

**no reaction operation** *operation-id*

## Syntax Description

<i>operation-id</i>	Number of the IP SLA operation for the reactions to be configured. Range is 1 to 2048.
---------------------	--

## Command Default

No reaction is configured.

## Command Modes

IP SLA configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **reaction operation** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 1
RP/0/0/CPU0:router(config-ipsla-react)#
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.

Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## reaction trigger

To define a second IP SLA operation to make the transition from a pending state to an active state when one of the trigger-type options is defined with the **reaction operation** command, use the **reaction trigger** command in IP SLA configuration mode. To remove the reaction trigger when the *triggering-operation* argument does not trigger any other operation, use the **no** form of this command.

**reaction trigger** *triggering-operation* *triggered-operation*

**no reaction trigger** *triggering-operation* *triggered-operation*

### Syntax Description

<i>triggering-operation</i>	Operation that contains a configured action-type trigger and can generate reaction events. Range is 1 to 2048.
<i>triggered-operation</i>	Operation that is started when the <i>triggering-operation</i> argument generates a trigger reaction event. Range is 1 to 2048.

### Command Default

No triggered operation is configured.

### Command Modes

IP SLA configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

Both the *triggering-operation* and *triggered-operation* arguments must be configured. The triggered operation must be in the pending state.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **ipsla reaction trigger** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction trigger 1 2
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# responder

To enable the IP SLA responder for UDP echo or jitter operations, use the **responder** command in IP SLA configuration mode. To disable the responder, use the **no** form of this command.

**responder**

**no responder**

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

**Command Default** The IP SLA **responder** command is disabled.

**Command Modes** IP SLA configuration

Release	Modification
Release 3.3.0	This command was introduced.

**Usage Guidelines** An IP address and port are configured and identified as a permanent port (for example, a port to which the responder is permanently listening). If no IP address and port are configured, the responder handles only dynamic ports (for example, ports that are listened to when requested by a remote operation).

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to enable the IP SLA responder:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# responder
RP/0/0/CPU0:router(config-ipsla-resp)#
```

Command	Description
<a href="#">type udp ipv4 address, on page 300</a>	Configures a permanent port in the IP SLA Responder for UDP echo or jitter operations.

# recurring

To indicate that the operation starts automatically at the specified time and for the specified duration every day, use the **recurring** command in IP SLA schedule configuration mode. To not start the operation everyday, use the **no** form of this command.

**recurring**

**no recurring**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Recurring is disabled.

## Command Modes

IP SLA schedule configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **recurring** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/0/CPU0:router(config-ipsla-sched)# recurring
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.

# reply dscp

To specify the differentiated services codepoint (DSCP) value used in echo reply packets, use the **reply dscp** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**reply dscp** *dscp-bits*

**no reply dscp**

## Syntax Description

<i>dscp-bits</i>	Differentiated services codepoint (DSCP) value for an echo reply packet. Valid values are from 0 to 63.  Reserved keywords such as EF (expedited forwarding) and AF11 (assured forwarding class AF11) can be specified instead of numeric values.
------------------	---

## Command Default

No default behavior or values

## Command Modes

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration  
IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

## Usage Guidelines

Use the **reply dscp** command to set the DSCP value used in the headers of IPv4 UDP packets sent as echo replies in an MPLS LSP ping or MPLS LSP trace operation.

The DSCP value consists of the six most significant bits of the 1-byte IP type of service (ToS) field. These bits determine the quality-of-service (QoS) treatment (per-hop behavior) that a transit LSR node gives to an echo reply packet. For information about how packets are classified and processed depending on the value you assign to the 6-bit DSCP field, refer to “The Differentiated Services Model (DiffServ)” at the following URL:

[http://www.cisco.com/en/US/products/ps6610/products\\_data\\_sheet09186a00800a3e30.html](http://www.cisco.com/en/US/products/ps6610/products_data_sheet09186a00800a3e30.html)

If the **reply dscp** command is used in IP SLA operation mode, it acts on the headers of echo replies for the specific operation being configured. If the **reply dscp** command is used in IP SLA MPLS LSP monitor mode,

it acts on the headers of echo replies for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **reply dscp** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# reply dscp 5
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# reply mode

To specify how to reply to echo requests, use the **reply mode** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**reply mode** {**control-channel**| **router-alert**}

**no reply mode**

## Syntax Description

<b>control-channel</b>	Sets echo requests to reply by way of a control channel.  <b>Note</b> This option is available only in IP SLA MPLS LSP ping configuration mode.
<b>router-alert</b>	Sets echo requests to reply as an IPv4 UDP packet with IP router alert.

## Command Default

The default reply mode for an echo request packet is an IPv4 UDP packet without IP router alert set.

## Command Modes

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration  
IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.  The <b>control-channel</b> keyword was added in IP SLA MPLS LSP ping configuration mode.

## Usage Guidelines

Use the **reply mode** command with the **control-channel** keyword to send echo reply packets by way of a control channel in an MPLS LSP ping operation. If the target is not set to pseudowire, the configuration of the **control-channel** keyword is rejected. Refer to the **target pseudowire** command for information about setting the target.

Use the **reply mode** command with the **router-alert** keyword to set the reply mode of echo reply packets in an MPLS LSP ping or MPLS LSP trace operation. After you enter this command, echo reply packets are set to reply as an IPv4 UDP packet with the IP router alert option in the UDP packet header.

If the **reply mode** command is used in IP SLA operation mode, it sets the reply mode of echo reply packets for the specific operation being configured. If the **reply mode** command is used in IP SLA MPLS LSP monitor mode, it sets the reply mode of echo reply packets for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

The router-alert reply mode forces an echo reply packet to be specially handled by the transit LSR router at each intermediate hop as it moves back to the destination. Because this reply mode is more expensive, it is recommended only if the headend router does not receive echo replies using the default reply mode.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **reply mode** command with the **router-alert** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# reply mode router-alert
```

The following example shows how to use the **reply mode** command with the **control-channel** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# target pseudowire 192.168.1.4 4211
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# reply mode control-channel
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# responder twamp

To configure the TWAMP responder, use the **responder twamp** command in the appropriate mode. To remove the set configuration, use the **no** form of the command.

**responder twamp** [ *timeout value* ]

**no responder twamp** [ *timeout value* ]

Syntax Description	<b>timeout</b> <i>value</i>	Inactivity timeout period (in seconds). Range is 1 to 604800.
--------------------	-----------------------------	---

Command Default	Default timeout is 900 seconds.
-----------------	---------------------------------

Command Modes	IPSLA configuration mode
---------------	--------------------------

Command History	Release	Modification
	Release 5.1.1	This command was introduced.

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

Task ID	Task ID	Operation
	monitor	read, write

Examples	<p>This example shows how to run the <b>responder twamp</b> command:</p> <pre>RP/0/0/CPU0:router (config-ipsla) # responder twamp timeout 100</pre>
----------	---

## scan delete-factor

To specify the frequency with which the MPLS LSP monitor (MPLSLM) instance searches for provider edge (PE) routers to delete, use the **scan delete-factor** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**scan delete-factor** *factor-value*

**no scan delete-factor**

### Syntax Description

<i>factor-value</i>	Specifies a factor that is multiplied by the scan interval to determine the frequency at which the MPLS LSP monitor instance deletes the provider edge (PE) routers that are no longer valid. Range is 0 to 2147483647.
---------------------	---

### Command Default

*factor-value*: 1

### Command Modes

IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

### Command History

Release	Modification
Release 3.5.0	This command was introduced.

### Usage Guidelines

The **scan delete-factor** command specifies a factor value for automatic PE deletion. The specified *factor-value* is multiplied by the scan interval to acquire the frequency at which the MPLS LSP monitoring instance deletes not-found PEs. A scan delete factor of zero (0) means that provider edge (PE) routers that are no longer valid are never removed.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **scan delete-factor** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
```



```
RP/0/0/CPU0:router(config-ipsla-mpls-lm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lm-lsp-ping)# scan delete-factor 214
```

**Related Commands**

Command	Description
<a href="#">monitor</a> , on page 170	Configures an IP SLA MPLS LSP monitor instance.
<a href="#">scan interval</a> , on page 214	Specifies the frequency at which the MPLSLM instance checks the scan queue for updates
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# scan interval

To specify the frequency at which the MPLS LSP monitor (MPLSLM) instance checks the scan queue for updates, use the **scan interval** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**scan interval** *scan-interval*

**no scan interval**

## Syntax Description

<i>scan-interval</i>	Time interval between provider edge (PE) router updates. Range is 1 to 70560.
----------------------	---

## Command Default

*interval*: 240 minutes

## Command Modes

IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

Use the **scan interval** command to specify a frequency value in minutes at which the MPLS LSP monitoring instance checks the scan queue for PE updates. Updates from PE discovery are not processed immediately, but rather stored in a scan queue for batched processing at periodic intervals, specified by this value.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **scan** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# scan interval 120
```

**Related Commands**

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">scan delete-factor</a> , on page 212	Specifies the frequency with which the MPLSLM instance searches for PE routers to delete.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# schedule monitor

To schedule MPLS LSP monitoring instances, use the **schedule monitor** command in IP SLA LSP monitor configuration mode. To unschedule the monitoring instances, use the **no** form of this command.

**schedule monitor** *monitor-id*

**no schedule monitor** [ *monitor-id* ]

## Syntax Description

<i>monitor-id</i>	Number of the monitoring instance to schedule. Range is 1 to 2048.
-------------------	--

## Command Default

No schedule is configured.

## Command Modes

IP SLA MPLS LSP monitor configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

The **schedule monitor** command enters IP SLA MPLS LSP monitor schedule configuration mode so that you can set the desired schedule parameters for the MPLS LSP monitor instance. This schedules the running of all operations created for the specified monitor instance.

To remove all configured schedulers, use the **no schedule monitor** command with no *monitor-id* argument.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to access and use the **schedule monitor** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# schedule monitor 1
RP/0/0/CPU0:router(config-ipsla-mplsml-sched)#
```

**Related Commands**

Command	Description
<a href="#">frequency (IP SLA), on page 146</a>	Configures the frequency interval during which LSP groups and operations are scheduled to start.
<a href="#">schedule period, on page 220</a>	Configures the amount of time during which all LSP operations are scheduled to start or run.
<a href="#">start-time , on page 261</a>	Determines the time when an operation starts.

# schedule operation

To enter schedule configuration mode, use the **schedule operation** command in IP SLA configuration mode. To remove the scheduler, use the **no** form of this command.

**schedule operation** *operation-number*

**no schedule operation** *operation-number*

## Syntax Description

operation-number	Configuration number or schedule number that is used to schedule an IP SLA operation. Range is 1 to 2048.
------------------	---

## Command Default

None

## Command Modes

IP SLA configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **schedule operation** command enters the IP SLA schedule configuration mode. You can configure more schedule configuration parameters to schedule the operation. When an operation is scheduled, it continues collecting information until the configured life expires.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **ipsla schedule operation** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/0/CPU0:router(config-ipsla-sched)#
```

**Related Commands**

Command	Description
<a href="#">ageout</a> , on page 121	Specifies the number of seconds to keep the operation in memory when it is not actively collecting information.
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">life</a> , on page 156	Specifies the length of time to execute.
<a href="#">recurring</a> , on page 206	Indicates that the operation starts automatically at the specified time and for the specified duration every day.
<a href="#">start-time</a> , on page 261	Determines the time when the operation starts.

## schedule period

To configure the amount of time during which all LSP operations are scheduled to start or run, use the **schedule period** command in IP SLA MPLS LSP monitor schedule configuration mode. To remove the scheduler, use the **no** form of this command.

**schedule period** *seconds*

**no schedule period**

### Syntax Description

<i>seconds</i>	Amount of time in seconds for which label switched path (LSP) operations are scheduled to run. Range is 1 to 604800.
----------------	--

### Command Default

None

### Command Modes

IP SLA MPLS LSP monitor schedule configuration

### Command History

Release	Modification
Release 3.5.0	This command was introduced.

### Usage Guidelines

Use the **schedule period** command to specify the amount of time in seconds during which all LSP operations are scheduled to start running. All LSP operations are scheduled equally spaced throughout the schedule period.

For example, if the schedule period is 600 seconds and there are 60 operations to be scheduled, they are scheduled at 10-second intervals.

Use the **frequency** command to specify how often the entire set of operations is performed. The frequency value must be greater than or equal to the schedule period.

You must configure the schedule period before you can start MPLS LSP monitoring. Start MPLS LSP monitoring using the **start-time** command.

### Task ID

Task ID	Operations
monitor	read, write



## Examples

The following example shows how to use the **schedule period** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# schedule monitor 20
RP/0/0/CPU0:router(config-ipsla-mplsml-sched)# schedule period 6000
```

## Related Commands

Command	Description
<a href="#">frequency (IP SLA), on page 146</a>	Configures the frequency interval during which LSP groups and operations are scheduled to start.
<a href="#">start-time , on page 261</a>	Determines the time when the operation starts.

## server twamp

To configure the TWAMP server, use the **server twamp** command in the appropriate mode. To remove the set configuration, use the **no** form of the command.

**server twamp** [ *port number* | *timer inactivity value* ]

**no server twamp** [ *port number* | *timer inactivity value* ]

### Syntax Description

<b>port</b>	Configures the port for the server.
<i>number</i>	Port number. Range is 1 to 65535.
<b>timer</b>	Configures the timer for the server.
<b>inactivity</b> <i>value</i>	Inactivity timer value in seconds. Range is 1 to 6000.

### Command Default

Default port is 862.

Default timer value is 900 seconds.

### Command Modes

IPSLA configuration mode

### Command History

Release	Modification
Release 5.1.1	This command was introduced.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

Task ID	Operation
monitor	read, write

### Examples

This example shows how to use the **server twamp** command:

```
RP/0/0/CPU0:router (config-ipsla) # server twamp timer inactivity 100
```

# show ipsla application

To display the information for the IP SLA application, use the **show ipsla application** command in EXEC mode.

**show ipsla application**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

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

Task ID	Task ID	Operations
	monitor	read

**Examples** The following sample output is from the **show ipsla application** command:

```
RP/0/0/CPU0:router# show ipsla application

Estimated system max number of entries: 2048
Number of Entries configured: 1
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 1

Supported Operation Types: 7

    Type of Operation: ICMP ECHO
    Type of Operation: ICMP PATH JITTER
    Type of Operation: ICMP PATH ECHO
    Type of Operation: UDP JITTER
    Type of Operation: UDP ECHO
    Type of Operation: MPLS LSP PING
    Type of Operation: MPLS LSP TRACE

Number of configurable probes : 2047
SA Agent low memory water mark: 20480 (KB)
```

This table describes the significant fields shown in the display.

**Table 14: show ipsla application Field Descriptions**

Field	Description
Estimated system max number of entries	Maximum number of operations that are configured in the system. The low-memory configured parameter and the available memory in the system are given.
Number of Entries configured	Total number of entries that are configured, such as active state, pending state, and inactive state.
Number of active Entries	Number of entries that are in the active state. The active entries are scheduled and have already started a life period.
Number of pending Entries	Number of entries that are in pending state. The pending entries have a start-time scheduled in the future. These entries either have not started the first life, or the entries are configured as recurring and completed one of its life.
Number of inactive Entries	Number of entries that are in the inactive state. The inactive entries do not have a start-time scheduled. Either the start-time has never been scheduled or life has expired. In addition, the entries are not configured as recurring.
Supported Operation Types	Types of operations that are supported by the system.
Number of configurable probes	Number of remaining entries that can be configured. The number is just an estimated value and it may vary over time according to the available resources.
SA Agent low memory water mark	Available memory for the minimum system below which the IP SLA feature does not configure any more operations.

#### Related Commands

Command	Description
<a href="#">low-memory, on page 160</a>	Configures a low-water memory mark.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.

# show ipsla history

To display the history collected for all IP SLA operations or for a specified operation, use the **show ipsla history** command in EXEC mode.

**show ipsla history** [ *operation-number* ]

## Syntax Description

<i>operation-number</i>	(Optional) Number of the IP SLA operation.
-------------------------	--

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

By default, history statistics are not collected. To have any data displayed by using the **show ipsla history** command, you must configure the history collection.

This table lists the response return values that are used in the **show ipsla history** command.

**Table 15: Response Return Values for the show ipsla history Command**

Code	Description
1	Okay
2	Disconnected
3	Over Threshold
4	Timeout
5	Busy
6	Not Connected
7	Dropped
8	Sequence Error

**show ipsla history**

Code	Description
9	Verify Error
10	Application Specific

If the default tabular format is used, the response return description is displayed as code in the Sense column. The Sense field is always used as a return code.

**Task ID**

Task ID	Operations
monitor	read

**Examples**

The following sample output is from the **show ipsla history** command:

```
RP/0/0/CPU0:router# show ipsla history 1
```

```
Point by point History
Multiple Lines per Entry
Line 1:
Entry      = Entry number
LifeI      = Life index
BucketI    = Bucket index
SampleI    = Sample index
SampleT    = Sample start time
CompT      = RTT (milliseconds)
Sense      = Response return code
Line 2 has the Target Address
Entry LifeI      BucketI    SampleI    SampleT      CompT      Sense      TargetAddr
1      0          0          0          1134419252539 9          1          192.0.2.6
1      0          1          0          1134419312509 6          1          192.0.2.6
1      0          2          0          1134419372510 6          1          192.0.2.6
1      0          3          0          1134419432510 5          1          192.0.2.6
```

This table describes the significant fields shown in the display.

**Table 16: show ipsla history Field Descriptions**

Field	Description
Entry number	Entry number.
LifeI	Life index.
BucketI	Bucket index.
SampleI	Sample index.
SampleT	Sample start time.
CompT	Completion time in milliseconds.

Field	Description
Sense	Response return code.
TargetAddr	IP address of intermediate hop device or destination device.

**Related Commands**

Command	Description
<a href="#">show ipsla statistics aggregated, on page 242</a>	Displays the statistical errors for all the IP SLA operations or for a specified operation.

# show ipsla mpls discovery vpn

To display routing information relating to the BGP next-hop discovery database in the MPLS VPN network, use the **show ipsla mpls discovery vpn** command in EXEC mode.

**show ipsla mpls discovery vpn**

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

**Command Default** No default behavior or values

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.5.0	This command was introduced.

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

Task ID	Task ID	Operations
	monitor	read

**Examples** The following sample output is from the **show ipsla mpls discovery vpn** command:

```
RP/0/0/CPU0:router# show ipsla mpls discovery vpn
```

```
Next refresh after: 46 seconds
```

BGP next hop	Prefix	VRF	PfxCount
192.255.0.4	192.255.0.4/32	red	10
		blue	5
		green	7
192.255.0.5	192.255.0.5/32	red	5
		green	3
192.254.1.6	192.254.1.0/24	yellow	4

This table describes the significant fields shown in the display.



**Table 17: show ipsla mpls discovery vpn Field Descriptions**

Field	Description
BGP next hop	Identifier for the BGP next-hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next-hop neighbor to be used by the MPLS LSP ping or trace operation.
VRF	Names of the virtual routing and forwarding instances (VRFs) that contain routing entries for the specified BGP next-hop neighbor.
PfxCount	Count of the routing entries that participate in the VRF for the specified BGP next-hop neighbor.

# show ipsla mpls lsp-monitor lpd

To display LSP Path Discovery (LPD) operational status, use the **show ipsla mpls lsp-monitor lpd** command in EXEC mode.

**show ipsla mpls lsp-monitor lpd** {**statistics** [*group-ID*] **aggregated** *group-ID*|| **summary** *group*}

<b>statistics</b> <i>group-ID</i>	Displays statistics for the specified LPD group, including the latest LPD start time, return code, completion time, and paths.
<b>aggregated</b> <i>group-ID</i>	Displays the aggregated statistics of the LPD group.
<b>summary</b> <i>group-ID</i>	Displays the current LPD operational status, which includes LPD start time, return code, completion time, and all ECMP path information.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

For the aggregated group ID, a maximum of two buckets are allowed.

## Task ID

Task ID	Operations
monitor	read

## Examples

The following sample output is from the **show ipsla mpls lsp-monitor lpd statistics** command:

```
RP/0/0/CPU0:router# show ipsla mpls lsp-monitor lpd statistics 10001
Group ID: 100001
  Latest path discovery start time      : 00:41:01.129 UTC Sat Dec 10 2005
  Latest path discovery return code     : OK
  Latest path discovery completion time (ms): 3450
  Completion Time Values:
    NumOfCompT: 1      CompTMin: 3450      CompTMax : 3450      CompTAvg: 3450
```

```
Number of Paths Values:  
  NumOfPaths: 10   MinNumOfPaths: 10   MaxNumOfPaths: 10
```

This table describes the significant fields shown in the display.

**Table 18: show ipsla mpls lsp-monitor lpd statistics Field Descriptions**

Field	Description
Group ID	LPD group ID number.
Latest path discovery start time	LPD start time.
Latest path discovery return code	LPD return code.
Latest path discovery completion time	LPD completion time.
Completion Time Values	Completion time values, consisting of Number of Completion Time samples and Minimum Completion Time.
Number of Paths Values	Number of paths values, consisting of Minimum number of paths and Maximum number of paths.

# show ipsla mpls lsp-monitor scan-queue

To display information about BGP next-hop addresses that are waiting to be added to or deleted from the MPLS label switched path (LSP) monitor instance, use the **show ipsla mpls lsp-monitor scan-queue** command in EXEC mode.

**show ipsla mpls lsp-monitor scan-queue** [ *monitor-id* ]

Syntax Description	<div><div><i>monitor-id</i></div><div>(Optional) Number of the IP SLA MPLS LSP monitor instance.</div></div>					
Command Default	None					
Command Modes	EXEC mode					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.5.0</td><td>This command was introduced.</td></tr></table>		Release	Modification	Release 3.5.0	This command was introduced.
Release	Modification					
Release 3.5.0	This command was introduced.					
Usage Guidelines	If the <i>monitor-id</i> argument is not specified, the scan-queue is displayed for all MPLS LSP monitor instances.					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>monitor</td><td>read</td></tr></table>		Task ID	Operations	monitor	read
Task ID	Operations					
monitor	read					

## Examples

The following sample output is from the **show ipsla mpls lsp-monitor scan-queue** command:

```
RP/0/0/CPU0:router# show ipsla mpls lsp-monitor scan-queue 1
```

```
IPSLA MPLS LSP Monitor : 1
```

```
Next scan Time after      : 23 seconds
Next Delete scan Time after: 83 seconds
```

BGP Next hop	Prefix	Add/Delete?
192.255.0.2	192.255.0.2/32	Add
192.255.0.3	192.255.0.5/32	Delete

This table describes the significant fields shown in the display.

**Table 19: show ipsla responder statistics port Field Descriptions**

Field	Description
IPSLA MPLS LSP Monitor	Monitor identifier.
Next scan Time after	Amount of time before the MPLS LSP monitor instance checks the scan queue for adding BGP next-hop neighbors. At the start of each scan time, IP SLA operations are created for all newly discovered neighbors.
Next delete Time after	Amount of time left before the MPLS LSP monitor instance checks the scan queue for deleting BGP next-hop neighbors. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP next hop	Identifier for the BGP next-hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next-hop neighbor to be used.
Add/Delete	Indicates that the specified BGP next-hop neighbor will be added or removed.

# show ipsla mpls lsp-monitor summary

To display the list of operations that have been created automatically by the specified MPLS LSP monitor (MPLSLM) instance, use the **show ipsla mpls lsp-monitor summary** command in EXEC mode.

**show ipsla mpls lsp-monitor summary** [*monitor-id* [**group** [*group id*]]]

## Syntax Description

<i>monitor-id</i>	(Optional) Displays a list of LSP group, ping, and trace operations created automatically by the specified MPLSLM instance.
<b>group</b> <i>group-id</i>	(Optional) Displays the ECMP LSPs found through ECMP path discovery within the specified LSP group.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.7.0	Show output response was expanded to add a pending status when waiting for an LSP ping or trace response.

## Usage Guidelines

The **show ipsla mpls lsp-monitor summary** command shows the list of LSP operations that were created automatically by the specified MPLS LSP monitor instance. It also shows the current status and the latest operation time of each operation.

If the *monitor-id* argument is not specified, the list of operations is displayed for all MPLS LSP monitor instances.

The **show ipsla mpls lsp-monitor summary** command with the **group** option shows the list of ECMP paths that are found automatically by the specified LSP path discovery (LPD). In addition, this command with option shows the current status; the number of successes, failures; the most recent round trip time (RTT); and the latest operation time of each path.

If the *group-id* argument is not specified, the list of paths is displayed for all operations created by the MPLS LSP monitor instance.

## Task ID

Task ID	Operations
monitor	read

## Examples

The following sample output is from the **show ipsla mpls lsp-monitor summary** command. This output shows a pending status when an MPLS LSP ping operation is waiting to receive the timeout response from the LSP Verification (LSPV) process.

```
RP/0/0/CPU0:router# show ipsla mpls lsp-monitor summary 1
```

MonID	Op/GrpID	TargetAddress	Status	Latest Operation Time
1	100001	192.255.0.4/32	up	19:33:37.915 EST Mon Feb 28 2005
1	100002	192.255.0.5/32	down	19:33:47.915 EST Mon Feb 28 2005
1	100003	192.255.0.6/32	pending	19:33:35.915 EST Mon Feb 28 2005

The following sample output shows that a down status is displayed after a timeout response is received.

```
RP/0/0/CPU0:router# show ipsla mpls lsp-monitor summary 1
```

MonID	Op/GrpID	TargetAddress	Status	Latest Operation Time
1	100001	193.100.0.1/32	down	12:47:16.417 PST Tue Oct 23 2007
1	100002	193.100.0.2/32	partial	12:47:22.418 PST Tue Oct 23 2007
1	100003	193.100.0.3/32	partial	12:47:22.429 PST Tue Oct 23 2007
1	100004	193.100.0.4/32	down	12:47:16.429 PST Tue Oct 23 2007
1	100005	193.100.0.5/32	down	12:47:21.428 PST Tue Oct 23 2007

This table describes the significant fields shown in the display.

**Table 20: show ipsla mpls lsp-monitor summary Field Descriptions**

Field	Description
MonID	Monitor identifier.
Op/GrpID	Operation identifiers that have been created by this MPLS LSP monitor instance.
TargetAddress	IPv4 Forward Equivalence Class (FEC) to be used by this operation.
Status	Status of the paths. Values can be as follows: <ul style="list-style-type: none"> <li>• up—Indicates that the latest operation cycle was successful.</li> <li>• down—Indicates that the latest operation cycle was not successful.</li> <li>• pending—Indicates that the latest operation cycle is waiting for an LSP ping or trace response.</li> </ul>
Latest Operation Time	Time the latest operation cycle was issued.

The following sample output is from the **show ipsla mpls lsp-monitor summary group** command:

```
RP/0/0/CPU0:router# show ipsla mpls lsp-monitor summary 1 group 100001
```

```

GrpID  LSP-Selector      Status Failure Success RTT   Latest Operation Time
100001 127.0.0.13          up      0      78     32   20:11:37.895 EST Feb 28 2005
100001 127.0.0.15          retry   1      77     0    20:11:37.995 EST Feb 28 2005
100001 127.0.0.16          up      0      78     32   20:11:38.067 EST Feb 28 2005
100001 127.0.0.26          up      0      78     32   20:11:38.175 EST Feb 28 2005

```

This table describes the significant fields shown in the display.

**Table 21: show ipsla mpls lsp-monitor summary group Field Descriptions**

Field	Description
GrpID	Group identifier that has been created by this MPLS LSP monitor instance.
LSP-Selector	LSP selector address.
Status	Status of the paths. Values can be as follows: <ul style="list-style-type: none"> <li>• up—Indicates that all the paths were successful.</li> <li>• down—Indicates that all the paths were not successful.</li> <li>• partial—Indicates that only some paths were successful.</li> <li>• unknown—Indicates that some (or all) of the paths did not complete a single LSP echo request so the group status could not be identified.</li> </ul>
Failure	Number of failures.
Success	Number of successes.
RTT	Round Trip Time (RTT) in milliseconds of the latest LSP echo request for the path.
Latest Operation Time	Time the latest operation cycle was issued for the path.



# show ipsla responder statistics

To display the number of probes that are received or handled by the currently active ports on the responder, use the **show ipsla responder statistics ports** command in EXEC mode.

**show ipsla responder statistics {all| permanent} ports**

## Syntax Description

<b>all</b>	Port statistics is displayed for all ports.
<b>permanent</b>	Port statistics is displayed only for permanent ports.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The output of the **show ipsla responder statistics port** command is available only for specific intervals of time in which only nonpermanent ports are being used at the responder. The reason is that the responder closes the nonpermanent ports after each operation cycle. However, if both permanent and nonpermanent ports are used, the output always contains rows for the permanent ports. The rows for the nonpermanent ports are displayed only if those nonpermanent ports are enabled at the instant the command is issued.

## Task ID

Task ID	Operations
monitor	read

## Examples

The following sample output is from the **show ipsla responder statistics port** command:

```
RP/0/0/CPU0:router# show ipsla responder statistics all port
```

```
Port Statistics
-----
```

Local Address	Port	Port Type	Probes	Drops	CtrlProbes	Discard
172.16.5.1	3001	Permanent	0	0	0	
172.16.5.1	10001	Permanent	728160	0	24272	

```

172.16.5.5      8201   Dynamic   12132   0       12135   ON
172.16.5.1      4441   Dynamic   207216  0       3641    ON

```

This table describes the significant fields shown in the display.

**Table 22: show ipsla responder statistics port Field Descriptions**

Field	Description
Local Address	Local IP address of the responder device used to respond to IPSLA probes.
Port	UDP socket local to the responder device used to respond to IPSLA probes.
Port Type	It could be "permanent" or "dynamic"; depends upon whether a permanent port configuration is done.
Probes	Number of probe packets the responder has received.
Drops	Number of probes dropped.
CtrlProbes	Number of control packets the responder has received.
Discard	If the state is ON, the responder will not respond to probes.

# show ipsla statistics

To display the operational data and the latest statistics for the IP SLA operation in tabular format, use the **show ipsla statistics** command in EXEC mode.

**show ipsla statistics** [ *operation-number* ]

## Syntax Description

<i>operation-number</i>	(Optional) Operation for which the latest statistics are to be displayed. Range is 1 to 2048.
-------------------------	---

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	Show output was expanded to include path information for LSP groups.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read

## Examples

The output of the **show ipsla statistics** command varies depending on the operation type.

The following sample output is from the **show ipsla statistics** command for an ICMP echo operation:

```
RP/0/0/CPU0:router# show ipsla statistics 100025
```

```
Entry number: 100025
Modification time: 00:36:58.602 UTC Sat Dec 10 2007
Start time       : 00:36:58.605 UTC Sat Dec 10 2007
Number of operations attempted: 5
Number of operations skipped   : 0
Current seconds left in Life   : Forever
Operational state of entry     : Active
Connection loss occurred      : FALSE
Timeout occurred              : FALSE
```

## show ipsla statistics

```

Latest RTT (milliseconds)      : 3
Latest operation start time    : 00:41:01.129 UTC Sat Dec 10 2007
Latest operation return code   : OK
RTT Values:
  RTTAvg   : 71          RTTMin: 71          RTTMax : 71
  NumOfRTT : 1          RTTSum: 71          RTTSum2: 729
Path Information:
  Path Path  LSP          Outgoing    Nexthop      Downstream
  Idx  Sense Selector      Interface    Address      Label Stack
  1    1      127.0.0.13    PO0/2/5/0    192.12.1.2    38
  2    1      127.0.0.6     PO0/2/5/0    192.12.1.2    38
  3    1      127.0.0.1     PO0/2/5/0    192.12.1.2    38
  4    1      127.0.0.2     PO0/2/5/0    192.12.1.2    38
  5    1      127.0.0.13    PO0/2/5/1    192.12.2.2    38
  6    1      127.0.0.6     PO0/2/5/1    192.12.2.2    38
  7    1      127.0.0.1     PO0/2/5/1    192.12.2.2    38
  8    1      127.0.0.2     PO0/2/5/1    192.12.2.2    38
  9    1      127.0.0.4     Gi0/2/0/0    192.15.1.2    38
  10   1      127.0.0.5     Gi0/2/0/0    192.15.1.2    38

```

This table describes the significant fields shown in the display.

**Table 23: show ipsla statistics Field Descriptions**

Field	Description
Entry number	Entry number.
Modification time	Latest time the operation was modified.
Start time	Time the operation was started.
Number of operations attempted	Number of operation cycles that were issued.
Number of operations skipped	Number of operation cycles that were not issued because one of the cycles extended over the configured time interval.
Current seconds left in Life	Time remaining until the operation stops execution.
Operational state of entry	State of the operation, such as active state, pending state, or inactive state.
Connection loss occurred	Whether or not a connection-loss error happened.
Timeout occurred	Whether or not a timeout error happened.
Latest RTT (milliseconds)	Value of the latest RTT sample.
Latest operation start time	Time the latest operation cycle was issued.
Latest operation return code	Return code of the latest operation cycle
RTTAvg	Average RTT value that is observed in the last cycle.
RTTMin	Minimum RTT value that is observed in the last cycle.

Field	Description
RTTMax	Maximum RTT value that is observed in the last cycle.
NumOfRTT	Number of successful round trips.
RTTSum	Sum of all successful round-trip values in milliseconds.
RTTSum2	Sum of squares of the round-trip values in milliseconds.
Path Idx	Path index number.
Path Sense	Response return code for the path. (See <a href="#">Table 15: Response Return Values for the show ipsla history Command, on page 225</a> , in <b>show ipsla history</b> command.)
LSP Selector	LSP selector address of the path.
Outgoing Interface	Outgoing interface of the path.
Nexthop Address	Next hop address of the path.
Downstream Label Stack	MPLS label stacks of the path.

**Related Commands**

Command	Description
<a href="#">show ipsla statistics aggregated, on page 242</a>	Displays the statistical errors for all the IP SLA operations or for a specified operation.

# show ipsla statistics aggregated

To display the hourly statistics for all the IP SLA operations or specified operation, use the **show ipsla statistics aggregated** command in EXEC mode.

**show ipsla statistics aggregated [detail] [ operation-number ]**

## Syntax Description

<b>detail</b>	Displays detailed information.
<i>operation-number</i>	(Optional) Number of IP SLA operations. Range is 1 to 2048.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	Show output was expanded to include detailed information when path discovery is enabled.

## Usage Guidelines

The **show ipsla statistics aggregated** command displays information such as the number of failed operations and the reason for failure. Unless you configured a different amount of time for the **buckets** command (**statistics** command with **hourly** keyword), the **show ipsla statistics aggregated** command displays the information collected over the past two hours.

For one-way delay and jitter operations to be computed for UDP jitter operations, the clocks on local and target devices must be synchronized using NTP or GPS systems. If the clocks are not synchronized, one-way measurements are discarded. If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round-trip time, the one-way measurement values are assumed to be faulty, and are discarded.

## Task ID

Task ID	Operations
monitor	read

## Examples

The output of the **show ipsla statistics aggregated** command varies depending on operation type. The following sample output shows the aggregated statistics for UDP echo operation from the **show ipsla statistics aggregated** command:

```
RP/0/0/CPU0:router# show ipsla statistics aggregated 1

Entry number: 1
Hour Index: 0
  Start Time Index: 21:02:32.510 UTC Mon Dec 12 2005
    Number of Failed Operations due to a Disconnect      : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg   : 6          RTTMin: 4          RTTMax : 38
      NumOfRTT: 36          RTTSum: 229         RTTSum2: 2563
```

The following sample output is from the **show ipsla statistics aggregated** command in which operation 10 is a UDP jitter operation:

```
RP/0/0/CPU0:router# show ipsla statistics aggregated 10

Entry number: 10
Hour Index: 0
  Start Time Index: 00:35:07.895 UTC Thu Mar 16 2006
    Number of Failed Operations due to a Disconnect      : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg   : 14          RTTMin: 2          RTTMax : 99
      NumOfRTT: 70          RTTSum: 1034         RTTSum2: 60610
  Packet Loss Values:
    PacketLossSD      : 0          PacketLossDS: 0
    PacketOutOfSequence: 0          PacketMIA   : 0
    PacketLateArrival : 0
    Errors            : 0          Busies       : 0
  Jitter Values :
    MinOfPositivesSD: 1          MaxOfPositivesSD: 19
    NumOfPositivesSD: 17         SumOfPositivesSD: 65
    Sum2PositivesSD : 629
    MinOfNegativesSD: 1          MaxOfNegativesSD: 16
    NumOfNegativesSD: 24         SumOfNegativesSD: 106
    Sum2NegativesSD : 914
    MinOfPositivesDS: 1          MaxOfPositivesDS: 7
    NumOfPositivesDS: 17         SumOfPositivesDS: 44
    Sum2PositivesDS : 174
    MinOfNegativesDS: 1          MaxOfNegativesDS: 8
    NumOfNegativesDS: 24         SumOfNegativesDS: 63
    Sum2NegativesDS : 267
    Interarrival jitterout: 0          Interarrival jitterin: 0
  One Way Values :
    NumOfOW: 0
    OWMinSD : 0          OWMaxSD: 0          OWSumSD: 0
    OWSum2SD: 0
    OWMinDS : 0          OWMaxDS: 0          OWSumDS: 0
```

This table describes the significant fields shown in the display.

**Table 24: show ipsla statistics aggregated Field Descriptions**

Field	Description
Busies	Number of times that the operation cannot be started because the previously scheduled run was not finished.
Entry Number	Entry number.
Hop in Path Index	Hop in path index.
Errors	Number of internal errors.
Jitter Values	Jitter statistics appear on the specified lines. Jitter is defined as interpacket delay variance.
NumOfJitterSamples	Number of jitter samples that are collected. The number of samples are used to calculate the jitter statistics.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.
MaxOfNegativesSD	Maximum negative jitter values from the source to the destination. The absolute value is given.
MaxOfPositivesSD	Maximum jitter values from the source to the destination in milliseconds.
MaxOfPositivesDS	Maximum jitter values from the destination to the source in milliseconds.
MaxOfNegativesDS	Maximum negative jitter values from destination-to-source. The absolute value is given.
MinOfPositivesDS	Minimum jitter values from the destination to the source in milliseconds.



Field	Description
MinOfNegativesSD	Minimum negative jitter values from the source to the destination. The absolute value is given.
MinOfPositivesSD	Minimum jitter values from the source to the destination in milliseconds.
MinOfNegativesDS	Minimum negative jitter values from the destination to the source. The absolute value is given.
NumOfOW	Number of successful one-way time measurements.
NumOfNegativesDS	Number of jitter values from the destination to the source that are negative; for example, network latency decreases for two consecutive test packets.
NumOfNegativesSD	Number of jitter values from the source to the destination that are negative; for example, network latency decreases for two consecutive test packets.
NumOfPositivesDS	Number of jitter values from the destination to the source that are positive; for example, network latency increases for two consecutive test packets.
NumOfPositivesSD	Number of jitter values from the source to the destination that are positive; for example, network latency increases for two consecutive test packets.
NumOfRTT	Number of successful round trips.
One Way Values	One-way measurement statistics appear on the specified lines. One Way (OW) values are the amount of time that it took the packet to travel from the source router to the target router or from the target router to the source router.
OWMaxDS	Maximum time from the destination to the source.
OWMaxSD	Maximum time from the source to the destination.
OWMinDS	Minimum time from the destination to the source.
OWMinSD	Minimum time from the source to the destination.
OWSumDS	Sum of one-way delay values from the destination to the source.
OWSumSD	Sum of one-way delay values from the source to the destination.

Field	Description
OWSum2DS	Sum of squares of one-way delay values from the destination to the source.
OWSum2SD	Sum of squares of one-way delay values from the source to the destination.
PacketLateArrival	Number of packets that arrived after the timeout.
PacketLossDS	Number of packets lost from the destination to the source (DS).
PacketLossSD	Number of packets lost from the source to the destination (SD).
PacketMIA	Number of packets lost in which the SD direction or DS direction cannot be determined.
PacketOutOfSequence	Number of packets that are returned out of order.
Path Index	Path index.
Port Number	Target port number.
RTTSum	Sum of all successful round-trip values in milliseconds.
RTTSum2	Sum of squares of the round-trip values in milliseconds.
RTT Values	Round-trip time statistics appear on the specified lines.
Start Time	Start time, in milliseconds.
Start Time Index	Statistics that are aggregated for over 1-hour intervals. The value indicates the start time for the 1-hour interval that is displayed.
SumOfPositivesDS	Sum of the positive jitter values from the destination to the source.
SumOfPositivesSD	Sum of the positive jitter values from the source to the destination.
SumOfNegativesDS	Sum of the negative jitter values from the destination to the source.
SumOfNegativesSD	Sum of the negative jitter values from the source to the destination.

Field	Description
Sum2PositivesDS	Sum of squares of the positive jitter values from the destination to the source.
Sum2PositivesSD	Sum of squares of the positive jitter values from the source to the destination.
Sum2NegativesDS	Sum of squares of the negative jitter values from the destination to the source.
Sum2NegativesSD	Sum of squares of the negative jitter values from the source to the destination.
Target Address	Target IP address.

The output of the **show ipsla statistics aggregated detail** command varies depending on operation type. The following sample output is from the **show ipsla statistics aggregated detail** command in tabular format, when the output is split over multiple lines:

```
RP/0/0/CPU0:router# show ipsla statistics aggregated detail 2
```

```
Captured Statistics
    Multiple Lines per Entry
Line1:
Entry      = Entry number
StartT     = Start time of entry (hundredths of seconds)
Pth        = Path index
Hop        = Hop in path index
Dst        = Time distribution index
Comps      = Operations completed
SumCmp     = Sum of RTT (milliseconds)

Line2:
SumCmp2H   = Sum of RTT squared high 32 bits (milliseconds)
SumCmp2L   = Sum of RTT squared low 32 bits (milliseconds)
TMax       = RTT maximum (milliseconds)
TMin       = RTT minimum (milliseconds)

Entry StartT      Pth Hop Dst Comps      SumCmp
      SumCmp2H    SumCmp2L  TMax  TMin
2      1134423910701 1 1 0 12      367
0      1231        6
2      1134423851116 1 1 1 2      129
0      2419        41
2      1134423070733 1 1 2 1      101
0      1119        16
2      0           1 1 3 0      0
0      0           0      0
```

This table describes the significant fields shown in the display.

**Table 25: show ipsla statistics aggregated detail Field Descriptions**

Field	Description
Entry	Entry number.
StartT	Start time of entry, in hundredths of seconds.

Field	Description
Pth	Path index.
Hop	Hop in path index.
Dst	Time distribution index.
Comps	Operations completed.
SumCmp	Sum of completion times, in milliseconds.
SumCmp2L	Sum of completion times squared low 32 bits, in milliseconds.
SumCmp2H	Sum of completion times squared high 32 bits, in milliseconds.
TMax	Completion time maximum, in milliseconds.
TMin	Completion time minimum, in milliseconds.

The following sample output is from the **show ipsla statistics aggregated** command when a path discovery operation is enabled. Data following the hourly index is aggregated for all paths in the group during the given hourly interval.

```
RP/0/0/CPU0:router# show ipsla statistics aggregated 100041
```

```
Entry number: 100041
```

```
Hour Index: 13
```

<The following data after the given hourly index is aggregated for all paths in the group during the given hourly interval.>

```
Start Time Index: 12:20:57.323 UTC Tue Nov 27 2007
Number of Failed Operations due to a Disconnect      : 0
Number of Failed Operations due to a Timeout         : 249
Number of Failed Operations due to a Busy            : 0
Number of Failed Operations due to a No Connection   : 0
Number of Failed Operations due to an Internal Error : 0
Number of Failed Operations due to a Sequence Error  : 0
Number of Failed Operations due to a Verify Error    : 0
<end>
```

```
RTT Values:
```

```
RTTAvg  : 21      RTTMin: 19      RTTMax : 73
NumOfRTT: 2780    RTTSum: 59191    RTTSum2: 1290993
```

<The following data for LSP path information is available after path discovery is enabled.>

```
Path Information:
```

Path Idx	Path Sense	LSP Selector	Outgoing Interface	Nexthop Address	Downstream Label Stack
1	1	127.0.0.1	Gi0/4/0/0	192.39.1.1	677
2	1	127.0.0.1	Gi0/4/0/0.1	192.39.2.1	677
3	1	127.0.0.1	Gi0/4/0/0.2	192.39.3.1	677
4	1	127.0.0.1	Gi0/4/0/0.3	192.39.4.1	677
5	1	127.0.0.8	Gi0/4/0/0	192.39.1.1	677
6	1	127.0.0.8	Gi0/4/0/0.1	192.39.2.1	677

```

      7      1      127.0.0.8      Gi0/4/0/0.2      192.39.3.1      677
      8      1      127.0.0.8      Gi0/4/0/0.3      192.39.4.1      677
<end>
Hour Index: 14
Start Time Index: 13:20:57.323 UTC Tue Nov 27 2007
Number of Failed Operations due to a Disconnect      : 0
Number of Failed Operations due to a Timeout         : 122
Number of Failed Operations due to a Busy            : 0
Number of Failed Operations due to a No Connection   : 0
Number of Failed Operations due to an Internal Error : 0
Number of Failed Operations due to a Sequence Error  : 0
Number of Failed Operations due to a Verify Error    : 0
RTT Values:
  RTTAvg   : 21          RTTMin: 19          RTTMax : 212
  NumOfRTT : 3059       RTTSum: 65272       RTTSum2: 1457612
Path Information:
  Path Path LSP      Outgoing      Nexthop      Downstream
  Idx  Sense Selector Interface      Address      Label Stack
  1    1    127.0.0.1  Gi0/4/0/0    192.39.1.1   677
  2    1    127.0.0.1  Gi0/4/0/0.1  192.39.2.1   677
  3    1    127.0.0.1  Gi0/4/0/0.2  192.39.3.1   677
  4    1    127.0.0.1  Gi0/4/0/0.3  192.39.4.1   677
  5    1    127.0.0.8  Gi0/4/0/0    192.39.1.1   677
  6    1    127.0.0.8  Gi0/4/0/0.1  192.39.2.1   677
  7    1    127.0.0.8  Gi0/4/0/0.2  192.39.3.1   677
  8    1    127.0.0.8  Gi0/4/0/0.3  192.39.4.1   677

```

This table describes the significant fields shown in the display.

**Table 26: show ipsla statistics aggregated (with Path Discovery enabled) Field Descriptions**

Field	Description
Entry Number	Entry number.
Start Time Index	Start time.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.
RTT Values	Round-trip time statistics appear on the specified lines.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.

**show ipsla statistics aggregated**

Field	Description
RTT Sum	Sum of all successful round-trip values, in milliseconds.
RTT Sum2	Sum of squares of the round-trip values, in milliseconds.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.
Path Idx	Path index number.
Path Sense	Response return code for the path. (See <a href="#">Table 15: Response Return Values for the show ipsla history Command</a> , on page 225, in <b>show ipsla history</b> command.)
LSP Selector	LSP selector address of the path.
Outgoing Interface	Outgoing interface name of the path.
Nexthop Address	Next hop address of the path.
Downstream Label Stack	MPLS label stacks of the path.

**Related Commands**

Command	Description
<a href="#">show ipsla statistics</a> , on page 239	Displays the operational data for the IP SLA operation.
<a href="#">show ipsla statistics enhanced aggregated</a> , on page 251	Displays the statistical errors for all the IP SLA operations or for a specified operation.

# show ipsla statistics enhanced aggregated

To display the enhanced history statistics for all collected enhanced history buckets for the specified IP SLA operation, use the **show ipsla statistics enhanced aggregated** command in EXEC mode.

**show ipsla statistics enhanced aggregated** [ *operation-number* ] [ **interval** *seconds* ]

## Syntax Description

<i>operation-number</i>	(Optional) Operation number for which to display the enhanced history distribution statistics.
<b>interval</b> <i>seconds</i>	(Optional) Specifies the aggregation interval in seconds for which to display the enhanced history distribution statistics.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **show ipsla statistics enhanced aggregated** command displays data for each bucket of enhanced history data shown individually; for example, one after the other. The number of buckets and the collection interval is set using the **interval** keyword, *seconds* argument, **buckets** keyword, and *number-of-buckets* argument.

## Task ID

Task ID	Operations
monitor	read

## Examples

The output of the **show ipsla statistics enhanced aggregated** command varies depending on the operation type.

The following sample output is from the **show ipsla statistics enhanced aggregated** command for the UDP echo operation:

```
RP/0/0/CPU0:router# show ipsla statistics enhanced aggregated 20
Entry number: 20
Interval : 300 seconds
Bucket : 1 (0 - 300 seconds)
```

**show ipsla statistics enhanced aggregated**

```

Start Time Index: 00:38:14.286 UTC Thu Mar 16 2006
Number of Failed Operations due to a Disconnect      : 0
Number of Failed Operations due to a Timeout         : 0
Number of Failed Operations due to a Busy            : 0
Number of Failed Operations due to a No Connection   : 0
Number of Failed Operations due to an Internal Error : 0
Number of Failed Operations due to a Sequence Error  : 0
Number of Failed Operations due to a Verify Error    : 0
RTT Values:
  RTTAvg  : 2          RTTMin: 2          RTTMax : 5
  NumOfRTT: 5          RTTSum: 13         RTTSum2: 41
Bucket : 2 (300 - 600 seconds)
Start Time Index: 00:43:12.747 UTC Thu Mar 16 2006
Number of Failed Operations due to a Disconnect      : 0
Number of Failed Operations due to a Timeout         : 0
Number of Failed Operations due to a Busy            : 0
Number of Failed Operations due to a No Connection   : 0
Number of Failed Operations due to an Internal Error : 0
Number of Failed Operations due to a Sequence Error  : 0
Number of Failed Operations due to a Verify Error    : 0
RTT Values:
  RTTAvg  : 2          RTTMin: 2          RTTMax : 2
  NumOfRTT: 1          RTTSum: 2          RTTSum2: 4

```

This table describes the significant fields shown in the display.

**Table 27: show ipsla statistics enhanced aggregated Field Descriptions**

Field	Description
Entry Number	Entry number.
Interval	Multiple of the frequency of the operation. The Enhanced interval field defines the interval in which statistics displayed by the <b>show ipsla statistics enhanced aggregated</b> command are aggregated. This field must be configured so that the enhanced aggregated statistics are displayed.
Bucket	Bucket index.
Start Time Index	Statistics that are aggregated depend on the interval configuration mode. The value depends on the interval configuration that is displayed.
RTT Values	Round-trip time statistics appear on the specified lines.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.
RTT Sum	Sum of all successful round-trip values, in milliseconds.
RTT Sum2	Sum of squares of the round-trip values, in milliseconds.



Field	Description
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.

**Related Commands**

Command	Description
<a href="#">show ipsla statistics, on page 239</a>	Displays the operational data for the IP SLA operation.
<a href="#">show ipsla statistics aggregated, on page 242</a>	Displays the statistical errors for all the IP SLA operations or for a specified operation.

# show ipsla twamp connection

To display the Two-Way Active Management Protocol (TWAMP) connections, use the **show ipsla twamp connection** command in the EXEC mode.

**show ipsla twamp connection** [ **detail***source-ip* | **requests** ]

## Syntax Description

<b>detail</b> <i>source-ip</i>	Displays details of the connection for a specified source-ip.
<b>requests</b>	Displays request details.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 5.1.1	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
ip-services	read

## Examples

This example shows how to run the **show ipsla twamp connection** command with the **requests** keyword:

```
RP/0/0/CPU0:router # show ipsla twamp connection requests
```

# show ipsla twamp session

To display the Two-way Active Management Protocol (TWAMP) sessions, use the **show ipsla twamp session** command in the EXEC mode.

**show ipsla twamp session** [ **source-ip** *host-name* ]

## Syntax Description

<b>source-ip</b> <i>host-name</i>	Displays session information for the specified source-ip and hostname.
-----------------------------------	--

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 5.1.1	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
monitor	read

## Examples

This example shows how to run **show ipsla twamp session** command:

```
RP/0/0/CPU0:router # show ipsla twamp session
```

# show ipsla twamp standards

To display the Two-way Active Management Protocol (TWAMP) standards, use the **show ipsla twamp standards** command in the EXEC mode.

The relevant RFC standards for the TWAMP server and TWAMP reflector are indicated.

**show ipsla twamp standards**

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

**Command Default** None

**Command Modes** EXEC mode

Release	Modification
Release 5.1.1	This command was introduced.

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

Task ID	Operation
ip-services	read

**Examples** This example shows how to use the **show ipsla twamp standards** command:

```
RP/0/0/CPU0:router # show ipsla twamp standards
Feature                Organization      Standard
TWAMP Server           IETF             RFC5357
TWAMP Reflector        IETF             RFC5357
```

## source address

To identify the address of the source device, use the **source address** command in the appropriate configuration mode. To use the best local address, use the **no** form of this command.

**source address** *ipv4-address*

**no source address**

### Syntax Description

*ipv4-address*

IP address or hostname of the source device.

### Command Default

IP SLA finds the best local address to the destination and uses it as the source address.

### Command Modes

IP SLA UDP echo configuration  
IP SLA UDP jitter configuration  
IP SLA ICMP path-jitter configuration  
IP SLA ICMP path-echo configuration  
IP SLA ICMP echo configuration  
IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	Support was added for IP SLA MPLS LSP Ping and IP SLA MPLS LSP Trace configuration modes.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to designate an IP address for the **source address** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# source address 192.0.2.9
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## source port

To identify the port of the source device, use the **source port** command in the appropriate configuration mode. To use the unused port number, use the **no** form of this command.

**source port** *port*

**no source port**

### Syntax Description

<b>port</b> <i>port</i>	Identifies the port number of the source device. Range is 1 to 65535.
-------------------------	---

### Command Default

IP SLA uses an unused port that is allocated by system.

### Command History

Releas	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

The **source port** command is not supported to configure ICMP operations; it is supported only to configure UDP operations.

The specified source port should not be used in other IPSLA operations configured on the same source IP address and source VRF.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to designate a port for the **source port** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# source port 11111
```

### Related Commands

Command	Description
<a href="#">operation</a> , <a href="#">on page 176</a>	Configures an IP SLA operation.

Command	Description
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# start-time

To determine the time when the operation or MPLS LSP monitor instance starts, use the **start-time** command in the appropriate configuration mode. To stop the operation and place it in the default state, use the **no** form of this command.

**start-time** {*hh:mm:ss* [*day* | *month* *day* *year*]} [**after** *hh:mm:ss*] [**now** | **pending**]

**no start-time**

## Syntax Description

<i>hh:mm:ss</i>	Absolute start time in hours, minutes, and seconds. You can use the 24-hour clock notation. For example, the <b>start-time</b> <i>01:02</i> is defined as 1:02 am, or <b>start-time</b> <i>13:01:30</i> is defined as start at 1:01 pm. and 30 seconds. The current day is used; unless, you specify a <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation. When you use the <i>month</i> argument, you are required to specify a day. You can specify the month by using the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day, in the range of 1 to 31, to start the operation. In addition, you must specify a month.
<i>year</i>	(Optional) Year in the range of 1993 to 2035.
<b>after</b> <i>hh:mm:ss</i>	Specifies that the operation starts at <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after the <b>start-time</b> command is used.
<b>now</b>	Specifies that the operation should start immediately.
<b>pending</b>	Specifies that no information is collected. The default value is the <b>pending</b> keyword.

## Command Default

If a month and day are not specified, the current month and day are used.

## Command Modes

IP SLA schedule configuration  
IP SLA MPLS LSP monitor schedule configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor schedule configuration mode.
Release 3.7.0	Added the ability to specify a year.

**Usage Guidelines**

If the **start-time** command is used in IP SLA operation mode, it configures the start time for the specific operation being configured. If the **start-time** command is used in IP SLA MPLS LSP monitor mode, it configures the start time for all monitor instances associated with the monitored provider edge (PE) routers.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **start-time** command option for the schedule operation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/0/CPU0:router(config-ipsla-sched)# start-time after 01:00:00
```

The following example shows how to use the **start-time** command in IP SLA MPLS LSP monitor schedule configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# schedule monitor 1
RP/0/0/CPU0:router(config-ipsla-mplsml-sched)# start-time after 01:00:00
```

The following example shows how to use the **start-time** command and specify a year for a scheduled operation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla operation 2
RP/0/0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/0/CPU0:router(config-ipsla-icmp-echo)# destination address 192.0.2.9
RP/0/0/CPU0:router(config-ipsla-icmp-echo)# exit
RP/0/0/CPU0:router(config-ipsla-op)# exit

RP/0/0/CPU0:router(config-ipsla)# schedule operation 2
RP/0/0/CPU0:router(config-ipsla-sched)# start 20:0:0 february 7 2008
RP/0/0/CPU0:router(config-ipsla-sched)#
```

**Related Commands**

Command	Description
<a href="#">life, on page 156</a>	Specifies the length of time to execute.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">recurring, on page 206</a>	Indicates that the operation starts automatically at the specified time and for the specified duration every day.
<a href="#">schedule monitor, on page 216</a>	Schedules an IP SLA MPLS LSP monitoring instance.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# statistics

To set the statistics collection parameters for the operation, use the **statistics** command in the appropriate configuration mode. To remove the statistics collection or use the default value, use the **no** form of this command.

**statistics** {**hourly**| **interval** *seconds*}

**no statistics** {**hourly**| **interval** *seconds*}

## Syntax Description

<b>hourly</b>	Sets the distribution for statistics configuration that is aggregated for over an hour.
<b>interval</b> <i>seconds</i>	Collects statistics over a specified time interval. Interval (in seconds) over which to collect statistics. Range is 1 to 3600 seconds.

## Command Default

None

## Command Modes

IP SLA operation UDP jitter configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

## Usage Guidelines

The **statistics interval** command is not supported for the configuration of ICMP path-echo and ICMP path-jitter operations, nor for the configuration of MPLS LSP monitor instances.

If the **statistics** command is used in IP SLA operation mode, it configures the statistics collection for the specific operation being configured. If the **statistics** command is used in IP SLA MPLS LSP monitor mode, it configures the statistics collection for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA UDP jitter operation for the **statistics** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-op-stats)#
```

The following example shows how to collect statistics for a specified time interval, using the **statistics** command in an IP SLA UDP jitter operation:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/0/CPU0:router(config-ipsla-op-stats)#
```

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA MPLS LSP monitor ping operation, using the **statistics** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# statistics hourly
RP/0/0/CPU0:router(config-ipsla-mplslm-stats)#
```

**Related Commands**

Command	Description
<a href="#">buckets (statistics hourly), on page 125</a>	Sets the number of hours in which statistics are kept.
<a href="#">buckets (statistics interval), on page 127</a>	Refers to the data buckets in which the enhanced history statistics are kept.
<a href="#">distribution count, on page 136</a>	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
<a href="#">distribution interval, on page 138</a>	Sets the time interval (in milliseconds) for each statistical distribution.
<a href="#">monitor, on page 170</a>	Configures an IP SLA MPLS LSP monitor instance.

Command	Description
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">maximum hops, on page 166</a>	Sets the number of hops in which statistics are maintained for each path for the IP SLA operation.
<a href="#">maximum paths (IP SLA), on page 168</a>	Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation.

## tag (IP SLA)

To create a user-specified identifier for an IP SLA operation, use the **tag** command in the appropriate configuration mode. To unset the tag string, use the **no** form of this command.

**tag** [ *text* ]

**no tag**

### Syntax Description

<i>text</i>	(Optional) Specifies a string label for the IP SLA operation.
-------------	---

### Command Default

No tag string is configured.

### Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	Support was added for IP SLA MPLS LSP ping and IP SLA MPLS LSP trace configuration modes.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

### Usage Guidelines

If the **tag** command is used in IP SLA operation mode, it configures the user-defined tag string for the specific operation being configured. If the **tag** command is used in IP SLA MPLS LSP monitor mode, it configures the user-defined tag string for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **tag** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# tag ipsla
```

The following example shows how to use the **tag** command in IP SLA MPLS LSP monitor ping configuration mode:

```
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# tag mplslm-tag
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# target ipv4

To specify the IPv4 address of the target router to be used in an MPLS LSP ping or MPLS LSP trace operation, use the **target ipv4** command in the appropriate configuration mode. To unset the address, use the **no** form of this command.

**target ipv4** *destination-address destination-mask*

**no target ipv4**

## Syntax Description

<i>destination-address</i>	IPv4 address of the target device to be tested.
<i>destination-mask</i>	Number of bits in the network mask of the target address. The network mask can be specified in either of two ways: <ul style="list-style-type: none"> <li>• The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address.</li> <li>• The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.</li> </ul>

## Command Default

None

## Command Modes

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.

## Usage Guidelines

Use the **target ipv4** command to specify the IPv4 address of the target router at the end of the LSP to be tested or traced and to indicate the destination as an Label Distribution Protocol (LDP) IPv4 address. The target IPv4 address identifies the appropriate label stack associated with the LSP.



### Note

Using the **target ipv4** command, you can configure only one LDP IPv4 address as the target in an MPLS LSP ping or trace operation. If you enter the command a second time and configure a different IPv4 target address, you overwrite the first IPv4 address.

An MPLS LSP ping operation tests connectivity in the LSP using verification on the specified Forwarding Equivalence Class (FEC)—in this case, LDP IPv4 prefix—between the ping origin and the egress node identified with the **target ipv4** command. This test is carried out by sending an MPLS echo request along the same data path as other packets belonging to the FEC. When the ping packet reaches the end of the path, it is sent to the control plane of the egress label switching router (LSR), which then verifies that it is indeed an egress for the LSP. The MPLS echo request contains information about the LSP that is being verified.

In an MPLS network, an MPLS LSP trace operation traces LSP paths to the target router identified with the **target ipv4** command. In the verification of LSP routes, a packet is sent to the control plane of each transit LSR, which performs various checks, including one that determines if it is a transit LSR for the LSP path. Each transit LSR also returns information related to the LSP being tested (that is, the label bound to the LDP IPv4 prefix).

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **target ipv4** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# target ipv4 192.168.1.4 255.255.255.255
```

### Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# target pseudowire

To specify the pseudowire as the target to be used in an MPLS LSP ping operation, use the **target pseudowire** command in IP SLA MPLS LSP ping configuration mode. To unset the target, use the **no** form of this command.

**target pseudowire** *destination-address circuit-id*

**no target pseudowire**

## Syntax Description

<i>destination-address</i>	IPv4 address of the target device to be tested.
<i>circuit-id</i>	Virtual circuit identifier. Range is 1 to 4294967295.

## Command Default

No default behavior or values

## Command Modes

IP SLA MPLS LSP ping configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

Use the **target pseudowire** command to specify a target router and to indicate the destination as a Layer 2 VPN pseudowire in an MPLS LSP ping operation. The **target pseudowire** command identifies the target address and the virtual circuit (VC) identifier.



### Note

Using the **target pseudowire** command, you can configure only one pseudowire address as the target in an MPLS LSP ping operation. If you use the command a second time and configure a different pseudowire target address, the first pseudowire address is overwritten.

A pseudowire target of the LSP ping operation allows active monitoring of statistics on Pseudowire Edge-to-Edge (PWE3) services across an MPLS network. PWE3 connectivity verification uses the Virtual Circuit Connectivity Verification (VCCV).

For more information on VCCV, refer to the VCCV draft, "Pseudowire Virtual Circuit Connectivity Verification (VCCV)" on the IETF web page.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **target pseudowire** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# target pseudowire 192.168.1.4 4211
```

## Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.

## target traffic-eng

To specify the target MPLS traffic engineering tunnel to be used in an MPLS LSP ping or MPLS LSP trace operation, use the **target traffic-eng** command in the appropriate configuration mode. To unset the tunnel, use the **no** form of this command.

**target traffic-eng tunnel** *tunnel-interface*

**no target traffic-eng**

### Syntax Description

<b>tunnel</b> <i>tunnel-interface</i>	Tunnel ID of an MPLS traffic-engineering tunnel (for example, tunnel 10) configured on the router. Range is 0 to 65535.
---------------------------------------	---

### Command Default

No default behavior or values

### Command Modes

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration

### Command History

Release	Modification
Release 3.4.0	This command was introduced.

### Usage Guidelines

Use the **target traffic-eng** command to specify a target router and to indicate the destination as an MPLS traffic-engineering (TE) tunnel in an MPLS LSP ping or MPLS LSP trace operation. The **target traffic-eng** command identifies the tunnel interface and the appropriate label stack associated with the LSP to be pinged or traced. An LSP tunnel interface is the head-end of a unidirectional virtual link to a tunnel destination.



#### Note

Using the **target traffic-eng** command, you can configure only one MPLS TE tunnel as the target in an MPLS LSP ping or trace operation. If you enter the command a second time and configure a different tunnel interfaces, you overwrite the first tunnel ID.

An IP SLA ping operation tests connectivity in the LSP using verification on the specified Forwarding Equivalence Class (FEC)—in this case, MPLS TE tunnel—between the ping origin and the egress node identified with the **target traffic-eng** command. This test is carried out by sending an MPLS echo request along the same data path as other packets belonging to the tunnel. When the ping packet reaches the end of the path, it is sent to the control plane of the egress label switching router (LSR), which then verifies that it is indeed an egress for the MPLS TE tunnel. The MPLS echo request contains information about the tunnel whose LSP path is being verified.

In an MPLS network, an IP SLA trace operation traces the LSP paths to a target router identified with the **target traffic-eng** command. In the verification of LSP routes, a packet is sent to the control plane of each

transit LSR, which performs various checks, including one that determines if it is a transit LSR for the LSP path. Each transit LSR also returns information related to the MPLS TE tunnel to see if the local forwarding information matches what the routing protocols determine as the LSP path.

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth.

For more information on MPLS traffic-engineering tunnels, refer to *MPLS Traffic Engineering and Enhancements*.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **target traffic-eng tunnel** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)# target traffic-eng tunnel 101
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# threshold

To set the lower-limit and upper-limit values, use the **threshold** command in IP SLA reaction condition configuration mode. To use the default value, use the **no** form of this command.

**threshold lower-limit** *value* **upper-limit** *value*

**no threshold lower-limit** *value* **upper-limit** *value*

## Syntax Description

<b>lower-limit</b> <i>value</i>	Specifies the threshold lower-limit value. Range is 1 to 4294967295 ms. Default <b>lower-limit</b> value is 3000 ms.
<b>upper-limit</b> <i>value</i>	Specifies the threshold upper-limit value. Range is 5000 to 4294967295 ms. Default <b>upper-limit</b> value is 5000 ms.

## Command Default

**lower-limit** *value*: 3000 ms

**upper-limit** *value*: 5000 ms

## Command Modes

IP SLA reaction condition configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **threshold** command is supported only when used with the **react** command and **jitter-average** and **packet-loss** keywords.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **jitter-average** keyword for the **threshold** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **packet-loss** keyword for the **threshold** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

#### Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.



# threshold type average

To take action on average values to violate a threshold, use the **threshold type average** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

**threshold type average** *number-of-probes*

**no threshold type**

## Syntax Description

<i>number-of-probes</i>	When the average of the last five values for the monitored element exceeds the upper threshold or the average of the last five values for the monitored element drops below the lower threshold, the action is performed as defined by the <b>action</b> command. Range is 1 to 16.
-------------------------	---

## Command Default

If there is no default value, no threshold type is configured.

## Command Modes

IP SLA reaction condition configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The **threshold type average** command is supported only when used with the **react** command and **jitter-average**, **packet-loss**, and **rtt** keywords.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to set the number of probes for the **react** command with the **jitter-average** keyword for the **threshold type average** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold type average 8
```

The following example shows how to set the number of probes for the **react** command with the **packet-loss** keyword for the **threshold type average** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold type average 8
```

#### Related Commands

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.

# threshold type consecutive

To take action after a number of consecutive violations, use the **threshold type consecutive** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

**threshold type consecutive** *occurrences*

**no threshold type**

## Syntax Description

<i>occurrences</i>	When the reaction condition is set for a consecutive number of occurrences, there is no default value. The number of occurrences is set when specifying the threshold type. The number of consecutive violations is 1 to 16.
--------------------	--

## Command Default

No default behavior or values

## Command Modes

IP SLA reaction condition configuration  
IP SLA MPLS LSP monitor reaction condition configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor reaction condition configuration mode.

## Usage Guidelines

If the **threshold type consecutive** command is used in IP SLA reaction condition mode, it configures the threshold for the specific operation being configured. If the **threshold type consecutive** command is used in IP SLA MPLS LSP monitor reaction condition configuration mode, it configures the threshold for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **threshold type consecutive** command:

```
RP/0/0/CPU0:router# configure
```

```

RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold type consecutive 8

```

The following example shows how to use the **threshold type consecutive** command in IP SLA MPLS LSP monitor reaction condition configuration mode:

```

RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplsml)# reaction monitor 2
RP/0/0/CPU0:router(config-ipsla-mplsml-react)# react connection-loss
RP/0/0/CPU0:router(config-ipsla-mplsml-react-cond)# threshold type consecutive 2

```

## Related Commands

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs.
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction monitor, on page 199</a>	Configures MPLS LSP monitoring reactions.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.

# threshold type immediate

To take action immediately upon a threshold violation, use the **threshold type immediate** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

**threshold type immediate**

**no threshold type**

## Syntax Description

This command has no keywords or arguments.

## Command Default

If there is no default value, no threshold type is configured.

## Command Modes

IP SLA reaction condition configuration

IP SLA MPLS LSP monitor reaction condition configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor reaction condition configuration mode.

## Usage Guidelines

When the reaction conditions, such as threshold violations, are met for the monitored element, the action is immediately performed as defined by the **action** command.

If the **threshold type immediate** command is used in IP SLA reaction condition mode, it configures the threshold for the specific operation being configured. If the **threshold type immediate** command is used in IP SLA MPLS LSP monitor reaction condition configuration mode, it configures the threshold for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **threshold type immediate** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
```

**threshold type immediate**

```
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold type immediate
```

The following example shows how to use the **threshold type immediate** command in IP SLA MPLS LSP monitor reaction condition configuration mode:

```
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# reaction monitor 2
RP/0/0/CPU0:router(config-ipsla-mplslm-react)# react connection-loss
RP/0/0/CPU0:router(config-ipsla-mplslm-react-cond)# threshold type immediate
```

**Related Commands**

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs.
<a href="#">mpls lsp-monitor, on page 174</a>	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction monitor, on page 199</a>	Configures MPLS LSP monitoring reactions.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type xofy, on page 283</a>	Takes action upon X violations in Y probe operations.

# threshold type xofy

To take action upon X violations in Y probe operations, use the **threshold type xofy** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

**threshold type xofy** *x-value y-value*

**no threshold type**

## Syntax Description

*x-value y-value* When the reaction conditions, such as threshold violations, are met for the monitored element after some *x* number of violations within some other *y* number of probe operations (for example, *x* of *y*), the action is performed as defined by the **action** command. Default is 5 for both *x-value* and *y-value*; for example, **xofy 5 5**. Range is 1 to 16.

## Command Default

If there is no default value, no threshold type is configured.

## Command Modes

IP SLA reaction condition configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **threshold type xofy** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/0/CPU0:router(config-ipsla-react-cond)# threshold type xofy 1 5
```

**Related Commands**

Command	Description
<a href="#">action (IP SLA), on page 119</a>	Specifies what action or combination of actions the operation performs.
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">reaction operation, on page 201</a>	Configures certain actions that are based on events under the control of the IP SLA agent.
<a href="#">react, on page 194</a>	Specifies an element to be monitored for a reaction.
<a href="#">threshold, on page 275</a>	Sets the lower-limit and upper-limit values.
<a href="#">threshold type average, on page 277</a>	Takes action on average values to violate a threshold.
<a href="#">threshold type consecutive, on page 279</a>	Takes action after a number of consecutive violations.
<a href="#">threshold type immediate, on page 281</a>	Takes action immediately upon a threshold violation.



## timeout (IP SLA)

To set the probe or control timeout interval, use the **timeout** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**timeout** *milliseconds*

**no timeout**

### Syntax Description

<i>milliseconds</i>	Sets the amount of time (in milliseconds) that the IP SLA operation waits for a response from the request packet. Range is 1 to 604800000.
---------------------	--

### Command Default

None.

### Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration  
 IP SLA MPLS LSP monitor ping configuration  
 IP SLA MPLS LSP monitor trace configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.4.0	Support was added for IP SLA MPLS LSP ping and IP SLA MPLS LSP trace configuration modes.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

### Usage Guidelines

If the **timeout** command is used in IP SLA operation mode, it configures the amount of time that a specific IP SLA operation waits for a response from the request packet. If the **timeout** command is used in IP SLA MPLS LSP monitor mode, it configures the amount of time that all operations associated with the monitored provider edge (PE) routers wait for a response from the request packet. This configuration is inherited by all LSP operations that are created automatically.

**Note**

The IP SLA responder needs at least one second to open a socket and program Local Packet Transport Services (LPTS). Therefore, configure the IP SLA timeout to at least 2000 milli seconds.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **timeout** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# timeout 10000
```

The following example shows how to use the **timeout** command in IP SLA MPLS LSP monitor configuration mode:

```
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)# timeout 10000
```

**Related Commands**

Command	Description
<a href="#">operation</a> , <a href="#">on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation</a> , <a href="#">on page 218</a>	Schedules an IP SLA operation.

# tos

To set the type of service (ToS) in a probe packet, use the **tos** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

**tos** *number*

**no tos**

## Syntax Description

<i>number</i>	Type of service number. Range is 0 to 255.
---------------	--

## Command Default

The type of service number is 0.

## Command Modes

IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

The ToS value is an 8-bit field in IP headers. The field contains information, such as precedence and ToS. The information is useful for policy routing and for features like Committed Access Rate (CAR) in which routers examine ToS values. When the type of service is defined for an operation, the IP SLA probe packet contains the configured tos value in the IP header.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **tos** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
```

tos

```
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# tos 60
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# ttl

To specify the time-to-live (TTL) value in the MPLS label of echo request packets, use the **ttl** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**ttl** *time-to-live*

**no ttl**

## Syntax Description

<i>time-to-live</i>	Maximum hop count for an echo request packet. Valid values are from 1 to 255.
---------------------	---

## Command Default

For an MPLS LSP ping operation, the default time-to-live value is 255.

For an MPLS LSP trace operations, the default time-to-live value is 30.

## Command Modes

IP SLA MPLS LSP ping configuration  
IP SLA MPLS LSP trace configuration  
IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor ping and monitor trace configuration modes.

## Usage Guidelines

Use the **ttl** command to set the maximum number of hops allowed for echo request packets in an MPLS LSP ping or MPLS LSP trace operation. Note that the number of possible hops differs depending the type of IP SLA operation:

- For MPLS LSP ping operations, valid values are from 1 to 255 and the default is 255.
- For MPLS LSP trace operations, valid values are from 1 to 30 and the default is 30.

If the **ttl** command is used in IP SLA operation mode, it configures the time-to-live value for the specific operation being configured. If the **ttl** command is used in IP SLA MPLS LSP monitor mode, it configures the time-to-live value for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **ttl** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)# ttl 200
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace, on page 296</a>	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

# type icmp echo

To use the ICMP echo operation type, use the **type icmp echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

**type icmp echo**

**no type icmp echo**

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

**Command Default** No default behavior or values

**Command Modes** IP SLA operation configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

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

Task ID	Task ID	Operations
	monitor	read, write

**Examples** The following example shows how to use the **type icmp echo** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/0/CPU0:router(config-ipsla-icmp-echo)#
```

Related Commands	Command	Description
	<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
	<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# type icmp path-echo

To use the ICMP path-echo operation type, use the **type icmp path-echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

**type icmp path-echo**

**no type icmp path-echo**

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

**Command Default** None

**Command Modes** IP SLA operation configuration

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

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

Task ID	Task ID	Operations
	monitor	read, write

**Examples** The following example shows how to use the **type icmp path-echo** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/0/CPU0:router(config-ipsla-icmp-path-echo)#
```

Related Commands	Command	Description
	<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
	<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.



# type icmp path-jitter

To use the ICMP path-jitter operation type, use the **type icmp path-jitter** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

**type icmp path-jitter**

**no type icmp path-jitter**

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

**Command Default** No default behavior or values

**Command Modes** IP SLA operation configuration

Release	Modification
Release 3.3.0	This command was introduced.

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

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to use the **type icmp path-jitter** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type icmp path-jitter
RP/0/0/CPU0:router(config-ipsla-icmp-path-jitter)#
```

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## type mpls lsp ping

To verify the end-to-end connectivity of a label switched path (LSP) and the integrity of an MPLS network, use the **type mpls lsp ping** command in the appropriate configuration mode. To remove the operation, use the **no** form of this command.

**type mpls lsp ping**

**no type mpls lsp ping**

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

**Command Default** No default behavior or values

**Command Modes** IP SLA operation configuration  
IP SLA MPLS LSP monitor definition configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced.
	Release 3.5.0	This command was added to IP SLA MPLS LSP monitor configuration mode.

**Usage Guidelines** Use the **type mpls lsp ping** command to configure parameters for an IP SLA LSP ping operation. After you enter the command, you enter IP SLA MPLS LSP Ping configuration mode.

An MPLS LSP ping operation tests connectivity between routers along an LSP path in an MPLS network and measures round-trip delay of the LSP by using an echo request and echo reply.

The MPLS LSP ping operation verifies LSP connectivity by using one of the supported Forwarding Equivalence Class (FEC) entities between the ping origin and egress node of each FEC. The following FEC types are supported for an MPLS LSP ping operation:

- IPv4 LDP prefixes (configured with the [target ipv4](#), on page 269 command)
- MPLS TE tunnels (configured with the [target traffic-eng](#), on page 273 command)
- Pseudowire (configured with the [target pseudowire](#), on page 271 command)

For MPLS LSP monitor ping operations, only IPv4 LDP prefixes are supported.

If the **type mpls lsp ping** command is used in IP SLA operation configuration mode, it configures the parameters for the specific operation being configured. If the **type mpls lsp ping** command is used in IP SLA MPLS LSP monitor configuration mode, it configures the parameters for all operations associated with the

monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

The following example shows how to use the **type mpls lsp ping** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-ping)#
```

The following example shows how to use the **type mpls lsp ping** command in IP SLA MPLS LSP monitor configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-ping)#
```

## Related Commands

Command	Description
<a href="#">monitor</a> , on page 170	Configures an IP SLA MPLS LSP monitor instance.
<a href="#">mpls lsp-monitor</a> , on page 174	Configures MPLS label switched path (LSP) monitoring.
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule monitor</a> , on page 216	Schedules an IP SLA MPLS LSP monitoring instance.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.

## type mpls lsp trace

To trace LSP paths and localize network faults in an MPLS network, use the **type mpls lsp trace** command in the appropriate configuration mode. To remove the operation, use the **no** form of this command.

**type mpls lsp trace**

**no type mpls lsp trace**

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

**Command Default** None

**Command Modes**

IP SLA operation configuration

IP SLA MPLS LSP monitor definition configuration

### Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	This command was added to IP SLA MPLS LSP monitor configuration mode.

### Usage Guidelines

Use the **type mpls lsp trace** command to configure parameters for an IP SLA LSP trace operation. After you enter the command, you enter IP SLA MPLS LSP Trace configuration mode.

An MPLS LSP trace operation traces the hop-by-hop route of LSP paths to a target router and measures the hop-by-hop round-trip delay for IPv4 LDP prefixes and TE tunnel FECs in an MPLS network. Echo request packets are sent to the control plane of each transit label switching router (LSR). A transit LSR performs various checks to determine if it is a transit LSR for the LSP path. A trace operation allows you to troubleshoot network connectivity and localize faults hop-by-hop.

In an MPLS LSP trace operation, each transit LSR returns information related to the type of Forwarding Equivalence Class (FEC) entity that is being traced. This information allows the trace operation to check if the local forwarding information matches what the routing protocols determine as the LSP path.

An MPLS label is bound to a packet according to the type of FEC used for the LSP. The following FEC types are supported for an MPLS LSP trace operation:

- LDP IPv4 prefixes (configured with the [target ipv4](#), on page 269 command)
- MPLS TE tunnels (configured with the [target traffic-eng](#), on page 273 command)

For MPLS LSP monitor trace operations, only IPv4 LDP prefixes are supported.

If the **type mpls lsp trace** command is used in IP SLA operation configuration mode, it configures the parameters for the specific operation being configured. If the **type mpls lsp trace** command is used in IP SLA

MPLS LSP monitor configuration mode, it configures the parameters for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **type mpls lsp trace** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mpls-lsp-trace)#
```

The following example shows how to use the **type mpls lsp trace** command in IP SLA MPLS LSP monitor configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-trace)#
```

### Related Commands

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule monitor, on page 216</a>	Schedules an IP SLA MPLS LSP monitoring instance.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type mpls lsp ping, on page 294</a>	Tests connectivity in an LSP path in an MPLS VPN.

# type udp echo

To use the UDP echo operation type, use the **type udp echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

**type udp echo**

**no type udp echo**

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

**Command Default** None

**Command Modes** IP SLA operation configuration

Release	Modification
Release 3.3.0	This command was introduced.

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

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to use the **type udp echo** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/0/CPU0:router(config-ipsla-udp-echo)#
```

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

# type udp jitter

To use the UDP jitter operation type, use the **type udp jitter** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

**type udp jitter**

**no type udp jitter**

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

**Command Default** None

**Command Modes** IP SLA operation configuration

Release	Modification
Release 3.3.0	This command was introduced.

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

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to use the **type udp jitter** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)#
```

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.

## type udp ipv4 address

To configure a permanent port in the IP SLA responder for UDP echo or jitter operations, use the **type udp ipv4 address** command in IP SLA responder configuration mode. To remove the specified permanent port, use the **no** form of this command.

**type udp ipv4 address** *ip-address* **port** *port*

**no type udp ipv4 address** *ip-address* **port** *port*

### Syntax Description

<i>ip-address</i>	Specifies the IPv4 address at which the operation is received.
<b>port</b> <i>port</i>	Specifies the port number at which the operation is received. Range is identical to the one used for the subagent that is, 1 to 65355.

### Command Default

If there is no default value, no permanent port is configured.

### Command Modes

IP SLA responder configuration

### Command History

Release	Modification
Release 3.3.0	This command was introduced.

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to configure a permanent port for the **type udp ipv4 address** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# responder
RP/0/0/CPU0:router(config-ipsla-resp)# type udp ipv4 address 192.0.2.11 port 10001
```



**Related Commands**

Command	Description
<a href="#">responder</a> , <a href="#">on page 205</a>	Enables the IP SLA responder for a UDP echo or jitter operation.

# verify-data

To check each IP SLA response for corruption, use the **verify-data** command in the appropriate configuration mode. To disable data corruption checking, use the **no** form of this command.

**verify-data**

**no verify-data**

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

**Command Default** The **verify-data** command is disabled.

**Command Modes** IP SLA UDP echo configuration  
IP SLA UDP jitter configuration

Release	Modification
Release 3.3.0	This command was introduced.

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

Task ID	Operations
monitor	read, write

**Examples** The following example shows how to use the **verify-data** command in IP SLA UDP jitter configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# verify-data
```

## Related Commands

Command	Description
<a href="#">operation</a> , on page 176	Configures an IP SLA operation.
<a href="#">schedule operation</a> , on page 218	Schedules an IP SLA operation.



## vrf (IP SLA)

To enable the monitoring of a Virtual Private Network (VPN) in an ICMP echo, ICMP path-echo, ICMP path-jitter, UDP echo, or UDP jitter operation, use the **vrf** command in the appropriate configuration mode. To disable VPN monitoring, use the **no** form of this command.

**vrf** *vrf-name*

**no vrf**

### Syntax Description

<i>vrf-name</i>	Name of the VPN. Maximum length is 32 alphanumeric characters.
-----------------	--

### Command Default

VPN monitoring is not configured for an IP SLA operation.

### Command Modes

IP SLA ICMP path-jitter configuration  
 IP SLA ICMP path-echo configuration  
 IP SLA ICMP echo configuration  
 IP SLA UDP echo configuration  
 IP SLA UDP jitter configuration  
 IP SLA MPLS LSP ping configuration  
 IP SLA MPLS LSP trace configuration

### Command History

Release	Modification
Release 3.4.0	This command was introduced.

### Usage Guidelines

Use the **vrf** command to configure a non-default VPN routing and forwarding (VRF) table for an IP SLA operation. A VPN is commonly identified using the name of a VRF table. If you use the **vrf** command in the configuration of an IP SLA operation, the *vrf-name* value is used to identify the VPN for the particular operation.

The default VRF table is used if no value is specified with the **vrf** command. If you enter a VPN name for an unconfigured VRF, the IP SLA operation fails and the following information is displayed in the results for the [show ipsla statistics](#), on [page 239](#) command:

```
Latest operation return code : VrfNameError
```

The **vrf** command is supported only to configure the following IP SLA operations:

- IP SLA ICMP echo

- IP SLA ICMP path-echo
- IP SLA ICMP path-jitter
- IP SLA UDP echo
- IP SLA UDP jitter
- IP SLA MPLS LSP ping
- IP SLA MPLS LSP trace

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

The following example shows how to use the **vrf** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# operation 1
RP/0/0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/0/CPU0:router(config-ipsla-udp-jitter)# vrf vpn2
```

**Related Commands**

Command	Description
<a href="#">operation, on page 176</a>	Configures an IP SLA operation.
<a href="#">schedule operation, on page 218</a>	Schedules an IP SLA operation.
<a href="#">type udp jitter, on page 299</a>	Configures an IP SLA UDP jitter operation.
<a href="#">type icmp echo, on page 291</a>	Configures an IP SLA ICMP echo operation.
<a href="#">type icmp path-echo, on page 292</a>	Configures an IP SLA ICMP path-echo operation.
<a href="#">type icmp path-jitter, on page 293</a>	Configures an IP SLA ICMP path-jitter operation.
<a href="#">type udp echo, on page 298</a>	Configures an IP SLA UDP echo operation.

## vrf (IP SLA MPLS LSP monitor)

To specify which virtual routing and forwarding instance (VRF) is monitored in an IP SLA MPLS LSP monitor ping or trace, use the **vrf** command in the appropriate configuration mode. To revert to the monitoring of all VRFs, use the **no** form of this command.

**vrf** *vrf-name*

**no vrf**

### Syntax Description

<i>vrf-name</i>	Name of the VRF. Maximum length is 32 alphanumeric characters.
-----------------	--

### Command Default

All VRFs are monitored.

### Command Modes

IP SLA MPLS LSP monitor ping configuration  
IP SLA MPLS LSP monitor trace configuration

### Command History

Release	Modification
Release 3.5.0	This command was introduced.

### Usage Guidelines

The **vrf** command in IP SLA MPLS LSP monitor configuration mode specifies to monitor a specific VRF in ping and trace operations. The default is that all VRFs are monitored.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

The following example shows how to use the **vrf** command in IP SLA MPLS LSP monitor configuration mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# ipsla
RP/0/0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/0/CPU0:router(config-ipsla-mplslm-lsp-trace)# vrf vpn-lsp
```

**Related Commands**

Command	Description
<a href="#">monitor</a> , on page 170	Configures an IP SLA MPLS LSP monitor instance.
<a href="#">type mpls lsp ping</a> , on page 294	Tests connectivity in an LSP path in an MPLS VPN.
<a href="#">type mpls lsp trace</a> , on page 296	Traces the hop-by-hop route of an LSP path in an MPLS VPN.







## Logging Services Commands

This module describes the Cisco IOS XR software commands to configure system logging (syslog) for system monitoring on the 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 detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [archive-length, page 311](#)
- [archive-size, page 312](#)
- [clear logging, page 313](#)
- [device, page 315](#)
- [file-size, page 316](#)
- [frequency \(logging\), page 317](#)
- [logging, page 318](#)
- [logging archive, page 320](#)
- [logging buffered, page 322](#)
- [logging console, page 324](#)
- [logging console disable, page 326](#)
- [logging events link-status, page 327](#)
- [logging events link-status \(interface\), page 329](#)

- [logging facility, page 332](#)
- [logging history, page 335](#)
- [logging history size, page 337](#)
- [logging hostnameprefix, page 339](#)
- [logging ipv4/ipv6, page 341](#)
- [logging localfilesize, page 344](#)
- [logging monitor, page 345](#)
- [logging source-interface, page 347](#)
- [logging suppress deprecated, page 349](#)
- [logging suppress duplicates, page 350](#)
- [logging trap, page 352](#)
- [service timestamps, page 354](#)
- [severity, page 356](#)
- [show logging, page 357](#)
- [show logging history, page 361](#)
- [terminal monitor, page 363](#)

# archive-length

To specify the length of time that logs are maintained in the logging archive, use the **archive-length** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**archive-length** *weeks*

**no archive-length**

## Syntax Description

<i>weeks</i>	Length of time (in weeks) that logs are maintained in the archive. Range is 0 to 4294967295.
--------------	--

## Command Default

*weeks*: 4 weeks

## Command Modes

Logging archive configuration

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **archive-length** command to specify the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to set the log archival period to 6 weeks:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# archive-length 6
```

## archive-size

To specify the amount of space allotted for syslogs on a device, use the **archive-size** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**archive-size** *size*

**no archive-size**

### Syntax Description

<i>size</i>	Amount of space (in MB) allotted for syslogs. The range is 0 to 2047.
-------------	---

### Command Default

*size*: 20 MB

### Command Modes

Logging archive configuration

### Command History

Release	Modification
Release 3.2	This command was introduced.

### Usage Guidelines

Use the **archive-length** command to specify the maximum total size of the syslog archives on a storage device. If the size is exceeded, then the oldest file in the archive is deleted to make space for new logs.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to set the allotted space for syslogs to 50 MB:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# archive-size 50
```

# clear logging

To clear system logging (syslog) messages from the logging buffer, use the **clear logging** command in EXEC mode.

**clear logging**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.2	This command was supported.
	Release 3.7.0	Removed the <b>internal</b> keyword.

**Usage Guidelines** Use the **clear logging** command to empty the contents of the logging buffer. When the logging buffer becomes full, new logged messages overwrite old messages.

Use the [logging buffered, on page 322](#) command to specify the logging buffer as a destination for syslog messages, set the size of the logging buffer, and limit syslog messages sent to the logging buffer based on severity.

Use the [show logging, on page 357](#) command to display syslog messages stored in the logging buffer.

Task ID	Task ID	Operations
	logging	execute

**Examples** This example shows how to clear the logging buffer:

```
RP/0/0/CPU0:router# clear logging
Clear logging buffer [confirm] [y/n] :y
```

**Related Commands**

Command	Description
<a href="#">logging buffered</a> , <a href="#">on page 322</a>	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits syslog messages sent to the logging buffer based on severity.
<a href="#">show logging</a> , <a href="#">on page 357</a>	Displays syslog messages stored in the logging buffer.

# device

To specify the device to be used for logging syslogs, use the **device** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**device** {**disk0**| **disk1**| **harddisk**}

**no device**

## Syntax Description

<b>disk0</b>	Uses disk0 as the archive device.
<b>disk1</b>	Uses disk1 as the archive device.
<b>harddisk</b>	Uses the harddisk as the archive device.

## Command Default

None

## Command Modes

Logging archive configuration

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **device** command to specify where syslogs are logged. The logs are created under the directory <device>/var/log. If the device is not configured, then all other logging archive configurations are rejected. Similarly, the configured device cannot be removed until the other logging archive configurations are removed. It is recommended that the syslogs be archived to the harddisk because it has more capacity.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to specify disk1 as the device for logging syslog messages:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# device disk1
```

# file-size

To specify the maximum file size for a log file in the archive, use the **file-size** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**file-size** *size*

**no file-size**

## Syntax Description

<i>size</i>	Maximum file size (in MB) for a log file in the logging archive. The range is 1 to 2047.
-------------	--

## Command Default

*size*: 1 MB

## Command Modes

Logging archive configuration

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **file-size** command to specify the maximum file size that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to set the maximum log file size to 10 MB:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# file-size 10
```



## frequency (logging)

To specify the collection period for logs, use the **frequency** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**frequency** {**daily**|**weekly**}

**no frequency**

### Syntax Description

<b>daily</b>	Logs are collected daily.
--------------	---------------------------

<b>weekly</b>	Logs are collected weekly.
---------------	----------------------------

### Command Default

Logs are collected daily.

### Command Modes

Logging archive configuration

### Command History

Release	Modification
Release 3.2	This command was introduced.

### Usage Guidelines

Use the **frequency** command to specify if logs are collected daily or weekly.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to specify that logs are collected weekly instead of daily:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# frequency weekly
```

# logging

To specify a system logging (syslog) server host as the recipient of syslog messages, use the **logging** command in Global Configuration mode. To remove the **logging** command from the configuration file and delete a syslog server from the list of syslog server hosts, use the **no** form of this command.

**logging** {*ip-address*| *hostname*} { **vrf** **severity** [**alerts**| **critical**| **debugging**| **emergencies**| **error**| **info**| **notifications**| **warning**] }

**no logging** {*ip-address*| *hostname*} { **vrf** **severity** [**alerts**| **critical**| **debugging**| **emergencies**| **error**| **info**| **notifications**| **warning**] }

## Syntax Description

<i>ip-address</i>   <i>hostname</i>	IP address or hostname of the host to be used as a syslog server.
<b>severity</b>	Set severity of messages for particular remote host/vrf.
<b>alerts</b>	Specifies Immediate action needed
<b>critical</b>	Specifies Critical conditions
<b>debugging</b>	Specifies Debugging messages
<b>emergencies</b>	Specifies System is unusable
<b>error</b>	Specifies Error conditions
<b>info</b>	Specifies Informational messages
<b>notifications</b>	Specifies Normal but significant conditions
<b>warning</b>	Specifies Warning conditions
<b>vrf</b> <i>vrf-name</i>	Name of the VRF. Maximum length is 32 alphanumeric characters.

## Command Default

No syslog server hosts are configured as recipients of syslog messages.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 4.1.0	The vrf keyword was added.
Release 4.3	The severity keyword was added.

**Usage Guidelines**

Use the **logging** command to identify a syslog server host to receive messages. By issuing this command more than once, you build a list of syslog servers that receive messages.

When syslog messages are sent to a syslog server, the Cisco IOS XR software includes a numerical message identifier in syslog messages. The message identifier is cumulative and sequential. The numerical identifier included in syslog messages sent to syslog servers provides a means to determine if any messages have been lost.

Use the [logging trap, on page 352](#) command to limit the messages sent to snmp server.

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to log messages to a host named host1:

```
RP/0/0/CPU0:router(config)# logging host1
RP/0/0/CPU0:router(config)#logging A.B.C.D
    severity Set severity of messages for particular remote host/vrf
    vrf      Set VRF option
RP/0/0/CPU0:router(config)#logging A.B.C.D
RP/0/0/CPU0:router(config)#commit
Wed Nov 14 03:47:58.976 PST

RP/0/0/CPU0:router(config)#do show run logging
Wed Nov 14 03:48:10.816 PST
logging A.B.C.D vrf default severity info
```

**Note**

Default level is severity info.

**Related Commands**

Command	Description
<a href="#">logging trap, on page 352</a>	Limits the messages sent to snmp server.

# logging archive

To configure attributes for archiving syslogs, use the **logging archive** command in Global Configuration mode. To exit the **logging archive** submode, use the **no** form of this command.

**logging archive** {archive-length| archive-size| device| file-size| frequency| severity}

**no logging archive**

## Syntax Description

<b>archive-length</b>	Maximum no of weeks that the log is maintained. Minimum number of week is 1 and the maximum number of weeks are 256. Recommended is 4 weeks.
<b>archive-size</b>	Total size of the archive. Value range from 1 MB to 2047 MB. Recommended is 20 MB.
<b>device</b>	Use configured devices (disk0   disk1   harddisk) as the archive device. Recommended is harddisk.
<b>file-size</b>	Maximum file size for a single log file. Value range from 1 MB to 2047 MB. Recommended is 1 MB.
<b>frequency</b>	Collection interval (daily or weekly) for logs. Recommend is daily.
<b>severity</b>	Specifies the filter levels for log messages to archive. <ul style="list-style-type: none"> <li>• alerts - Immediate action needed (severity=1)</li> <li>• critical - Critical conditions (severity=2)</li> <li>• debugging - Debugging messages (severity=7)</li> <li>• emergencies - System is unusable (severity=0)</li> <li>• errors - Error conditions (severity=3)</li> <li>• informational - Informational messages (severity=6)</li> <li>• notifications - Normal but significant conditions (severity=5)</li> <li>• warnings Warning conditions (severity=4)</li> </ul> <p>Recommended is informational (severity=6).</p>

## Command Default

None

## Command Modes

Global Configuration mode

**Command History**

Release	Modification
Release 3.2	This command was introduced.

**Usage Guidelines**

Use the **logging archive** command to configure attributes for archiving syslogs. This command enters logging archive configuration mode and allows you to configure the commands.

**Note**

The configuration attributes must be explicitly configured in order to use the logging archive feature.

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to enter logging archive configuration mode and change the device to be used for logging syslogs to disk1:

```
RP/0/0/CPU0:router(config)# logging archive  
RP/0/0/CPU0:router(config-logging-arch)# device disk1
```

# logging buffered

To specify the logging buffer as a destination for system logging (syslog) messages, use the **logging buffered** command in Global Configuration mode. To remove the **logging buffered** command from the configuration file and cancel the use of the buffer, use the **no** form of this command.

**logging buffered** {*size*| *severity*}

**no logging buffered** {*size*| *severity*}

## Syntax Description

<i>size</i>	Size of the buffer, in bytes. Range is 307200 to 125000000 bytes. The default is 307200 bytes.
<i>severity</i>	Severity level of messages that display on the console. Possible severity levels and their respective system conditions are listed under <a href="#">Table 28: Severity Levels for Messages, on page 322</a> in the “Usage Guidelines” section. The default is <b>debugging</b> .

## Command Default

*size*: 307200 bytes

*severity*: **debugging**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 4.0.0	The value of size argument is changed from 4096 to 307200.

## Usage Guidelines

Use the **logging buffered** command to copy messages to the logging buffer. The logging buffer is circular, so newer messages overwrite older messages after the buffer is filled. This command is related to the **show logging buffer** command, which means that when you execute a **logging buffered warnings** command, it enables the logging for all the levels below the configured level, including log for LOG\_ERR, LOG\_CRIT, LOG\_ALERT, LOG\_EMERG, and LOG\_WARNING messages. Use the **logging buffer size** to change the size of the buffer.

The value specified for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the console terminal. See [Table 28: Severity Levels for Messages, on page 322](#) for a list of the possible severity level keywords for the *severity* argument.

This table describes the acceptable severity levels for the *severity* argument.

**Table 28: Severity Levels for Messages**

Level Keywords	Level	Description	Syslog Definition
emergencies	0	Unusable system	LOG_EMERG
alerts	1	Need for immediate action	LOG_ALERT
critical	2	Critical condition	LOG_CRIT
errors	3	Error condition	LOG_ERR
warnings	4	Warning condition	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational message only	LOG_INFO
debugging	7	Debugging message	LOG_DEBUG

**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to set the severity level of syslog messages logged to the buffer to **notifications**:

```
RP/0/0/CPU0:router(config)# logging buffered notifications
```

**Related Commands**

Command	Description
<a href="#">archive-size, on page 312</a>	Clears messages from the logging buffer.
<a href="#">show logging, on page 357</a>	Displays syslog messages stored in the logging buffer.

# logging console

To enable logging of system logging (syslog) messages logged to the console by severity level, use the **logging console** command in Global Configuration mode. To return console logging to the default setting, use the **no** form of this command.

**logging console** [*severity*] **disable**

**no logging console**

## Syntax Description

<i>severity</i>	Severity level of messages logged to the console, including events of a higher severity level (numerically lower). The default is <b>informational</b> . Settings for the severity levels and their respective system conditions are listed in <a href="#">Table 28: Severity Levels for Messages, on page 322</a> under the “Usage Guidelines” section for the <a href="#">logging buffered, on page 322</a> command.
<b>disable</b>	Removes the <b>logging console</b> command from the configuration file and disables logging to the console terminal.

## Command Default

By default, logging to the console is enabled.

*severity*: **informational**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	Added the <b>disable</b> keyword. The command <b>no logging console</b> was changed to reset console logging to the default setting.

## Usage Guidelines

Use the **logging console** command to prevent debugging messages from flooding your screen.

The **logging console** is for the console terminal. The value specified for the *severity* argument causes messages at that level and at numerically lower levels (higher severity levels) to be displayed on the console.

Use the **logging console disable** command to disable console logging completely.

Use the **no logging console** command to return the configuration to the default setting.

Use the [show logging, on page 357](#) command to display syslog messages stored in the logging buffer.



**Task ID**

Task ID	Operations
logging	read, write

**Examples**

This example shows how to change the level of messages displayed on the console terminal to **alerts** (1), which means that **alerts** (1) and **emergencies** (0) are displayed:

```
RP/0/0/CPU0:router(config)# logging console alerts
```

This example shows how to disable console logging:

```
RP/0/0/CPU0:router(config)# logging console disable
```

This example shows how to return console logging to the default setting (the console is enabled, *severity*: **informational**):

```
RP/0/0/CPU0:router# no logging console
```

**Related Commands**

Command	Description
<a href="#">show logging, on page 357</a>	Displays syslog messages stored in the logging buffer.

# logging console disable

To disable logging of system logging (syslog) messages logged to the console, use the **logging console disable** command in Global Configuration mode. To return logging to the default setting, use the **no** form of this command.

**logging console disable**

**no logging console disable**

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

**Command Default** By default, logging is enabled.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

**Usage Guidelines**

Use the **logging console disable** command to disable console logging completely.

Use the **no logging console disable** command to return the configuration to the default setting.

Task ID	Task ID	Operations
	logging	read, write

**Examples** This example shows how to disable syslog messages:

```
RP/0/0/CPU0:router(config)# logging console disable
```

# logging events link-status

To enable the logging of link-status system logging (syslog) messages for logical and physical links, use the **logging events link-status** command in Global Configuration mode. To disable the logging of link status messages, use the **no** form of this command.

**logging events link-status** {**disable**|**software-interfaces**}

**no logging events link-status** [**disable**|**software-interfaces**]

## Syntax Description

<b>disable</b>	Disables the logging of link-status messages for all interfaces, including physical links.
<b>software-interfaces</b>	Enables the logging of link-status messages for logical links as well as physical links.

## Command Default

The logging of link-status messages is enabled for physical links.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	The <b>logical</b> and <b>physical</b> keywords were replaced by the <b>software-interfaces</b> and <b>disable</b> keywords.

## Usage Guidelines

When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages.

Use the **no logging events link-status** command to enable the logging of link-status messages for physical links only, which is the default behavior.



### Note

Enabling the [logging events link-status \(interface\)](#), on page 329 command on a specific interface overrides the global configuration set using the **logging events link-status** command described in this section.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to disable the logging of physical and logical link-status messages:

```
RP/0/0/CPU0:router(config)# logging events link-status disable
```

## Related Commands

Command	Description
<a href="#">logging events link-status (interface), on page 329</a>	Enables the logging of link-status system logging (syslog) messages on a specific interface for virtual interfaces and subinterfaces.

# logging events link-status (interface)

To enable the logging of link-status system logging (syslog) messages on a specific interface for virtual interfaces and subinterfaces, use the **logging events link-status** command in the appropriate interface or subinterface mode. To disable the logging of link status messages, use the **no** form of this command.

**logging events link-status**

**no logging events link-status**

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

**Command Default** The logging of link-status messages is disabled for virtual interfaces and subinterfaces.

**Command Modes** Interface configuration

Release	Modification
Release 3.2	This command was introduced.

**Usage Guidelines** When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages. The **logging events link-status** command enables messages for virtual interfaces and subinterfaces only.

The **logging events link-status** command allows you to enable and disable logging on a specific interface for bundles, tunnels, and VLANs.

Use the **no logging events link-status** command to disable the logging of link-status messages.



**Note** Enabling the **logging events link-status** command on a specific interface overrides the global configuration set using the [logging events link-status](#), [on page 327](#) command in global configuration mode.

Task ID	Operations
logging	read, write

**Examples** This example shows the results of turning on logging for a bundle interface:

```
RP/0/0/CPU0:router(config)# int bundle-pos 1
```

```

RP/0/0/CPU0:router(config-if)# logging events link-status
RP/0/0/CPU0:router(config-if)# no shutdown
RP/0/0/CPU0:router(config-if)# commit

LC/0/4/CPU0:Jun 29 12:51:26.887 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface POS0/4/0/0, changed state to Up

LC/0/4/CPU0:Jun 29 12:51:26.897 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface POS0/4/0/0, changed state to Up

RP/0/0/CPU0:router(config-if)#
RP/0/0/CPU0:router(config-if)# shutdown
RP/0/0/CPU0:router(config-if)# commit

LC/0/4/CPU0:Jun 29 12:51:32.375 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface POS0/4/0/0, changed state to Down

LC/0/4/CPU0:Jun 29 12:51:32.376 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface POS0/4/0/0, changed state to
Down

```

This example shows a sequence of commands for a tunnel interface with and without logging turned on:

```

RP/0/0/CPU0:router(config)# int tunnel-te 1
RP/0/0/CPU0:router(config-if)# commit
RP/0/0/CPU0:router(config-if)# shutdown
RP/0/0/CPU0:router(config-if)# commit
RP/0/0/CPU0:router(config-if)# no shutdown
RP/0/0/CPU0:router(config-if)# commit
RP/0/0/CPU0:router(config-if)# logging events link-status
RP/0/0/CPU0:router(config-if)# commit
RP/0/0/CPU0:router(config-if)# shutdown
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:Jun 29 14:05:57.732 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Administratively Down

RP/0/0/CPU0:Jun 29 14:05:57.733 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Administratively Down

RP/0/0/CPU0:router(config-if)# no shutdown
RP/0/0/CPU0:router(config-if)# commit

RP/0/0/CPU0:Jun 29 14:06:02.104 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Down

RP/0/0/CPU0:Jun 29 14:06:02.109 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Down

```

This example shows the same process for a subinterface:

```

RP/0/0/CPU0:router(config)# int gigabitEthernet 0/5/0/0.1
RP/0/0/CPU0:router(config-subif)# commit
RP/0/0/CPU0:router(config-subif)# shutdown
RP/0/0/CPU0:router(config-subif)# commit
RP/0/0/CPU0:router(config-subif)# no shutdown
RP/0/0/CPU0:router(config-subif)# commit
RP/0/0/CPU0:router(config-subif)# logging events link-status
RP/0/0/CPU0:router(config-subif)# commit
RP/0/0/CPU0:router(config-subif)# shutdown
RP/0/0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:46.710 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface GigabitEthernet0/5/0/0.1, changed
state to Administratively Down

LC/0/5/CPU0:Jun 29 14:06:46.726 : ifmgr[142]:

```

```
%PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/5/0/0.1, changed state to  
Administratively Down
```

```
RP/0/0/CPU0:router(config-subif)# no shutdown  
RP/0/0/CPU0:router(config-subif)# commit
```

```
LC/0/5/CPU0:Jun 29 14:06:52.229 : ifmgr[142]:  
%PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/5/0/0.1, changed state to Up
```

```
LC/0/5/CPU0:Jun 29 14:06:52.244 : ifmgr[142]:  
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface GigabitEthernet0/5/0/0.1, changed  
state to Down
```

# logging facility

To configure the type of syslog facility in which system logging (syslog) messages are sent to syslog servers, use the **logging facility** command in Global Configuration mode. To remove the **logging facility** command from the configuration file and disable the logging of messages to any facility type, use the **no** form of this command.

**logging facility** [ *type* ]

**no logging facility**

## Syntax Description

*type* (Optional) Syslog facility type. The default is **local7**. Possible values are listed under [Table 29: Facility Type Descriptions](#), on page 332 in the “Usage Guidelines” section.

## Command Default

*type*: **local7**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

This table describes the acceptable options for the *type* argument.

**Table 29: Facility Type Descriptions**

Facility Type	Description
auth	Authorization system
cron	Cron/at facility
daemon	System daemon
kern	Kernel
local0	Reserved for locally defined messages
local1	Reserved for locally defined messages
local2	Reserved for locally defined messages



Facility Type	Description
local3	Reserved for locally defined messages
local4	Reserved for locally defined messages
local5	Reserved for locally defined messages
local6	Reserved for locally defined messages
local7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Use the [logging, on page 318](#) command to specify a syslog server host as a destination for syslog messages.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure the syslog facility to the **kern** facility type:

```
RP/0/0/CPU0:router(config)# logging facility kern
```

**Related Commands**

Command	Description
<a href="#">logging</a> , on page 318	Specifies a syslog server host as a destination for syslog messages.

# logging history

To change the severity level of system logging (syslog) messages sent to the history table on the router and a Simple Network Management Protocol (SNMP) network management station (NMS), use the **logging history** command in Global Configuration mode. To remove the **logging history** command from the configuration and return the logging of messages to the default level, use the **no** form of this command.

**logging history** *severity*

**no logging history**

## Syntax Description

<i>severity</i>	Severity level of messages sent to the history table on the router and an SNMP NMS, including events of a higher severity level (numerically lower). Settings for the severity levels and their respective system conditions are listed in <a href="#">Table 28: Severity Levels for Messages</a> , on page 322 under the “Usage Guidelines” section for the <b>logging buffered</b> command.
-----------------	---

## Command Default

*severity*: **warnings**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Logging of messages to an SNMP NMS is enabled by the **snmp-server enable traps** command. Because SNMP traps are inherently unreliable and much too important to lose, at least one syslog message, the most recent message, is stored in a history table on the router.

Use the **logging history** command to reflect the history of last 500 syslog messages. For example, when this command is issued, the last 500 syslog messages with severity less than warning message are displayed in the output of **show logging history** command.

Use the [show logging history](#), on page 361 command to display the history table, which contains table size, message status, and message text data.

Use the [logging history size](#), on page 337 command to change the number of messages stored in the history table.

The value specified for the *severity* argument causes messages at that severity level and at numerically lower levels to be stored in the history table of the router and sent to the SNMP NMS. Severity levels are numbered 0 to 7, with 1 being the most important message and 7 being the least important message (that is, the lower the number, the more critical the message). For example, specifying the level critical with the **critical** keyword causes messages at the severity level of **critical** (2), **alerts** (1), and **emergencies** (0) to be stored in the history table and sent to the SNMP NMS.

The **no logging history** command resets the history level to the default.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to change the level of messages sent to the history table and to the SNMP server to **alerts** (1), which means that messages at the severity level of **alerts** (1) and **emergencies** (0) are sent:

```
RP/0/0/CPU0:router(config)# logging history alerts
```

### Related Commands

Command	Description
<a href="#">logging history size, on page 337</a>	Changes the number of messages stored in the history table.
<a href="#">show logging history, on page 361</a>	Displays information about the state of the syslog history table.

# logging history size

To change the number of system logging (syslog) messages that can be stored in the history table, use the **logging history size** command in Global Configuration mode. To remove the **logging history size** command from the configuration and return the number of messages to the default value, use the **no** form of this command.

**logging history size** *number*

**no logging history** *number*

## Syntax Description

<i>number</i>	Number from 1 to 500 indicating the maximum number of messages that can be stored in the history table. The default is 1 message.
---------------	---

## Command Default

*number*: 1 message

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **logging history size** command to change the number of messages that can be stored in this history table. When the history table is full (that is, when it contains the maximum number of messages specified with the command), the oldest message is deleted from the table to allow the new message to be stored.

Use the [logging history](#), on page 335 command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to set the number of messages stored in the history table to 20:

```
RP/0/0/CPU0:router(config)# logging history size 20
```

**Related Commands**

Command	Description
<a href="#">logging history, on page 335</a>	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
<a href="#">show logging history, on page 361</a>	Displays information about the state of the syslog history table.

# logging hostnameprefix

To append a hostname prefix to system logging (syslog) messages logged to syslog servers, use the **logging hostnameprefix** command in Global Configuration mode. To remove the **logging hostnameprefix** command from the configuration file and disable the logging host name prefix definition, use the **no** form of this command.

**logging hostnameprefix** *hostname*

**no logging hostnameprefix**

## Syntax Description

<i>hostname</i>	Hostname that appears in messages sent to syslog servers.
-----------------	---

## Command Default

No hostname prefix is added to the messages logged to the syslog servers.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **logging hostnameprefix** command to append a hostname prefix to messages sent to syslog servers from the router. You can use these prefixes to sort the messages being sent to a given syslog server from different networking devices.

Use the [logging, on page 318](#) command to specify a syslog server host as a destination for syslog messages.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to add the hostname prefix host1 to messages sent to the syslog servers from the router:

```
RP/0/0/CPU0:router(config)# logging hostnameprefix host1
```

**Related Commands**

Command	Description
<a href="#">logging</a> , on page 318	Specifies a syslog server host as a destination for syslog messages.



## logging ipv4/ipv6

To configure the differentiated services code point (DSCP) or the precedence value for the IPv4 or IPv6 header of the syslog packet in the egress direction, use the **logging {ipv4 | ipv6} {dscp dscp-value | precedence {number | name}}** command in EXEC mode. To remove the configured DSCP or precedence value, use the **no** form of this command.

**logging {ipv4 | ipv6} {dscp dscp-value | precedence {number | name}}**

**no logging {ipv4 | ipv6} {dscp dscp-value | precedence {number | name}}**

### Syntax Description

<b>ipv4 / ipv6</b>	Sets the DSCP or precedence bit for IPv4 or IPv6 packets.
<b>dscp</b> <i>dscp-value</i>	Specifies differentiated services code point value or per hop behavior values (PHB). For more information on PHB values, see Usage Guideline section below. The range is from 0 to 63. The default value is 0.
<b>precedence</b> { <i>number</i>   <i>name</i> }	<p>Sets Type of Service (TOS) precedence value. You can specify either a precedence number or name. The range of argument <i>number</i> is between 0 to 7.</p> <p>The <i>name</i> argument has following keywords:</p> <ul style="list-style-type: none"> <li>• routine—Match packets with routine precedence ( 0)</li> <li>• priority—Match packets with priority precedence (1)</li> <li>• immediate—Match packets with immediate precedence (2)</li> <li>• flash—Match packets with flash precedence (3)</li> <li>• flash-override—Match packets with flash override precedence (4)</li> <li>• critical—Match packets with critical precedence (5)</li> <li>• internet—Match packets with internetwork control precedence (6)</li> <li>• network—Match packets with network control precedence (7)</li> </ul>

### Command Default

None.

### Command Modes

EXEC mode

### Command History

Release	Modification
Release 5.1.1	The <b>ipv4</b> and <b>ipv6</b> keywords were added.

**Usage Guidelines**

By specifying PHB values you can further control the format of locally generated syslog traffic on the network. You may provide these PHB values:

- af11—Match packets with AF11 DSCP (001010)
- af12—Match packets with AF12 dscp (001100)
- af13—Match packets with AF13 dscp (001110)
- af21— Match packets with AF21 dscp (010010)
- af22—Match packets with AF22 dscp (010100)
- af23—Match packets with AF23 dscp (010110)
- af31—Match packets with AF31 dscp (011010)
- af32—Match packets with AF32 dscp (011100)
- af33—Match packets with AF33 dscp (011110)
- af41—Match packets with AF41 dscp (100010)
- af42—Match packets with AF42 dscp (100100)
- af43— Match packets with AF43 dscp (100110)
- cs1—Match packets with CS1(precedence 1) dscp (001000)
- cs2—Match packets with CS2(precedence 2) dscp (010000)
- cs3—Match packets with CS3(precedence 3) dscp (011000)
- cs4—Match packets with CS4(precedence 4) dscp (100000)
- cs5—Match packets with CS5(precedence 5) dscp (101000)
- cs6—Match packets with CS6(precedence 6) dscp (110000)
- cs7—Match packets with CS7(precedence 7) dscp (111000)
- default—Match packets with default dscp (000000)
- ef—Match packets with EF dscp (10111)

Assured Forwarding (AF) PHB group is a means for a provider DS domain to offer different levels of forwarding assurances for IP packets. The Assured Forwarding PHB guarantees an assured amount of bandwidth to an AF class and allows access to additional bandwidth, if obtainable.

For example AF PHB value af11 - Match packets with AF11 DSCP (001010), displays the DSCP values as 10 and 11. The DSCP bits are shown as 001010 and 001011 .

AF11 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (1)
- Dropped last in AF1 class

Similarly AF PHB value af12 - Match packets with AF12 dscp (001100), displays the DSCP values as 12 and 13. The DSCP bits are shown as 001100 and 001101.

AF12 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (2)
- Dropped second in AF1 class

Class Selector (CS) provides backward compatibility bits,

CS PHB value cs1 - Match packets with CS1(precedence 1) dscp (001000)

CS1 stands for:

- CS1 DSCP bits are displayed as 001000 and 001001
- priority stated as 1

Expedited Forwarding (EF) PHB is defined as a forwarding treatment to build a low loss, low latency, assured bandwidth, end-to-end service. These characteristics are suitable for voice, video and other realtime services.

EF PHB Value ef - Match packets with EF dscp (101110) - this example states the recommended EF value (used for voice traffic).

#### Task ID

Task ID	Operation
logging	read, write

#### Examples

This example shows how to configure DSCP value as 1 for IPv4 header of syslog packet.

```
RP/0/0/CPU0:router(config)#logging ipv4 dscp 1
```

This example shows how to configure DSCP value as 21 for IPv6 header of syslog packet.

```
RP/0/0/CPU0:router(config)#logging ipv6 dscp 21
```

This example shows how to configure precedence value as 5 for IPv6 header of syslog packet.

```
RP/0/0/CPU0:router(config)#logging ipv6 precedence 5
```

# logging localfilesize

To specify the size of the local logging file, use the **logging localfilesize** command in Global Configuration mode. To remove the **logging localfilesize** command from the configuration file and restore the system to the default condition, use the **no** form of this command.

**logging localfilesize** *bytes*

**no logging localfilesize** *bytes*

## Syntax Description

<i>bytes</i>	Size of the local logging file in bytes. Range is 0 to 4294967295. Default is 32000 bytes.
--------------	--

## Command Default

*bytes*: 32000 bytes

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **logging localfilesize** command to set the size of the local logging file.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to set the local logging file to 90000 bytes:

```
RP/0/0/CPU0:router(config)# logging localfilesize 90000
```

## Related Commands

Command	Description
<a href="#">show logging</a> , <a href="#">on page 357</a>	Displays syslog messages stored in the logging buffer.

# logging monitor

To specify terminal lines other than the console terminal as destinations for system logging (syslog) messages and limit the number of messages sent to terminal lines based on severity, use the **logging monitor** command in Global Configuration mode. To remove the **logging monitor** command from the configuration file and disable logging to terminal lines other than the console line, use the **no** form of this command.

**logging monitor** [ *severity* ]

**no logging monitor**

## Syntax Description

<i>severity</i>	(Optional) Severity level of messages logged to the terminal lines, including events of a higher severity level (numerically lower). The default is <b>debugging</b> . Settings for the severity levels and their respective system conditions are listed under <a href="#">Table 28: Severity Levels for Messages, on page 322</a> in the “Usage Guidelines” section for the <b>logging buffered</b> command.
-----------------	--

## Command Default

*severity*: **debugging**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

The **logging monitor** is for the terminal monitoring. Use the **logging monitor** command to restrict the messages displayed on terminal lines other than the console line (such as virtual terminals). The value set for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the monitor.

Use the [terminal monitor, on page 363](#) command to enable the display of syslog messages for the current terminal session.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to set the severity level of messages logged to terminal lines to errors:

```
RP/0/0/CPU0:router(config)# logging monitor errors
```

**Related Commands**

Command	Description
<a href="#">terminal monitor</a> , on page 363	Enables the display of syslog messages for the current terminal session.

# logging source-interface

To set all system logging (syslog) messages being sent to syslog servers to contain the same IP address, regardless of which interface the syslog message uses to exit the router, use the **logging source-interface** command in Global Configuration mode. To remove the **logging source-interface** command from the configuration file and remove the source designation, use the **no** form of this command.

**logging source-interface** *type interface-path-id*

**no logging source-interface**

## Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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 source IP address is specified.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Normally, a syslog message contains the IP address of the interface it uses to leave the networking device. Use the **logging source-interface** command to specify that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the networking device.

Use the [logging](#), on page 318 command to specify a syslog server host as a destination for syslog messages.

## Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to specify that the IP address for Packet-over-SONET/SDH (POS) interface 0/1/0/1 be set as the source IP address for all messages:

```
RP/0/0/CPU0:router(config)# logging source-interface pos 0/1/0/1
```

### Related Commands

Command	Description
<a href="#">logging</a> , on page 318	Specifies a syslog server host as a destination for syslog messages.



# logging suppress deprecated

To prevent the logging of messages to the console to indicate that commands are deprecated, use the **logging suppress deprecated** command in Global Configuration mode. To remove the **logging suppress deprecated** command from the configuration file, use the **no** form of this command.

**logging suppress deprecated**

**no logging suppress deprecated**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Console messages are displayed when deprecated commands are used.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

The **logging suppress deprecated** command affects messages to the console only.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to suppress the consecutive logging of deprecated messages:

```
RP/0/0/CPU0:router(config)# logging suppress deprecated
```

# logging suppress duplicates

To prevent the consecutive logging of more than one copy of the same system logging (syslog) message, use the **logging suppress duplicates** command in Global Configuration mode. To remove the **logging suppress duplicates** command from the configuration file and disable the filtering process, use the **no** form of this command.

**logging suppress duplicates**

**no logging suppress duplicates**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Duplicate messages are logged.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

If you use the **logging suppress duplicates** command during debugging sessions, you might not see all the repeated messages and could miss important information related to problems that you are attempting to isolate and resolve. In such a situation, you might consider disabling this command.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to suppress the consecutive logging of duplicate messages:

```
RP/0/0/CPU0:router(config)# logging suppress duplicates
```

## Related Commands

Command	Description
<a href="#">logging, on page 318</a>	Specifies a syslog server host as a destination for syslog messages.

Command	Description
<a href="#">logging buffered</a> , on page 322	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits the syslog messages sent to the logging buffer based on severity.
<a href="#">logging monitor</a> , on page 345	Specifies terminal lines other than the console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.

# logging trap

To specify the severity level of messages logged to snmp server, use the **logging trap** command in Global Configuration mode. To restore the default behavior, use the **no** form of this command.

**logging trap** [ *severity* ]

**no logging trap**

## Syntax Description

*severity* (Optional) Severity level of messages logged to the snmp server, including events of a higher severity level (numerically lower). The default is **informational**. Settings for the severity levels and their respective system conditions are listed under [Table 28: Severity Levels for Messages, on page 322](#) in the “Usage Guidelines” section for the **logging buffered** command.

## Command Default

*severity*: **informational**

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3	Change in the behavior of logging trap and logging severity for snmp and syslog servers.

## Usage Guidelines

Use the **logging trap** command to limit the logging of messages sent to snmp servers to only those messages at the specified level.

[Table 28: Severity Levels for Messages, on page 322](#) under the “Usage Guidelines” section for the **logging buffered, on page 322** command lists the syslog definitions that correspond to the debugging message levels.

Use the **logging, on page 318** command to specify a syslog server host as a destination for syslog messages.

The **logging trap disable** will disable the logging of messages to both snmp server and syslog servers.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to restrict messages to **notifications** (5) and numerically lower levels.

```
RP/0/0/CPU0:router(config)# logging trap notifications
```

## Related Commands

Command	Description
<a href="#">logging</a> , on page 318	Specifies a syslog server host as a destination for syslog messages.

## service timestamps

To modify the time-stamp format for system logging (syslog) and debug messages, use the **service timestamps** command in Global Configuration mode. To revert to the default timestamp format, use the **no** form of this command.

**service timestamps** [[debug|log] {datetime [localtime] [msec] [show-timezone] [year]}|disable|uptime}]  
**no service timestamps** [[debug|log] {datetime [localtime] [msec] [show-timezone] [year]}|disable|uptime}]

### Syntax Description

<b>debug</b>	(Optional) Specifies the time-stamp format for debugging messages.
<b>log</b>	(Optional) Specifies the time-stamp format for syslog messages.
<b>datetime</b>	(Optional) Specifies that syslog messages are time-stamped with date and time.
<b>localtime</b>	(Optional) When used with the <b>datetime</b> keyword, includes the local time zone in time stamps.
<b>msec</b>	(Optional) When used with the <b>datetime</b> keyword, includes milliseconds in the time stamp.
<b>show-timezone</b>	(Optional) When used with the <b>datetime</b> keyword, includes time zone information in the time stamp.
<b>year</b>	(Optional) Adds year information to timestamp.
<b>disable</b>	(Optional) Causes messages to be time-stamped in the default format.
<b>uptime</b>	(Optional) Specifies that syslog messages are time-stamped with the time that has elapsed since the networking device last rebooted.

### Command Default

Messages are time-stamped in the month day hh:mm:ss by default.

The default for the **service timestamps debug datetime** and **service timestamps log datetime** forms of the command with no additional keywords is to format the time in Coordinated Universal Time (UTC) without milliseconds and time zone information.

### Command Modes

Global Configuration mode

### Command History

Release	Modification
Release 3.2	This command was introduced.
Release 4.3	The keyword year was added.

### Usage Guidelines

Time stamps can be added to either debugging or syslog messages independently. The **uptime** keyword adds time stamps in the format `hhhh:mm:ss`, indicating the elapsed time in hours:minutes:seconds since the networking device last rebooted. The **datetime** keyword adds time stamps in the format `mmm dd hh:mm:ss`, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (\*), which indicates that the date and time have not been set and should be verified.

The **no** form of the **service timestamps** command causes messages to be time-stamped in the default format.

Entering the **service timestamps** form of this command without any keywords or arguments is equivalent to issuing the **service timestamps debug uptime** form of this command.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to enable time stamps on debugging messages, which show the elapsed time since the networking device last rebooted:

```
RP/0/0/CPU0:router(config)# service timestamps debug uptime
```

This example shows how to enable time stamps on syslog messages, which show the current time and date relative to the local time zone, with the time zone name included:

```
RP/0/0/CPU0:router(config)# service timestamps log datetime localtime show-timezone
```

```
RP/0/0/CPU0:router(config)# service timestamps log datetime year
```

# severity

To specify the filter level for logs, use the **severity** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

**severity** {*severity*}

**no severity**

## Syntax Description

<i>severity</i>	Severity level for determining which messages are logged to the archive. Possible severity levels and their respective system conditions are listed under <a href="#">Table 28: Severity Levels for Messages</a> , on page 322 in the “Usage Guidelines” section. The default is <b>informational</b> .
-----------------	---

## Command Default

Informational

## Command Modes

Logging archive configuration

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **severity** command to specify the filter level for syslog messages. All syslog messages higher in severity or the same as the configured value are logged to the archive.

[Table 28: Severity Levels for Messages](#), on page 322 describes the acceptable severity levels for the *severity* argument.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to specify that warning conditions and higher-severity messages are logged to the archive:

```
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# severity warnings
```



# show logging

To display the contents of the logging buffer, use the **show logging** command in EXEC mode.

**show logging** [**local location** *node-id*] [**location** *node-id*] [**start** *month day hh : mm : ss*] [**process name**] [**string** *string*] [**end** *month day hh : mm :ss*]

## Syntax Description

**end** *month day hh : mm : ss*

(Optional) Displays syslog messages with a time stamp equal to or lower than the time stamp specified with the *monthday hh : mm : ss* argument.

The ranges for the *month day hh : mm : ss* arguments are as follows:

- *month*—The month of the year. The values for the *month* argument are:
  - january
  - february
  - march
  - april
  - may
  - june
  - july
  - august
  - september
  - october
  - november
  - december
- *day*—Day of the month. Range is 01 to 31.
- *hh* :—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
- *mm* :—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
- *ss*—Seconds. Range is 00 to 59.

**local location** *node-id*

(Optional) Displays system logging (syslog) messages from the specified local buffer. The *node-id* argument is entered in the *rack/slot/module* notation.

<b>location</b> <i>node-id</i>	(Optional) Displays syslog messages from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>start</b> <i>month day hh : mm : ss</i>	<p>(Optional) Displays syslog messages with a time stamp equal to or higher than the time stamp specified with the <i>month day hh : mm : ss</i> argument.</p> <p>The ranges for the <i>month day hh : mm : ss</i> arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <i>month</i>—The month of the year. The values for the <i>month</i> argument are: <ul style="list-style-type: none"> <li>◦ january</li> <li>◦ february</li> <li>◦ march</li> <li>◦ april</li> <li>◦ may</li> <li>◦ june</li> <li>◦ july</li> <li>◦ august</li> <li>◦ september</li> <li>◦ october</li> <li>◦ november</li> <li>◦ december</li> </ul> </li> <li>• <i>day</i>—Day of the month. Range is 01 to 31.</li> <li>• <i>hh</i> :—Hours. Range is 00 to 23. You must insert a colon after the <i>hh</i> argument.</li> <li>• <i>mm</i> :—Minutes. Range is 00 to 59. You must insert a colon after the <i>mm</i> argument.</li> <li>• <i>ss</i>—Seconds. Range is 00 to 59.</li> </ul>
<b>process</b> <i>name</i>	(Optional) Displays syslog messages related to the specified process.
<b>string</b> <i>string</i>	(Optional) Displays syslog messages that contain the specified string.

**Command Default**

None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.2	This command was introduced.

**Usage Guidelines** Use the **show logging** command to display the state of syslog error and event logging on the processor console. The information from the command includes the types of logging enabled and the size of the buffer.

Task ID	Task ID	Operations
	logging	read

**Examples** This is the sample output from the **show logging** command with the **process** keyword and *name* argument. Syslog messages related to the init process are displayed in the sample output.

```
RP/0/0/CPU0:router# show logging process init

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level , 59 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 0 messages logged
Buffer logging: level debugging, 75 messages logged

Log Buffer (16384 bytes):

LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
SP/0/1/SP:May 24 22:18:54.925 : init[65541]: %INIT-7-MBI_STARTED : total time 7.159 seconds

SP/0/1/SP:May 24 22:20:16.737 : init[65541]: %INIT-7-INSTALL_READY : total time 88.984
seconds
SP/0/SM1/SP:May 24 22:18:40.993 : init[65541]: %INIT-7-MBI_STARTED : total time 7.194 seconds

SP/0/SM1/SP:May 24 22:20:17.195 : init[65541]: %INIT-7-INSTALL_READY : total time 103.415
seconds
SP/0/2/SP:May 24 22:18:55.946 : init[65541]: %INIT-7-MBI_STARTED : total time 7.152 seconds

SP/0/2/SP:May 24 22:20:18.252 : init[65541]: %INIT-7-INSTALL_READY : total time 89.473
seconds
```

This is the sample output from the **show logging** command using both the **processname** keyword argument pair and **location node-id** keyword argument pair. Syslog messages related to the “init” process emitted from node 0/1/CPU0 are displayed in the sample output.

```
RP/0/0/CPU0:router# show logging process init location 0/1/CPU0

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level , 59 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 0 messages logged
Buffer logging: level debugging, 75 messages logged
```

```
Log Buffer (16384 bytes):
LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
```

This table describes the significant fields shown in the display.

**Table 30: show logging Field Descriptions**

Field	Description
Syslog logging	If enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, the host captures and saves the messages.
Console logging	If enabled, the level and the number of messages logged to the console are stated; otherwise, this field displays “disabled.”
Monitor logging	If enabled, the minimum level of severity required for a log message to be sent to the monitor terminal (not the console) and the number of messages logged to the monitor terminal are stated; otherwise, this field displays “disabled.”
Trap logging	If enabled, the minimum level of severity required for a log message to be sent to the syslog server and the number of messages logged to the syslog server are stated; otherwise, this field displays “disabled.”
Buffer logging	If enabled, the level and the number of messages logged to the buffer are stated; otherwise, this field displays “disabled.”

#### Related Commands

Command	Description
<a href="#">clear logging</a> , on page 313	Clears messages from the logging buffer.

# show logging history

To display information about the state of the system logging (syslog) history table, use the **show logging history** command in EXEC mode mode.

**show logging history**

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

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.2	This command was introduced.

**Usage Guidelines** Use the **show logging history** command to display information about the syslog history table, such as the table size, the status of messages, and the text of messages stored in the table. Simple Network Management Protocol (SNMP) configuration parameters and protocol activity also are displayed.

Use the [logging history](#), on page 335 command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Use the [logging history size](#), on page 337 to change the number of syslog messages that can be stored in the history table.

Task ID	Task ID	Operations
	logging	read

**Examples** This is the sample output from the **show logging history** command:

```
RP/0/0/CPU0:router# show logging history
```

```
Syslog History Table: '1' maximum table entries
saving level 'warnings' or higher
137 messages ignored, 0 dropped, 29 table entries flushed
SNMP notifications disabled
```

This table describes the significant fields shown in the display.

**Table 31: show logging history Field Descriptions**

Field	Description
maximum table entries	Number of messages that can be stored in the history table. Set with the <b>logging history size</b> command.
saving level	Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notifications are enabled). Set with the <b>logging history</b> command.
messages ignored	Number of messages not stored in the history table because the severity level is greater than that specified with the <b>logging history</b> command.
SNMP notifications	Status of whether syslog traps of the appropriate level are sent to the SNMP server. Syslog traps are either enabled or disabled through the <b>snmp-server enable</b> command.

**Related Commands**

Command	Description
<a href="#">logging history, on page 335</a>	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
<a href="#">logging history size, on page 337</a>	Changes the number of syslog messages that can be stored in the history table.

# terminal monitor

To enable the display of debug command output and system logging (syslog) messages for the current terminal session, use the **terminal monitor** command in EXEC mode.

**terminal monitor [disable]**

Syntax Description	<b>disable</b> (Optional) Disables the display of syslog messages for the current terminal session.
--------------------	---

Command Default	None
-----------------	------

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	Release 3.2	This command was introduced.

**Usage Guidelines** Use the **terminal monitor** command to enable the display of syslog messages for the current terminal session.

**Note**

Syslog messages are not sent to terminal lines unless the [logging monitor, on page 345](#) is enabled.

Use the **terminal monitor disable** command to disable the display of logging messages for the current terminal session. If the display of logging messages has been disabled, use the **terminal monitor** command to re-enable the display of logging messages for the current terminal session.

The **terminal monitor** command is set locally, and does not remain in effect after a terminal session has ended; therefore, you must explicitly enable or disable the **terminal monitor** command each time that you would like to monitor a terminal session.

Task ID	Task ID	Operations
	logging	execute

**Examples** This example shows how to enable the display syslog messages for the current terminal session:

```
RP/0/0/CPU0:router# terminal monitor
```

**Related Commands**

Command	Description
<a href="#">logging monitor</a> , on page 345	Specifies terminal lines other than console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.





## Onboard Failure Logging Commands

This module describes the Cisco IOS XR software commands used to configure onboard failure logging (OBFL) for system monitoring on the router. OBFL gathers boot, environmental, and critical hardware failure data for field-replaceable units (FRUs), and stores the information in the nonvolatile memory of the FRU. This information is used for troubleshooting, testing, and diagnosis if a failure or other error occurs.

Because OBFL is on by default, data is collected and stored as soon as the card is installed. If a problem occurs, the data can provide information about historical environmental conditions, uptime, downtime, errors, and other operating conditions.

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.



### Caution

OBFL is activated by default in all cards and should not be deactivated. OBFL is used to diagnose problems in FRUs and to display a history of FRU data.

### Related Documents

For detailed information about OBFL concepts, configuration tasks, and examples, see the *Onboard Failure Logging Services* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [show logging onboard](#), page 366
- [clear logging onboard](#), page 369
- [hw-module logging onboard](#) , page 371

# show logging onboard

To display the onboard failure logging (OBFL) messages, use the **show logging onboard** command in Admin EXEC mode.

**show logging onboard** [**all**|**cbc**|**common** {**dump-all**|**dump-range** {*start-address*|*end-address*}}|**most-recent** {*fans fan-tray-slot*| [**location** *node-id*]}|**diagnostic**|**environment**|**error**|**genstr**|**temperature**|**uptime**|**voltage**}] [**all**|**continuous**|**historical**|**static-data**] [**detail**|**raw**|**summary**] [*location node-id*] [**verbose**]

## Syntax Description

<b>all</b>	Displays all file information.
<b>cbc</b>	Displays Can Bus Controller (CBC) OBFL commands.
<b>common</b>	Displays the generic OBFL message logging output of multiple clients from string application.
<b>dump-all</b>	Displays all OBFL records.
<b>dump-range</b> { <i>start-address</i>   <i>end-address</i> }	Displays OBFL EEPROM data for a given range. Start and end address ranges are from 0 to 4294967295.
<b>most-recent</b>	Displays the last five OBFL data records.
<b>fans</b> <i>fan-tray-slot</i>	Displays a specific fan tray slot.
<b>location</b> <i>node-id</i>	Displays OBFL messages from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>diagnostic</b>	Displays diagnostic information.
<b>environment</b>	Displays system environment information.
<b>error</b>	Displays output from the message application.
<b>temperature</b>	Displays temperature information.
<b>uptime</b>	Displays the OBFL uptime.
<b>voltage</b>	Displays voltage information.
<b>continuous</b>	Displays continuous information.
<b>historical</b>	Displays historical information.
<b>static-data</b>	Display system descriptor data.
<b>detail</b>	Displays detailed logging information.
<b>raw</b>	Displays raw OBFL data.

<b>summary</b>	Displays a summary of OBFL logging information.
<b>verbose</b>	Displays internal debugging information.

**Command Default** None

**Command Modes** Admin EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.4.1	This command was introduced.

**Usage Guidelines**

Use the **show logging onboard** command to display all logging messages for OBFL.

To narrow the output of the command, enter the **show logging onboard** command with one of the optional keywords.

Use the **location node-id** keyword and argument to display OBFL messages for a specific node.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	logging	read

**Examples** This example displays uptime information from the OBFL feature:

```
RP/0/0/CPU0:router(admin)# show logging onboard uptime detail location 0/7/cpu0

-----
UPTIME CONTINUOUS DETAIL INFORMATION (Node: node0_7_CPU0)
-----
The first record      : 01/05/2007 00:58:41
The last record       : 01/17/2007 16:07:13
Number of records    :          478
File size             :       15288 bytes
Current reset reason  : 0x00
Current uptime       :    0 years  0 weeks 0 days  3 hours  0 minutes
-----
Time Stamp           |
MM/DD/YYYY HH:MM:SS | Users operation
-----
01/05/2007 01:44:35  File cleared by user request.
-----
```

This example displays continuous information about the temperature:

```
RP/0/0/CPU0:router(admin)# show logging onboard temperature continuous
```

**show logging onboard**

```
RP/0/RSP1/CPU0:ios(admin)#show logging onboard temperature continuous
Fri Dec 11 02:22:16.247 UTC
```

```
-----
TEMPERATURE CONTINUOUS INFORMATION (Node: node0_RSP0_CPU0)
-----
Sensor                                | ID |
-----
Inlet0                                0x1
Hotspot0                              0x2
-----
Time Stamp          |Sensor Temperature C
MM/DD/YYYY HH:MM:SS | 1    2    3    4    5    6    7    8    9    10
-----
11/24/2009 20:55:28    23    36
11/24/2009 21:08:47    22    36
+32 minutes           22    37
+32 minutes           22    37
```

This example displays raw information about the temperature:

```
RP/0/0/CPU0:router(admin)# show logging onboard temperature raw
```

```
Feature: Temperature
node: node0_2_CPU0, file name: nvram:/temp_cont, file size: 47525
00000000: 00 29 01 02 45 79 d8 a8 00 00 00 00 00 00 ba 37 .)..Ey.....7
00000010: aa 0d 00 00 45 79 d8 a8 1c 18 2b 2c 2f 1d 28 27 ....Ey.....+./.( '
00000020: 1b 26 2a 20 27 00 00 fa fa 00 1f 01 02 45 79 da .&* '.....Ey.
00000030: 2b 00 00 00 00 00 00 ba 38 ca 0d 00 06 00 00 00 +.....8.....
00000040: 0f 00 00 00 00 00 fa fa 00 1f 01 02 45 79 db ae .....Ey..
00000050: 00 00 00 00 00 00 ba 39 ca 0d 00 06 00 00 00 00 .....9.....
00000060: 00 f0 00 00 00 00 fa fa 00 1f 01 02 45 79 dd 32 00 .....Ey.2.
00000070: 00 00 00 00 00 00 ba 3a ca 0d 00 06 00 00 00 00 .....:.....
00000080: 00 00 00 00 00 fa fa 00 1f 01 02 45 79 de b8 00 00 .....:Ey....
00000090: 00 00 00 00 00 ba 3b ca 0d 00 06 00 00 00 00 10 .....;.....
000000a0: 00 00 00 fa fa 00 1f 01 02 45 79 e0 3c 00 00 00 .....:Ey.<...
000000b0: 00 00 00 ba 3c ca 0d 00 06 00 00 01 00 00 00 00 ....<.....
000000c0: 00 00 fa fa 00 1f 01 02 45 79 e1 be 00 00 00 00 .....:Ey.....
000000d0: 00 00 ba 3d ca 0d 00 06 11 00 00 00 00 00 00 00 ....=.....
000000e0: 00 fa fa 00 1f 01 02 45 79 e3 43 00 00 00 00 00 .....:Ey.C....
000000f0: 00 ba 3e ca 0d 00 06 ff 00 0f 00 00 00 00 00 00 ...>.....
00000100: fa fa 00 1f 01 02 45 79 e4 c6 00 00 00 00 00 00 .....:Ey.....
00000110: ba 3f ca 0d 00 06 00 00 00 00 00 00 00 00 00 fa .?.....
00000120: fa 00 1f 01 02 45 79 e6 49 00 00 00 00 00 00 00 ba .....:Ey.I.....
00000130: 40 ca 0d 00 06 00 00 00 00 00 00 00 00 00 fa fa @.....
00000140: 00 1f 01 02 45 79 e7 cc 00 00 00 00 00 00 00 00 ba 41 ....:Ey.....A
00000150: ca 0d 00 06 00 00 00 10 00 f0 00 00 00 fa fa 00 .....:.....
00000160: 1f 01 02 45 79 e9 4f 00 00 00 00 00 00 00 00 00 ba 42 ca ...:Ey.O.....B.
00000170: 0d 00 06 00 00 00 f0 00 10 00 00 00 fa fa 00 1f .....:.....
00000180: 01 02 45 79 ea d2 00 00 00 00 00 00 00 00 00 00 ..:Ey.....C..
00000190: 00 06 00 00 01 01 00 00 00 00 00 fa fa 00 1f 01 .....:.....
000001a0: 02 45 79 ec 55 00 00 00 00 00 00 00 ba 44 ca 0d 00 .:Ey.U.....D...
000001b0: 06 01 00 00 10 00 00 00 00 00 fa fa 00 1f 01 02 .....:.....
000001c0: 45 79 ed d8 00 00 00 00 00 00 00 ba 45 ca 0d 00 06 Ey.....E....
000001d0: 0f 00 0f ff 00 00 00 00 00 fa fa 00 1f 01 02 45 .....:.....E
```

**Related Commands**

Command	Description
<a href="#">clear logging onboard, on page 369</a>	Clears OBFL logging messages from a node or from all nodes.
<a href="#">hw-module logging onboard , on page 371</a>	Enables or disables OBFL.

# clear logging onboard

To clear OBFL logging messages from a node or from all nodes, use the **clear logging onboard** command in Admin EXEC mode.

**clear logging onboard** [**all**| **cbc common** {**obfl** {**fans** *fan-tray-slot* [**location** *node-id*]}| **corrupted-files**| **diagnostic**| **environment**| **error**| **poweron-time**| **temperature**| **uptime**| **voltage**}] [**location** *node-id*]

## Syntax Description

<b>all</b>	Clears all OBFL logs.
<b>cbc</b>	Clears commands for Can Bus Controller (CBC).
<b>common</b>	Clears the generic OBFL message logging output of multiple clients from string application.
<b>obfl</b>	Clears OBFL EEPROM.
<b>fans</b> <i>fan-tray-slot</i>	Clears a specific fan tray slot.
<b>location</b> <i>node-id</i>	(Optional) Clears OBFL messages from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>corrupted-files</b>	Clears corrupted file information.
<b>diagnostic</b>	Clears the online diagnostics information from the OBFL logs.
<b>environment</b>	Clears the environmental information from the OBFL logs.
<b>error</b>	Clear syslog information.
<b>poweron-time</b>	Clears time of first customer power on.
<b>temperature</b>	Clears temperature information.
<b>uptime</b>	Clears uptime information.
<b>voltage</b>	Clears voltage information.
<b>continuous</b>	Clears continuous information.
<b>historical</b>	Clears historical information.

## Command Default

All OBFL logging messages are cleared from all nodes.

## Command Modes

Admin EXEC mode

**Command History**

Release	Modification
Release 3.4.1	This command was introduced.

**Usage Guidelines**

Use the **clear logging onboard** command to clear OBFL messages from all nodes. Use the **clear logging onboard** command with the **location** *node-id* keyword and argument to clear OBFL messages for a specific node. If the specified node is not present, an error message is displayed.

**Caution**

The **clear logging onboard** command permanently deletes all OBFL data for a node or for all nodes. Do not clear the OBFL logs without specific reasons, because the OBFL data is used to diagnose and resolve problems in FRUs.

**Caution**

If OBFL is actively running on a card, issuing the **clear logging onboard** command can result in a corrupt or incomplete log at a later point in time. OBFL should always be disabled before this command is issued.

**Task ID**

Task ID	Operations
logging	read

**Examples**

In the following example, the OBFL data is cleared for all nodes in the system:

```
RP/0/0/CPU0:router(admin)# clear logging onboard
```

**Related Commands**

Command	Description
<a href="#">hw-module logging onboard</a> , on page 371	Enables or disables OBFL.
<a href="#">show logging onboard</a> , on page 366	Displays the OBFL messages.

# hw-module logging onboard

To disable onboard failure logging (OBFL), use the **hw-module logging onboard** command in Admin Configuration mode. To enable OBFL again, use the **no** form of this command.

**hw-module** {all|subslot *node-id*} **logging onboard** [disable|severity {alerts|emergencies}]

**no hw-module** {all|subslot *node-id*} **logging onboard** [disable]

## Syntax Description

<b>all</b>	Enables or disables OBFL for all nodes.
<b>subslot</b> <i>node-id</i>	Enables or disables OBFL for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>disable</b>	Enables or disables OBFL. See the Usage Guidelines for more information.
<b>severity</b>	(Optional) Specifies the severity level for the syslog message that is logged into the OBFL storage device.
<b>alerts</b>	Specifies that both emergency and alert syslog messages are logged. The default is the <b>alerts</b> keyword.
<b>emergencies</b>	Specifies that only the emergency syslog messages are logged.

## Command Default

By default, OBFL logging is enabled.

*severity*: 1 (alerts) and 0 (emergencies)

## Command Modes

### Command History

Release	Modification
Release 3.4.1	This command was introduced.

## Usage Guidelines

Use the **hw-module logging onboard** command to enable or disable OBFL.

- To disable OBFL use the **disable** keyword. OBFL is enabled by default.  
**hw-module** {all|subslot *node-id*} **logging onboard disable**
- To enable OBFL, use the **no** form of the **hw-module logging onboard** command with the **disable** keyword. OBFL is enabled by default. Use this command only if you disabled OBFL:  
**no hw-module** {all|subslot *node-id*} **logging onboard disable**
- To enable OBFL and return the configuration to the default message severity level, use the **no** form of the **hw-module logging onboard** command with the **severity** keyword:

**no hw-module {all | subslot *node-id*} logging onboard severity**

When the OBFL feature is disabled, existing OBFL logs are preserved. To resume OBFL data collection, enable the OBFL feature again.

**Note**

If a new node is inserted, and OBFL is enabled for that slot, then OBFL is enabled for the new node. If a card is removed from a router and inserted into a different router, the card assumes the OBFL configuration for the new router.

**Task ID**

Task ID	Operations
logging	read, write
root-lr	read, write

**Examples**

The following example shows how to disable OBFL for all cards:

```
RP/0/0/CPU0:router(admin-config)# hw-module all logging onboard disable
```

The following example shows how to disable OBFL for a card:

```
RP/0/0/CPU0:router(admin-config)# hw-module subslot 0/2/CPU0 logging onboard disable
```

The following example shows how to enable OBFL again:

```
RP/0/0/CPU0:router(admin-config)# no hw-module all logging onboard disable
```

The following example shows how to save only the syslog message in which the severity level is set to 0 (emergency) to a storage device:

```
RP/0/0/CPU0:router(admin-config)# hw-module subslot 0/2/CPU0 logging onboard severity
emergencies
```

The following example shows how to save the syslog message in which the severity level is set to 0 (emergency) and 1 (alert) to a storage device:

```
RP/0/0/CPU0:router(admin-config)# hw-module subslot 0/2/CPU0 logging onboard severity alerts
```

**Related Commands**

Command	Description
<a href="#">clear logging onboard</a> , <a href="#">on page 369</a>	Clears OBFL logging messages from a node or from all nodes.



Command	Description
<a href="#">show logging onboard, on page 366</a>	Displays the OBFL messages.





## Performance Management Commands

This module describes the performance management and monitoring commands available on the router. These commands are used to monitor, collect, and report statistics, and to adjust statistics gathering for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) protocol, generic interfaces, and individual nodes.

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 detailed information about performance management concepts, configuration tasks, and examples, see the *Implementing Performance Management* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- [monitor controller fabric, page 377](#)
- [monitor controller sonet, page 379](#)
- [monitor interface, page 381](#)
- [performance-mgmt apply monitor, page 386](#)
- [performance-mgmt apply statistics, page 389](#)
- [performance-mgmt apply thresholds, page 392](#)
- [performance-mgmt regular-expression, page 395](#)
- [performance-mgmt resources dump local, page 396](#)
- [performance-mgmt resources memory, page 397](#)
- [performance-mgmt resources tftp-server, page 399](#)
- [performance-mgmt statistics, page 401](#)
- [performance-mgmt thresholds, page 404](#)
- [show performance-mgmt bgp, page 416](#)
- [show performance-mgmt interface , page 418](#)
- [show performance-mgmt mpls, page 421](#)
- [show performance-mgmt node, page 423](#)

- [show performance-mgmt ospf](#), page 425
- [show running performance-mgmt](#), page 427

# monitor controller fabric

To monitor controller fabric counters in real time, use the **monitor controller fabric** command in EXEC mode.

**monitor controller fabric** *{plane-id| all}*

## Syntax Description

<i>plane-id</i>	Plane ID number of the fabric plane to be monitored. The range is 0 to 7.
<b>all</b>	Monitors all fabric planes.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **monitor controller fabric** command to display controller fabric counters. The display refreshes every 2 seconds.

The interactive commands that are available during a controller fabric monitoring session are described in this table.

**Table 32: Interactive Commands Available for the monitor controller fabric Command**

Command	Description
<b>c</b>	Resets controller fabric counters to 0.
<b>f</b>	Freezes the display screen, thereby suspending the display of fresh counters.
<b>t</b>	Thaws the display screen, thereby resuming the display of fresh counters.
<b>q</b>	Terminates the controller fabric monitoring session.
<b>s</b>	Enables you to jump to a nonsequential fabric plane. You are prompted to enter the plane ID of the fabric to be monitored.

Task ID

Task ID	Operations
fabric	read
basic-services	execute
monitor	read

Examples

This is sample output from the **monitor controller fabric** command. The output in this example displays fabric controller counters from fabric plane 0.

```
RP/0/0/CPU0:router# monitor controller fabric 0

rack3-3 Monitor
Time: 00:00:24 SysUptime: 03:37:57 Controller fabric for 0x0 Controller Fabric Stats:
Delta In Cells 0 ( 0 per-sec) 0 Out Cells 0 ( 0 per-sec) 0 CE Cells 0 ( 0 per-sec) 0 UCE
Cells 0 ( 0 per-sec) 0 PE Cells 0 ( 0 per-sec) 0 Quit='q', Freeze='f', Thaw='t',
Clear='c', Select controller='s'
```

# monitor controller sonet

To monitor SONET controller counters, use the **monitor controller sonet** command in EXEC mode.

**monitor controller sonet** *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 Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **monitor controller sonet** command to display SONET controller counters. The display refreshes every 2 seconds.

The interactive commands that are available during a controller monitoring session are described in this table.

**Table 33: Interactive Commands for the monitor controller sonet Command**

Command	Description
<b>c</b>	Resets controller SONET counters to 0.
<b>f</b>	Freezes the display screen, thereby suspending the display of fresh counters.
<b>t</b>	Thaws the display screen, thereby resuming the display of fresh counters.
<b>q</b>	Terminates the controller SONET monitoring session.
<b>s</b>	Enables you to jump to a nonsequential SONET controller. You are prompted to enter the SONETcontroller to be monitored.

Task ID

Task ID	Operations
fabric	read
basic-services	execute
monitor	read

Examples

This is the sample output from the **monitor controller sonet** command. The output in this example displays counters from SONET controller 0/3/0/0.

```
RP/0/0/CPU0:router# monitor controller sonet 0/3/0/0 rack3-3
Monitor Time: 00:00:06 SysUptime: 01:23:56 Controller for SONET0_3_0_0 Controller
Stats:
Delta Path LOP 0 ( 0 per-sec) 0 Path AIS 0 ( 0 per-sec) 0 Path RDI 0 ( 0 per-sec)
0 Path
BIP 0 ( 0 per-sec) 0 Path FEBE 0 ( 0 per-sec) 0 Path NEWPTR 0 ( 0 per-sec) 0
Path PSE 0
( 0 per-sec) 0 Path NSE 0 ( 0 per-sec) 0 Line AIS 0 ( 0 per-sec) 0 Line RDI 0
( 0 per-sec) 0 Line BIP 0 ( 0 per-sec) 0 Line FEBE 0 ( 0 per-sec) 0 Section LOS 1
per-sec) 1 Section LOF 0 ( 0 per-sec) 0 Section BIP 0 ( 0 per-sec) 0 Quit='q',
Freeze='f', Thaw='t', Clear='c', Select controller='s'
```



# monitor interface

To monitor interface counters in real time, use the **monitor interface** command in EXEC mode or Admin EXEC mode.

**monitor interface** [*type1 interface-path-id1* [...[*type32 interface-path-id32*]]]

## Syntax Description

<i>type</i>	Interface type. For more information, use the question mark ( ? ) online help function.
<i>interface-path-id</i>	Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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

Use the **monitor interface** command without an argument to display statistics for all interfaces in the system.

## Command Modes

EXEC mode  
Admin EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	Support was added for multiple interfaces. Support was added for default behavior to monitor all interfaces. Support was added for wildcards in the interface syntax. Support was added for additional display options.
Release 3.7.0	Added summary enhancements for the AF aggregates.

## Usage Guidelines

Use the **monitor interface** command without any keywords or arguments to display interface counters for all interfaces. The display refreshes every 2 seconds.

Use the **monitor interface** command with the *type interface-path-id* arguments to display counters for a single interface. For example: **monitor interface pos0/2/0/0**

To display more than one selected interface, enter the **monitor interface** command with multiple *type interface-path-id* arguments. For example: **monitor interface pos0/2/0/0 pos0/5/0/1 pos0/5/0/2**

To display a range of interfaces, enter the **monitor interface** command with a wildcard. For example:  
**monitor interface pos0/5/\***

You can display up to 32 specific interfaces and ranges of interfaces.

The interactive commands that are available during an interface monitoring session are described in this table.

**Table 34: Interactive Commands Available for the monitor interface Command (Functional Summary)**

Command	Description
<b>Use the following keys to suspend or resume the counter refresh:</b>	
<b>f</b>	Freezes the display screen, thereby suspending the display of fresh counters.
<b>t</b>	Thaws the display screen, thereby resuming the display of fresh counters.
<b>Use the following key to reset the counters:</b>	
<b>c</b>	Resets interface counters to 0.
<b>Use the following keys when displaying statistics for a single interface. These keys display counters in normal or detailed view.</b>	
<b>d</b>	Changes the display mode for the interface monitoring session to display detailed counters. Use the <b>b</b> interactive command to return to the regular display mode.
<b>r</b>	Displays the protocol divided by IPv4 or IPv6, and multicast and unicast. When the statistics are displayed using the <b>r</b> option, you can also use the <b>k</b> , <b>y</b> , or <b>o</b> keys to display statistics in packets (“ <b>k</b> ”), bytes (“ <b>y</b> ”) or packets and bytes (“ <b>o</b> ”).
<b>b</b>	Returns the interface monitoring session to the regular display mode for counters. Statistics are not divided by protocol.
<b>Use the following keys when displaying statistics for multiple interfaces. These keys modify the display to show statistics in bytes, packets, or bytes and packets.</b>	
<b>k</b>	Displays statistics in packets (“ <b>k</b> ”).
<b>y</b>	(Default) Displays statistics in bytes (“ <b>y</b> ”).
<b>o</b>	Displays statistics in both bytes and packets (“ <b>o</b> ”).
<b>Use the following keys to display statistics for a different interface:</b>	

<b>i</b>	Enables you to jump to a nonsequential interface. You are prompted to enter the interface type and interface path ID to be monitored.
<b>p</b>	Displays the previous sequential interface in the list of available interfaces.
<b>n</b>	Displays the next sequential interface in the list of available interfaces.
<b>q</b>	Terminates the interface monitoring session.

**Task ID**

Task ID	Operations
basic-services	execute
monitor	read

**Examples**

When more than one interface is specified, the statistics for each interface are displayed on a separate line. This display format appears anytime more than one interface is specified. For example:

- To display statistics for all interfaces, enter the command **monitor interface**.
- To display all the interfaces for an interface type, such as all POS interface, enter the command and wildcard **monitor interface pos \***.
- To display statistics for three specified interfaces, enter the command **monitor interface pos0/2/0/0 pos0/5/0/1 pos0/5/0/2**.

This is the sample output for the **monitor interface** command entered without an argument. This command displays statistics for all interfaces in the system.

```
RP/0/0/CPU0:router# monitor interface Protocol:General
Rack6-1 Monitor Time: 00:00:01 SysUptime: 165:52:41 Interface In(bps) Out(bps)
InBytes/Delta OutBytes/Delta Mg0/0/CPU0/0 1500/ 0% 7635/ 0% 58.4M/420 8.1M/2138
PO0/4/0/0 578/ 0% 535/ 0% 367.2M/162 377.5M/150 PO0/4/0/1 278/ 0% 0/ 0% 345.7M/78
360.1M/0 Gi0/5/0/1 3128/ 0% 2171/ 0% 382.8M/876 189.1M/608 Gi0/5/0/1.1 0/ 0%
0/ 0% 824.6G/0 1.0T/0 Gi0/5/0/1.2 0/ 0% 0/ 0% 1.0T/0 824.6G/0 Gi0/5/0/1.3 678/ 0% 0/
0% 1.0T/190 1.0T/0 Gi0/5/0/1.4 0/ 0% 0/ 0% 824.6G/0 824.6G/0 Gi0/5/0/1.5 0/ 0%
350/ 0% 824.6G/0 1.0T/98 Gi0/5/0/1.6 327/ 0% 348/ 0% 824.6G/92 1.0T/98 Gi0/5/0/1.7 0/
0% 346/ 0% 824.6G/0 1.0T/98 Gi0/5/0/1.8 325/ 0% 0/ 0% 824.6G/92 1.0T/0 Quit='q', Clear='c',
Freeze='f', Thaw='t', Next set='n', Prev set='p', Bytes='y', Packets='k'
(General='g',
IPv4 Uni='4u', IPv4 Multi='4m', IPv6 Uni='6u', IPv6 Multi='6m') Rack6-1 Monitor
Time:
00:00:01 SysUptime: 165:52:41 Protocol:IPv4 Unicast Interface In(bps) Out(bps)
InBytes/Delta OutBytes/Delta Mg0/0/CPU0/0 0/ 0% 0/ 0% 85.3M/0 6.9M/0 PO0/4/0/0
```

```

0/ 0% 0/
0% 3.1G/0 224/0 PO0/4/0/1 0/ 0% 0/ 0% 3.0G/0 152582/0 Gi0/5/0/1 0/ 0% 0/ 0% 0/0
28168/0
Gi0/5/0/1.1 0/ 0% 0/ 0% 0/0 441174/0 Gi0/5/0/1.2 0/ 0% 0/ 0% 540/0 0/0 Gi0/5/0/1.3
0/ 0%
0/ 0% 13.4M/0 462549/0 Gi0/5/0/1.4 0/ 0% 0/ 0% 12.2M/0 0/0 Gi0/5/0/1.5 0/ 0%
0/ 0% 0/0
427747/0 Gi0/5/0/1.6 0/ 0% 0/ 0% 3072/0 500/0 Gi0/5/0/1.7 0/ 0% 0/ 0% 0/0
568654/0
Gi0/5/0/1.8 0/ 0% 0/ 0% 8192/0 5.1M/0 Quit='q', Clear='c', Freeze='f', Thaw='t',
Next
set='n', Prev set='p', Bytes='y', Packets='k' (General='g', IPv4 Uni='4u', IPv4
Multi='4m', IPv6 Uni='6u', IPv6 Multi='6m') Rack6-1 Monitor Time: 00:00:03
SysUptime:
165:52:56 Protocol:IPv4 Multicast Interface In(bps) Out(bps) InBytes/Delta
OutBytes/Delta Mg0/0/CPU0/0 (statistics not available) PO0/4/0/0 (statistics
not
available) PO0/4/0/1 (statistics not available) Gi0/5/0/1 (statistics not
available)
Gi0/5/0/1.1 (statistics not available) Gi0/5/0/1.2 (statistics not available)
Gi0/5/0/1.3 (statistics not available) Gi0/5/0/1.4 (statistics not available)
Gi0/5/0/1.5 (statistics not available) Gi0/5/0/1.6 (statistics not available)
Gi0/5/0/1.7 (statistics not available) Gi0/5/0/1.8 (statistics not available)
Quit='q',
Clear='c', Freeze='f', Thaw='t', Next set='n', Prev set='p', Bytes='y',
Packets='k'
(General='g', IPv4 Uni='4u', IPv4 Multi='4m', IPv6 Uni='6u', IPv6 Multi='6m')
Rack6-1
Monitor Time: 00:00:01 SysUptime: 165:53:04 Protocol:IPv6 Unicast Interface
In(bps)
Out(bps) InBytes/Delta OutBytes/Delta Mg0/0/CPU0/0 0/ 0% 0/ 0% 0/0 0/0 PO0/4/0/0
0/ 0%
0/ 0% 0/0 0/0 PO0/4/0/1 0/ 0% 0/ 0% 0/0 0/0 Gi0/5/0/1 0/ 0% 0/ 0% 0/0 0/0
Gi0/5/0/1.1
0/
0% 0/ 0% 0/0 0/0 Gi0/5/0/1.2 0/ 0% 0/ 0% 0/0 0/0 Gi0/5/0/1.3 0/ 0% 0/ 0% 0/0
0/0
Gi0/5/0/1.4 0/ 0% 0/ 0% 0/0 0/0 Gi0/5/0/1.5 0/ 0% 0/ 0% 0/0 0/0 Gi0/5/0/1.6 0/
0% 0/ 0%
0/0 0/0 Gi0/5/0/1.7 0/ 0% 0/ 0% 0/0 0/0 Gi0/5/0/1.8 0/ 0% 0/ 0% 0/0 0/0 Quit='q',
Clear='c', Freeze='f', Thaw='t', Next set='n', Prev set='p', Bytes='y',
Packets='k'
(General='g', IPv4 Uni='4u', IPv4 Multi='4m', IPv6 Uni='6u', IPv6 Multi='6m')
Rack6-1
Monitor Time: 00:00:00 SysUptime: 165:53:19 Protocol:IPv6 Multicast Interface
In(bps)
Out(bps) InBytes/Delta OutBytes/Delta Mg0/0/CPU0/0 (statistics not available)
PO0/4/0/0
(statistics not available) PO0/4/0/1 (statistics not available) Gi0/5/0/1
(statistics
not available) Gi0/5/0/1.1 (statistics not available) Gi0/5/0/1.2 (statistics
not
available) Gi0/5/0/1.3 (statistics not available) Gi0/5/0/1.4 (statistics not
available)
Gi0/5/0/1.5 (statistics not available) Gi0/5/0/1.6 (statistics not available)
Gi0/5/0/1.7 (statistics not available) Gi0/5/0/1.8 (statistics not available)
Quit='q',
Clear='c', Freeze='f', Thaw='t', Next set='n', Prev set='p', Bytes='y',
Packets='k'
(General='g', IPv4 Uni='4u', IPv4 Multi='4m', IPv6 Uni='6u', IPv6 Multi='6m')

```

This is the sample output for **monitor interface pos \*** command that displays statistics for all POS interfaces:

```

RP/0/0/CPU0:router# monitor interface pos 0/*
Protocol:General router Monitor Time: 00:00:02 SysUptime: 186:37:44 Interface
In(bps)
Out(bps) InBytes/Delta OutBytes/Delta POS0/1/0/0 1263/ 0% 0/ 0% 5.3M/330 1.4M/0
1.4M/0
POS0/1/0/1 84/ 0% 0/ 0% 274.8M/22 274.6M/0 POS0/6/0/0 1275/ 0% 0/ 0% 5.3M/330
POS0/6/0/1 85/ 0% 0/ 0% 2.6M/22 1.4M/0 POS0/6/4/4 0/ 0% 0/ 0% 15.1M/0 1.4M/0
POS0/6/4/5

```

```

      85/ 0% 0/ 0% 2.6M/22 1.4M/0 POS0/6/4/6 0/ 0% 0/ 0% 1.3M/0 1.4M/0 POS0/6/4/7 85/
0% 0/ 0%
      2.6M/22 1.4M/0 Quit='q', Clear='c', Freeze='f', Thaw='t', Next set='n', Prev
set='p',
      Bytes='y', Packets='k' (General='g', IPv4 Uni='4u', IPv4 Multi='4m', IPv6
Uni='6u', IPv6
Multi='6m')

```

This is the sample output for a single interface using the **monitor interface** command with the *type interface-path-id* argument. In this example, the output displays interface counters from POS interface 0/6/4/4. By default, statistics are displayed in “Brief” state (statistics are not divided by protocol).

```

RP/0/0/CPU0:router# monitor interface pos0/6/4/4 router
Monitor Time: 00:00:24 SysUptime: 186:43:04 POS0/6/4/4 is up, line protocol is
up
Encapsulation HDLC Traffic Stats:(2 second rates) Delta Input Packets: 232450
0 Input
pps: 0 Input Bytes: 15179522 0 Input Kbps (rate): 0 ( 0%) Output Packets: 67068
0 Output
pps: 0 Output Bytes: 1475484 0 Output Kbps (rate): 0 ( 0%) Errors Stats: Input
Total:
2146 0 Input CRC: 2134 0 Input Frame: 2135 0 Input Overrun: 0 0 Output Total:
0 0 Output
Underrun: 0 0 Quit='q', Freeze='f', Thaw='t', Clear='c', Interface='i', Next='n',
Prev='p' Brief='b', Detail='d', Protocol(IPv4/IPv6)='r'

```

This is the sample output from the **monitor interface** command in the protocol state for the POS interface 0/6/4/4. Use the **r** key to display statics by protocol:

```

RP/0/0/CPU0:router# monitor interface pos0/6/4/4 router
Monitor Time: 00:00:02 SysUptime: 186:49:15 POS0/6/4/4 is up, line protocol is
up
Encapsulation HDLC Traffic Stats:(2 second rates) Delta Input Bytes: 15188186
0 Input
Kbps (rate): 0 ( 0%) Output Bytes: 1476298 0 Output Kbps (rate): 0 ( 0%) IPv4
Unicast
Input Bytes: 0 0 Input Kbps (rate): 0 ( 0%) Output Bytes: 0 0 Output Kbps (rate):
0 (
0%) IPv4 Multicast Input Bytes: 10160304 66 Input Kbps (rate): 0 ( 0%) Output
Bytes: 0 0
Output Kbps (rate): 0 ( 0%) IPv6 Unicast Input Bytes: 0 0 Input Kbps (rate): 0
( 0%)
Output Bytes: 0 0 Output Kbps (rate): 0 ( 0%) IPv6 Multicast Input Bytes: 0 0
Input Kbps
(rate): 0 ( 0%) Output Bytes: 0 0 Output Kbps (rate): 0 ( 0%) Errors Stats:
Input Total:
2146 0 Input CRC: 2134 0 Input Frame: 2135 0 Input Overrun: 0 0 Output Total:
0 0 Output
Underrun: 0 0 Quit='q', Freeze='f', Thaw='t', Clear='c', Interface='i', Next='n',
Prev='p' Brief='b', Detail='d', Protocol(IPv4/IPv6)='r' (Additional options in
'Protocol'): Bytes='y', Packets='k', Both of bytes/packets='o'

```

# performance-mgmt apply monitor

To apply a statistics template to gather a sampling-size set of samples for a particular instance, use the **performance-mgmt apply monitor** command in Global Configuration mode. To stop monitoring statistics, use the **no** form of this command.

**performance-mgmt apply monitor** *entity* {*ip-address* | *type* | *interface-path-id* | *node-id* | *node-id process-id* | *process-name*} [*template-name*] **default**}

**no performance-mgmt apply monitor**

## Syntax Description

<i>entity</i>	<p>Specifies an entity for which you want to apply the statistics template:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b>—Applies a template for monitoring a Border Gateway Protocol (BGP) neighbor.</li> <li>• <b>interface basic-counters</b>—Applies a template for monitoring basic counters on an interface. If you enter this keyword, supply values for the <i>type</i> and <i>interface-path-id</i> arguments.</li> <li>• <b>interface data-rates</b>—Applies a template for monitoring data rates on an interface. If you enter this keyword, supply values for the <i>type</i> and <i>interface-path-id</i> arguments.</li> <li>• <b>interface generic-counters</b>—Applies a template for monitoring generic counters on an interface. If you enter this keyword, supply values for the <i>type</i> and <i>interface-path-id</i> arguments.</li> <li>• <b>mpls ldp</b>—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.</li> <li>• <b>node cpu</b>—Applies a template for monitoring the central processing unit (CPU) on a node. Use the <i>node-id</i> argument with this entity.</li> <li>• <b>node memory</b>—Applies a template for monitoring memory utilization on a node. Use the <b>location</b> keyword and <i>node-id</i> argument with this entity.</li> <li>• <b>node process</b>—Applies a template for monitoring a process on a node. Use the <i>node-id</i> and <i>process-id</i> arguments with this entity.</li> <li>• <b>ospf v2protocol</b>—Applies a template for monitoring an Open Shortest Path First v2 (OSPFv2) process instance.</li> <li>• <b>ospf v3protocol</b>—Applies a template for monitoring an OSPFv3 process instance.</li> </ul>
<i>ip-address</i>	IP or neighbor address. Used with the <b>bgp</b> or <b>ldp</b> keyword.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	<p>Physical interface or virtual interface.</p> <p><b>Note</b> Use the <b>show interfaces</b> command to see a list of all interfaces currently configured on the router.</p> <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

<i>node-id</i>	Designated node. Used with the <b>node cpu</b> or <b>node memory</b> keyword. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<i>node-id</i> <i>process-id</i>	Designated node and process ID. Used with the <b>node process</b> keyword. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<i>process-name</i>	Process name of the OSPF instance. Used with the <b>ospfv2protocol</b> and <b>ospfv3protocol</b> keywords.
<i>template-name</i>	Name of a predefined template used for statistics collection. A template name can be any combination of alphanumeric characters, and may include the underscore character (_). Use the <b>show running performance-mgmt</b> command to display a list of available templates.
<b>default</b>	Applies the default template.

**Command Default**

Monitoring is disabled.

**Command Modes**

Global Configuration mode

**Command History**

Release	Modification
Release 2.0	This command was introduced.
Release 3.2	The <b>enable</b> keyword was replaced by the <b>apply</b> keyword. In previous releases, this command was referred to as <b>performance-mgmt enable monitor</b> . The <b>disable</b> keyword was deprecated. The <b>ospf v2protocol</b> and <b>ospf v3protocol</b> keywords were introduced to support the monitoring of OSPF entity instances.
Release 3.3.0	Removed support for MPLS interfaces.
Release 4.0.1	The <b>interface basic-counters</b> keyword was added to support the monitoring of basic counters on the interface.

**Usage Guidelines**

Use the **performance-mgmt apply monitor** command to apply a statistics template and enable monitoring. This command captures one cycle of a sample to analyze an instance of an entity. Rather than collect statistics for all instances, which is the purpose of the **performance-mgmt apply statistics** command, the **performance-mgmt apply monitor** command captures statistics for a specific entity instance for one sampling period.

The *type* and *interface-path-id* arguments are only to be used with the **interface data-rates** or **interface generic-counter** keyword.

For information about creating templates, see the [performance-mgmt apply statistics, on page 389](#) command.

**Task ID**

Task ID	Operations
monitor	read, write, execute

**Examples**

This example shows how to enable the BGP protocol monitoring using the criterion set in the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply monitor bgp 10.0.0.0 default
```

This example shows how to enable monitoring for data rates according to the criterion set in the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply monitor interface data-rates pos 0/2/0/0 default
```

This example shows how to enable memory monitoring based on the criterion set in the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply monitor node memory location 0/1/cpu0 default
```

This example shows how to enable monitoring for counters according to the criterion set in the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply monitor interface basic-counters hundredGigE 0/2/0/0 default
```

**Related Commands**

Command	Description
<a href="#">performance-mgmt apply statistics, on page 389</a>	Applies a statistics template and enables statistics collection.
<a href="#">performance-mgmt statistics, on page 401</a>	Creates a template to use for collecting performance management statistics.
<a href="#">show running performance-mgmt, on page 427</a>	Displays a list of templates and the template being applied.



## performance-mgmt apply statistics

To apply a statistics template and enable statistics collection, use the **performance-mgmt apply statistics** command in Global Configuration mode. To stop statistics collection, use the **no** form of this command.

**performance-mgmt apply statistics** *entity* **location** {**all** | *node-id*} {*template-name* | **default**}

**no performance-mgmt apply statistics**

### Syntax Description

<i>entity</i>	<p>Specifies an entity for which you want to apply a statistics template:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b>—Applies a statistics collection template for Border Gateway Protocol (BGP).</li> <li>• <b>interface basic-counters</b>—Applies a statistics collection template for basic counters.</li> <li>• <b>interface data-rates</b>—Applies a statistics collection template for data rates.</li> <li>• <b>interface generic-counters</b>—Applies a statistics collection template for generic counters.</li> <li>• <b>mpls ldp</b>—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.</li> <li>• <b>node cpu</b>—Applies a statistics collection template for the central processing unit (CPU). Use the <b>location</b> keyword with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>node memory</b>—Applies a statistics collection template for memory utilization. Use the <b>location</b> keyword with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>node process</b>—Applies a statistics collection template for processes. Use the <b>location</b> keyword with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>ospf v2protocol</b>—Applies a statistics collection template for Open Shortest Path First v2 (OSPFv2) process instances.</li> <li>• <b>ospf v3protocol</b>—Applies a statistics collection template for OSPFv3 process instances.</li> </ul>
<b>location</b> { <b>all</b>   <i>node-id</i> }	<p>Specifies all nodes or a particular node.</p> <p>Specify the <b>location all</b> keywords for all nodes, or the <i>node-id</i> argument to specify a particular node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. You must specify either the <b>location all</b> keywords or the <b>location</b> keyword and <i>node-id</i> argument with the <b>node cpu</b>, <b>node memory</b>, or <b>node process</b> entity.</p>
<i>template-name</i>	<p>Name of a predefined template used for statistics collection. A template name can be any combination of alphanumeric characters, and may include the underscore character (_). Use the <a href="#">show running performance-mgmt</a>, on page 427 command to display a list of available templates.</p>
<b>default</b>	<p>Applies the default template.</p>

**Command Default** Statistics collection is disabled.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.2	The <b>enable</b> keyword was replaced by the <b>apply</b> keyword. In previous releases, this command was referred to as <b>performance-mgmt enable statistics</b> . The <b>disable</b> keyword was deprecated. The <b>ospf v2protocol</b> and <b>ospf v3protocol</b> keywords were introduced to support the enabling of statistics collection templates for the OSPF entity. The <b>location</b> keyword was added. The <b>global</b> keyword was deprecated and replaced by the <b>location all</b> keywords.
	Release 3.3.0	Removed support for MPLS interfaces.
	Release 4.0.1	The <b>interface basic-counters</b> keyword was added to support the enabling of statistics collection template for the basic counters.

**Usage Guidelines** Use the **performance-mgmt apply statistics** command to apply a statistics template and enable statistics collection. Only one template for each entity can be enabled at a time. After samples are taken, the data is sent to a directory on an external TFTP server, and a new collection cycle starts. The directory where data is copied to is configured using the [performance-mgmt resources tftp-server, on page 399](#) command. The statistics data in the directory contains the type of entity, parameters, instances, and samples. They are in binary format and must be viewed using a customer-supplied tool, or they can be queried as they are being collected using XML.

Use the **performance-mgmt apply statistics** command to collect data for all the instances on a continuous basis. To analyze a particular instance for a limited period of time, use the [performance-mgmt apply monitor, on page 386](#) command.

Use the **no** form of the command to disable statistics collection. Because only one performance management statistics collection can be enabled for any given entity at any given time, you are not required to specify the template name with the **default** keyword or **template** keyword and *template-name* argument when disabling a performance management statistics collection.

For information about creating templates, see the [performance-mgmt statistics, on page 401](#) command.



**Caution**

Each particular collection enabled requires a certain amount of resources. These resources are allocated for as long as the collection is enabled.

**Task ID**

Task ID	Operations
monitor	read, write, execute

**Examples**

This example shows how to start statistics collection for BGP using the template named bgp1:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply statistics bgp template bgp1
```

This example shows how to enable statistics collection for generic counters using the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply statistics interface generic-counters default
```

This example shows how to enable CPU statistics collection based on the settings set in the default template:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply statistics node cpu location all default
```

This example shows how to enable statistics collection for basic counters using the default template:

**Related Commands**

Command	Description
<a href="#">performance-mgmt apply monitor, on page 386</a>	Applies a statistics template to gather one sampling-size set of samples for a particular instance.
<a href="#">performance-mgmt apply thresholds, on page 392</a>	Applies a threshold template and enables threshold monitoring.
<a href="#">performance-mgmt resources tftp-server, on page 399</a>	Configures a destination TFTP server for statistics collections.
<a href="#">performance-mgmt statistics, on page 401</a>	Creates a template to use for collecting performance management statistics.
<a href="#">show running performance-mgmt, on page 427</a>	Displays a list of templates and the template being applied.

## performance-mgmt apply thresholds

To apply a thresholds template and enable threshold collection, use the **performance-mgmt apply thresholds** command in Global Configuration mode. To stop threshold collection, use the **no** form of this command.

**performance-mgmt apply thresholds** *entity* **location** {**all** | *node-id*} {*template-name* | **default**}

**no performance-mgmt apply thresholds**

### Syntax Description

<i>entity</i>	<p>Specifies an entity for which you want to apply a threshold template:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b>—Applies a threshold monitoring template for Border Gateway Protocol (BGP).</li> <li>• <b>interface basic-counters</b>—Applies a threshold monitoring template for basic counters.</li> <li>• <b>interface data-rates</b>—Applies a threshold monitoring template for data rates.</li> <li>• <b>interface generic-counters</b>—Applies a threshold monitoring template for generic counters.</li> <li>• <b>mpls ldp</b>—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.</li> <li>• <b>node cpu</b>—Applies a threshold monitoring template for central processing unit (CPU) utilization. Use the <b>location</b> keyword in conjugation with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>node memory</b>—Applies a threshold monitoring template for memory utilization. Use the <b>location</b> keyword in conjugation with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>node process</b>—Applies a threshold monitoring template for processes. Use the <b>location</b> keyword in conjugation with the <b>all</b> keyword or <i>node-id</i> argument when enabling a statistics collection template for this entity.</li> <li>• <b>ospf v2protocol</b>—Applies a threshold monitoring template for OSPFv2.</li> <li>• <b>ospf v3protocol</b>—Applies a threshold monitoring template for OSPFv3.</li> </ul>
<b>location</b> { <b>all</b>   <i>node-id</i> }	<p>Specifies all nodes or a particular node.</p> <p>Specify the <b>location all</b> keywords for all nodes, or the <i>node-id</i> argument to specify a particular node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. You must specify either the <b>location all</b> keywords or the <b>location</b> keyword and <i>node-id</i> argument with the <b>node cpu</b>, <b>node memory</b>, or <b>node process</b> entity.</p>
<b>template-name</b>	<p>Name of a predefined template used for threshold collection. A template name can be any combination of alphanumeric characters, and may include the underscore character (_). Use the <a href="#">show running performance-mgmt</a>, on page 427 command to display a list of available templates.</p>
<b>default</b>	<p>Applies the default template.</p>

**Command Default** Threshold collection is disabled.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.2	The <b>enable</b> keyword was replaced by the <b>apply</b> keyword. In previous releases, this command was referred to as <b>performance-mgmt enable thresholds</b> . The <b>disable</b> keyword was deprecated. The <b>ospf v2protocol</b> and <b>ospf v3protocol</b> keywords were introduced to support the enabling of threshold monitoring templates for the OSPF entity. The <b>location</b> keyword was added. The <b>global</b> keyword was deprecated and replaced by the <b>location all</b> keywords.
	Release 3.3.0	Removed support for MPLS interfaces.
	Release 4.0.1	The <b>interface basic-counters</b> keyword was added to support the enabling of threshold monitoring template for the basic counter.

**Usage Guidelines** Use the **performance-mgmt apply thresholds** command to apply a threshold template and enable threshold collection. Several templates can be configured, but only one template for each entity can be enabled at a time.

Use the **no** form of the command to disable threshold collection. Because only one performance management threshold monitoring template can be enabled for any given entity at any given time, you are not required to specify the template name with the **default** keyword or **template** keyword and *template-name* argument when disabling a performance management statistics collection.

For information about creating threshold templates, see the [performance-mgmt thresholds](#), on page 404 command.

Task ID	Task ID	Operations
	monitor	read, write, execute

**Examples** This example shows how to start threshold collection for BGP using a template named stats1:

```
RP/0/0/CPU0:router (config) #performance-mgmt apply thresholds bgp stats1
```

This example shows how to enable threshold collection for generic counters using a template named stats2:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply thresholds interface generic-counters stats2
```

This example shows how to enable CPU threshold collection using the template named cpu12:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply thresholds node cpu global cpu12
```

This example shows how to enable threshold checking for basic counters using a template named stats3:

```
RP/0/0/CPU0:router(config)#performance-mgmt apply thresholds interface basic-counters stats3
```

Related Commands

Command	Description
<a href="#">performance-mgmt thresholds, on page 404</a>	Creates a template to use for threshold collection.
<a href="#">show running performance-mgmt, on page 427</a>	Displays a list of templates and the template being applied.

# performance-mgmt regular-expression

To apply a defined regular expression group to one or more statistics or threshold template, use the **performance-mgmt regular-expression** *regular-expression-name* command in Global Configuration mode. To stop the usage of regular expression, use the **no** form of this command.

**performance-mgmt regular-expression** *regular-expression-name* **index** *number* *regular-expression-string*  
**no performance-mgmt regular-expression** *regular-expression-name*

## Syntax Description

<i>regular-expression-string</i>	Specifies a defined regular expression group to one or more statistics or threshold template.
<b>index</b>	Specifies a regular expression index. Range is 1 to 100.

## Command Default

No regular expression is configured by default.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 4.0.1	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
monitor	read, write

## Examples

This is the sample output from the **performance-mgmt regular-expression** command:

```
RP/0/0/CPU0:router# performance-mgmt regular-expression reg1 index 10
```

# performance-mgmt resources dump local

To configure the local filesystem on which the statistics data is dumped, use the **performance-mgmt resources dumplocal** command in Global Configuration mode. To stop dumping of statistics data on the local filesystem, use the **no** form of this command.

**performance-mgmt resources dump local**

**no performance-mgmt resources dump local**

## Syntax Description

<b>dump</b>	Configures data dump parameters.
<b>local</b>	Sets the local filesystem on which statistics data is dumped.
<b>Note</b>	You can also dump the statistics data on the TFTP server location. But the configuration is rejected if you configure both local dump and TFTP server at the same time.

## Command Default

Local filesystem is disabled.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 4.0.1	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
monitor	read, write

## Examples

This is the sample output for the **performance-mgmt resources dumplocal** command:

```
RP/0/0/CPU0:router# performance-mgmt resources dump local
```



## performance-mgmt resources memory

To configure memory consumption limits for performance management (PM), use the **performance-mgmt resources memory** command in Global Configuration mode. To restore the default memory consumption limits, use the **no** form of this command.

**performance-mgmt resources memory max-limit** *kilobytes* **min-reserved** *kilobytes*  
**no performance-mgmt resources memory**

### Syntax Description

<b>max-limit</b> <i>kilobytes</i>	Specifies the maximum amount of memory (specified with the <i>kilobytes</i> argument) that the PM statistics collector can use for serving data collection requests. Range is 0 to 4294967295 kilobytes. The default is 50000 kilobytes.
<b>min-reserved</b> <i>kilobytes</i>	Specifies a minimum amount of memory (specified with the <i>kilobytes</i> argument) that must remain available in the system after allowing a new PM data collection request. Range is 0 to 4294967295 kilobytes. The default is 10000 kilobytes.

### Command Default

**max-limit**—50000 *kilobytes*  
**min-reserved**—10000 *kilobytes*

### Command Modes

Global Configuration mode

### Command History

Release	Modification
Release 3.2	This command was introduced.

### Usage Guidelines

Use the **performance-mgmt resource memory** command to ensure that the total memory consumed by data buffers in PM does not exceed a maximum limit and that any new PM data request does not cause available memory in the system to fall below a certain threshold.

### Task ID

Task ID	Operations
monitor	read, write

## Examples

This example shows how to ensure that the total memory consumed by PM data buffers does not exceed 30,000 kilobytes and that any new PM data request does not cause available memory in the system to fall below 5000 kilobytes:

```
RP/0/0/CPU0:router(config)# performance-mgmt resources memory max-limit 30000 min-reserved  
5000
```

## performance-mgmt resources tftp-server

To configure a destination TFTP server for PM statistics collections, use the **performance-mgmt resources tftp-server** command in Global Configuration mode. To disable the resource, use the **no** form of this command.

**performance-mgmt resources tftp-server** *ip-address* [**directory** *dir-name*] [**vrf** *{vrf\_name| default}*] [**directory** *dir-name*]

**no performance-mgmt resources tftp-server**

### Syntax Description

<b>tftp-server</b> <i>ip-address</i>	Specifies the IP address of the TFTP server.
<b>directory</b> <i>dir-name</i>	Specifies the directory where performance management statistics will be copied.
<b>vrf</b> <i>vrf_name</i>	Specifies the name of the VRF instance.
<b>default</b>	Specifies the default VRF.

### Command Default

A destination TFTP server is not configured and data is not copied out of the system after a collection cycle (sampling-size) ends.

### Command Modes

Global Configuration mode

### Command History

Release	Modification
Release 3.2	This command was introduced.

### Usage Guidelines

Use the **performance-mgmt resources tftp-server** command to configure a TFTP resource for performance management. By creating a directory name on the TFTP server, you create a place where statistics can be collected when statistics collection is enabled.

Use the **no** form of this command to disable the TFTP resource.



#### Note

Files copied to the TFTP server contain a timestamp in their name, which makes them unique. For that reason the TFTP server used should support creation of files as data is transferred, without requiring users to manually create them at the TFTP server host in advance.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

This example shows how to specify a TFTP server with the IP address 192.168.134.254 as the performance management resource and a directory named /user/perfmgmt/tftpdump as the destination for PM statistic collections:

```
RP/0/0/CPU0:router(config)#performance-mgmt resources tftp-server 192.168.134.254 directory /user/perfmgmt/tftpdump
```

**Related Commands**

Command	Description
<a href="#">performance-mgmt apply statistics, on page 389</a>	Applies a statistics template and enables statistics collection.
<a href="#">performance-mgmt apply thresholds, on page 392</a>	Applies a threshold template and enables threshold monitoring.

# performance-mgmt statistics

To create a template to use for collecting performance management statistics, use the **performance-mgmt statistics** command in Global Configuration mode. To remove a template, use the **no** form of this command.

**performance-mgmt statistics** *entity* {**template** *template-name* | **default**} [**sample-size** *size*] [**sample-interval** *minutes*]**history-persistent** **regular-expression**

**no performance-mgmt statistics**

## Syntax Description

*entity*

Specify an entity for which you want to create a statistics template:

- **bgp**—Creates a statistics collection template for Border Gateway Protocol (BGP).
- **interface basic-counters**—Creates a statistics collection template for basic counters.
- **interface data-rates**—Creates a statistics collection template for data rates.
- **interface generic-counters**—Creates a statistics collection template for generic counters.
- **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.
- **node cpu**—Creates a statistics collection template for the central processing unit (CPU).
- **node memory**—Creates a statistics collection template for memory utilization.
- **node process**—Creates a statistics collection template for processes.
- **ospf v2protocol**—Creates a statistics template for Open Shortest Path First v2 (OSPFv2) protocol instances.
- **ospf v3protocol**—Creates a statistics template for OSPFv3 protocol instances.

**template**

Specifies that a template will be used for collection.

<i>template-name</i>	<p>A template name can be any combination of alphanumeric characters, and may include the underscore character (_).</p> <p>Use the <a href="#">show running performance-mgmt</a>, on page 427 to display information about templates, and to display the templates that are being used.</p>
<b>default</b>	<p>Applies the settings of the default template. The default template contains the following statistics and values. Values are in minutes.</p> <p>Each entity has a default template. In each default template, the sample interval is 10 minutes, and the default sample count is 5.</p>
<b>sample-size</b> <i>size</i>	(Optional) Sets the number of samples to be taken.
<b>sample-interval</b> <i>minutes</i>	(Optional) Sets the frequency of each sample, in minutes.
<b>history-persistent</b>	(Optional) Maintains the history of statistics collections persistently.
<b>regular-expression</b> <i>regular-expression-group-name</i>	(Optional) Sets instance filtering by regular expression.

**Command Default** Statistics collections for all entities is disabled.

**Command Modes** Global Configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.
	Release 3.2	The <b>ospf v2protocol</b> and <b>ospf v3protocol</b> keywords were introduced to support the creation of statistics collection templates for the OSPF entity.
	Release 3.3.0	Removed support for MPLS interfaces.
	Release 4.0.1	The <b>interface basic-counters</b> keyword was added to support the creation of statistics collection templates for the basic counters. The <b>history-persistent</b> and <b>regular-expression</b> keywords were added.

**Usage Guidelines** If you have not yet created a directory for the statistics, use the [performance-mgmt resources tftp-server](#), on page 399 command to create a directory on an external TFTP server. When you apply the template and enable

statistics collection with the [performance-mgmt apply statistics, on page 389](#) command, the samples are collected and sent to that directory for later retrieval.

The statistics collected contain type of entity, parameters, instances, and samples. The collection files on the TFTP server are in binary format and must be viewed using a customer-supplied tool or they can be queried as they are being collected using XML.

### Task ID

Task ID	Operations
monitor	read, write

### Examples

This example shows how to create a template named int\_data\_rates for data rate statistics collection, how to set the sample size to 25, and how to set the sample interval to 5 minutes:

```
RP/0/0/CPU0:router(config)#performance-mgmt statistics interface data-rates int_data_rates
RP/0/0/CPU0:router(config_stats-if-rate)# sample-size 25
RP/0/0/CPU0:router(config_stats-if-rate)# sample-interval 5
```

### Related Commands

Command	Description
<a href="#">performance-mgmt apply statistics, on page 389</a>	Applies a statistics template and enables statistics collection.
<a href="#">performance-mgmt resources tftp-server, on page 399</a>	Configures resources for the performance management system that are independent of any particular entity.
<a href="#">performance-mgmt thresholds, on page 404</a>	Configures a template for collecting threshold statistics.
<a href="#">show running performance-mgmt, on page 427</a>	Displays a list of templates and the template being applied.

# performance-mgmt thresholds

To configure a template for threshold checking, use the **performance-mgmt thresholds** command in Global Configuration mode. To remove a threshold template, use the **no** form of this command.

**performance-mgmt thresholds** *entity* {**template** *template-name*| **default**} *attribute* *operation* *value* [ *value2* ] [ *percent* ] [**rearm** {**toggle**| **window** *window-size*}]

**no performance-mgmt thresholds**

## Syntax Description

<i>entity</i>	Specify an entity for which you want to create a template: <ul style="list-style-type: none"> <li>• <b>bgp</b> —Creates a template for threshold collection for Border Gateway Protocol (BGP).</li> <li>• <b>interface basic-counters</b> —Creates a threshold monitoring template for basic counters.</li> <li>• <b>interface data-rates</b> —Creates a threshold monitoring template for data rates.</li> <li>• <b>interface generic-counters</b> —Creates a threshold monitoring template for generic counters.</li> <li>• <b>mpls ldp</b> —Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.</li> <li>• <b>node cpu</b> —Creates a threshold monitoring template for the central processing unit (CPU).</li> <li>• <b>node memory</b> —Creates a threshold monitoring template for memory utilization.</li> <li>• <b>node process</b> —Creates a threshold monitoring template for processes.</li> <li>• <b>ospf v2protocol</b> —Creates a threshold monitoring template for Open Shortest Path First v2 (OSPFv2) process instances.</li> <li>• <b>ospf v3protocol</b> —Creates a threshold monitoring template for OSPFv3 process instances.</li> </ul>
<b>template</b>	Specifies that a template will be used for collection.
<i>template-name</i>	Name of a predefined template used for threshold collection. A template name can be any combination of alphanumeric characters, and may include the underscore character (_). Use the <a href="#">show running performance-mgmt</a> , <a href="#">on page 427</a> to display information about templates, and to display the templates that are being used.
<b>default</b>	Applies the settings of the default template.
<i>attribute</i>	The attributes for the entity. See <a href="#">Table 36: Attribute Values</a> , <a href="#">on page 406</a> for a list of attributes.



<i>operation</i>	<p>A limiting operation for thresholding that includes:</p> <ul style="list-style-type: none"> <li>• <b>EQ</b> —Equal to.</li> <li>• <b>GE</b> —Greater than or equal to.</li> <li>• <b>GT</b> —Greater than.</li> <li>• <b>LE</b> —Less than or equal to.</li> <li>• <b>LT</b> —Less than.</li> <li>• <b>NE</b> —Not equal to.</li> <li>• <b>RG</b> —Not in range.</li> </ul>
<i>value</i>	The base value against which you want to sample.
<i>value2</i>	(Optional) This value can only be used with the operator <b>RG</b> . For example, if you use <b>RG</b> for the operation argument value, you create a range between <i>value</i> and <i>value2</i> .
<i>percent</i>	(Optional) Specifies a value relative to the previous sample interval value. See the “Usage Guidelines” section for more information.
<b>rearm {toggle   window}</b>	<p>(Optional) It can be used to reduce the number of events by suppressing redundant events from being reported. Normally, every time a condition is met in a sample interval, a syslog error is generated. Using the <b>toggle</b> keyword works in this manner: If a condition is true, a syslog error message is generated, but it is not generated again until the condition becomes false, and then true again. In this way, only “fresh” events are seen when the threshold is crossed.</p> <p>Use the <b>window</b> keyword to specify that an event be sent only once for each window. If a condition is true, a syslog error message is generated. You set your window size by using the <b>window</b> keyword and specify the number of intervals. With a window size, you specify that you want event notification at that number of intervals. For example, if you window size is 2 and your sample interval is 10, you would want notification of the event (for each instance in an entity) only every 20 minutes when the condition has been met.</p>
<i>window-size</i>	The number of intervals to use with the <b>rearm</b> keyword.

**Command Default**

None

**Command Modes**

Global Configuration mode

**Command History**

Release	Modification
Release 2.0	This command was introduced.

Release	Modification
Release 3.2	The <b>ospf v2protocol</b> and <b>ospf v3protocol</b> keywords were introduced to support the creation of OSPF threshold monitoring templates. OSPF attribute values were introduced for threshold monitoring.
Release 3.3.0	Removed support for MPLS interfaces.
Release 4.0.1	The <b>interface basic-counters</b> keyword was added to support the creation of threshold monitoring template for the basic counter.

### Usage Guidelines

Use the *percent* argument to specify a value that is relative to the previous sample's interval value. When you use the *percent* argument with a *value* of 50, the calculation is performed in this manner, assuming that your current sampled value is sample1 (S1) and the value sampled in the previous sampling period is sample 0 (S0):

$(S1 - S0) \text{ GT } 50\% \text{ of } S0$

For example, if you wanted to check for an increase of 50 percent in the counter BGPInputErrors, you could use the following *attribute* and *operation* with the *percent* argument:

BGPInputErrors GT 50

This table shows threshold behavior, assuming the values for BGPInputErrors are at consecutive samplings.

**Table 35: Threshold Behavior**

Value	Calculation	Event
10	—	—
16	16 - 10 = 6, which is > than 50 percent of 10	Generate event
20	20 - 16 = 4, which is not > than 50 percent of 16	No event generated
35	35 - 20 = 15, which is > than 50 percent of 20	Generate event

This table shows the attribute values supported by the entities.

**Table 36: Attribute Values**

Entity	Attributes	Description
bgp	ConnDropped	Number of times the connection was dropped.
	ConnEstablished	Number of times the connection was established.
	ErrorsReceived	Number of error notifications received on the connection.
	ErrorsSent	Number of error notifications sent on the connection.
	InputMessages	Number of messages received.
	InputUpdateMessages	Number of update messages received.
	OutputMessages	Number of messages sent.
	OutputUpdateMessages	Number of update messages sent.
interface basic-counters	InOctets	Bytes received (64-bit).
	InPackets	Packets received (64-bit).
	InputQueueDrops	Input queue drops (64-bit).
	InputTotalDrops	Inbound correct packets discarded (64-bit).
	InputTotalErrors	Inbound incorrect packets discarded (64-bit).
	OutOctets	Bytes sent (64-bit).
	OutPackets	Packets sent (64-bit).
	OutputQueueDrops	Output queue drops (64-bit).
	OutputTotalDrops	Outbound correct packets discarded (64-bit).
	OutputTotalErrors	Outbound incorrect packets discarded (64-bit).

Entity	Attributes	Description
interface data-rates	Bandwidth	Bandwidth, in kbps.
	InputDataRate	Input data rate in kbps.
	InputPacketRate	Input packets per second.
	InputPeakRate	Peak input data rate.
	InputPeakPkts	Peak input packet rate.
	OutputDataRate	Output data rate in kbps.
	OutputPacketRate	Output packets per second.
	OutputPeakPkts	Peak output packet rate.
	OutputPeakRate	Peak output data rate.

Entity	Attributes	Description
interface generic-counters	InBroadcastPkts	Broadcast packets received.
	InMulticastPkts	Multicast packets received.
	InOctets	Bytes received.
	InPackets	Packets received.
	InputCRC	Inbound packets discarded with incorrect CRC.
	InputFrame	Inbound framing errors.
	InputOverrun	Input overruns.
	InputQueueDrops	Input queue drops.
	InputTotalDrops	Inbound correct packets discarded.
	InputTotalErrors	Inbound incorrect packets discarded.
	InUcastPkts	Unicast packets received.
	InputUnknownProto	Inbound packets discarded with unknown proto.
	OutBroadcastPkts	Broadcast packets sent.
	OutMulticastPkts	Multicast packets sent.
	OutOctets	Bytes sent.
	OutPackets	Packets sent.
	OutputTotalDrops	Outbound correct packets discarded.
	OutputTotalErrors	Outbound incorrect packets discarded.
	OutUcastPkts	Unicast packets sent.
	OutputUnderrun	Output underruns.

Entity	Attributes	Description
mpls ldp	AddressMsgsRcvd	Address messages received.
	AddressMsgsSent	Address messages sent.
	AddressWithdrawMsgsRcvd	Address withdraw messages received.
	AddressWithdrawMsgsSent	Address withdraw messages sent.
	InitMsgsSent	Initial messages sent.
	InitMsgsRcvd	Initial messages received.
	KeepaliveMsgsRcvd	Keepalive messages received.
	KeepaliveMsgsSent	Keepalive messages sent.
	LabelMappingMsgsRcvd	Label mapping messages received.
	LabelMappingMsgsSent	Label mapping messages sent.
	LabelReleaseMsgsRcvd	Label release messages received.
	LabelReleaseMsgsSent	Label release messages sent.
	LabelWithdrawMsgsRcvd	Label withdraw messages received.
	LabelWithdrawMsgsSent	Label withdraw messages sent.
	NotificationMsgsRcvd	Notification messages received.
	NotificationMsgsSent	Notification messages sent.
	TotalMsgsRcvd	Total messages received.
	TotalMsgsSent	Total messages sent.
node cpu	AverageCPUUsed	Average system percent CPU utilization.
	NoProcesses	Number of processes.
node memory	CurrMemory	Current application memory (in bytes) in use.
	PeakMemory	Maximum system memory (in MB) used since bootup.

Entity	Attributes	Description
node process	AverageCPUUsed	Average percent CPU utilization.
	NumThreads	Number of threads.
	PeakMemory	Maximum dynamic memory (in KB) used since startup time.

Entity	Attributes	Description
ospf v2protocol	InputPackets	Total number of packets received
	OutputPackets	Total number of packets sent
	InputHelloPackets	Number of Hello packets received
	OutputHelloPackets	Number of Hello packets sent
	InputDBDs	Number of DBD packets received
	InputDBDsLSA	Number of LSA received in DBD packets
	OutputDBDs	Number of DBD packets sent.
	OutputDBDsLSA	Number of LSA sent in DBD packets
	InputLSRequests	Number of LS requests received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSRequests	Number of LS requests sent.
	OutputLSRequestsLSA	Number of LSA sent in LS requests.
	InputLSAUpdates	Number of LSA updates received.
	InputLSAUpdatesLSA	Number of LSA received in LSA updates.
	OutputLSAUpdates	Number of LSA updates sent.
	OutputLSAUpdatesLSA	Number of LSA sent in LSA updates.
	InputLSAAcks	Number of LSA acknowledgements received.
	InputLSAAcksLSA	Number of LSA received in LSA acknowledgements.
	OutputLSAAcks	Number of LSA acknowledgements sent.
	OutputLSAAcksLSA	Number of LSA sent in LSA acknowledgements.



Entity	Attributes	Description
	ChecksumErrors	Number of packets received with checksum errors.

Entity	Attributes	Description
ospf v3protocol	InputPackets	Total number of packets received.
	OutputPackets	Total number of packets sent.
	InputHelloPackets	Number of Hello packets received.
	OutputHelloPackets	Number of Hello packets sent.
	InputDBDs	Number of DBD packets received.
	InputDBDsLSA	Number of LSA received in DBD packets.
	OutputDBDs	Number of DBD packets sent.
	OutputDBDsLSA	Number of LSA sent in DBD packets.
	InputLSRequests	Number of LS requests received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSRequests	Number of LS requests sent.
	OutputLSRequestsLSA	Number of LSA sent in LS requests.
	InputLSAUpdates	Number of LSA updates received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSAUpdates	Number of LSA updates sent.
	OutputLSAUpdatesLSA	Number of LSA sent in LSA updates.
	InputLSAAcks	Number of LSA acknowledgements received.
	InputLSAAcksLSA	Number of LSA received in LSA acknowledgements.
	OutputLSAAcks	Number of LSA acknowledgements sent
	OutputLSAAcksLSA	Number of LSA sent in LSA acknowledgements.

**Task ID**

Task ID	Operations
monitor	read, write

**Examples**

This example shows how to create a template for monitoring BGP thresholds, which checks if the number of connections dropped exceeds 50 for any BGP peers. The **toggle rearm** keywords are included so that once the threshold is passed, the event will not be reported unless the value of ConnDropped is reset:

```
RP/0/0/CPU0:router(config)# performance-mgmt thresholds bgp template bgp_thresh1
RP/0/0/CPU0:router(config-threshold-bgp)# ConnDropped GT 50 rearm toggle
```

This example shows how to create a template for monitoring node CPU utilization that checks if there is a 25 percent increase at any given interval:

```
RP/0/0/CPU0:router(config)# performance-mgmt thresholds node cpu template cpu_thresh1
RP/0/0/CPU0:router(config-threshold-bgp)# AverageCPUUsed GT 25percent
```

This example shows how to create a template for monitoring the input CRC errors for interfaces. The rule checks whether the number of errors reach or exceed 1000 for any given interface:

```
RP/0/0/CPU0:router(config)# performance-mgmt thresholds interface generic_ctr template
intf_crc_thresh1
RP/0/0/CPU0:router(config-threshold-bgp)# InputCRC GE 1000
```

**Related Commands**

Command	Description
<a href="#">performance-mgmt apply thresholds, on page 392</a>	Enables threshold monitoring for BGP.
<a href="#">performance-mgmt resources tftp-server, on page 399</a>	Configures a TFTP resource for performance management.
<a href="#">show running performance-mgmt, on page 427</a>	Displays a list of templates and the template being applied.

# show performance-mgmt bgp

To display performance management (PM) data from Border Gateway Protocol (BGP) entity instance monitoring or statistics collections, use the **show performance-mgmt bgp** command in EXEC mode.

**show performance-mgmt {monitor|statistics} bgp {ip-address| all} {sample-id| all-samples| last-sample}**

Syntax Description

<b>monitor</b>	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle of a BGP statistics collection template. The data is available only as the monitor data is enabled.
<b>statistics</b>	Displays the data collected from statistics collection samples.
<i>ip-address</i>	IP address of a BGP peer.
<b>all</b>	Displays all BGP peer instances. <b>Note</b> This option is available only with the <b>statistics</b> keyword. It is not available with the <b>monitor</b> keyword because an entity instance monitoring collection captures data from an entity instance for one sampling cycle.
<i>sample-id</i>	Sample ID of the monitoring or statistics collection to be displayed.
<b>all-samples</b>	Displays all collected samples.
<b>last-sample</b>	Displays the last collected samples.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

## Examples

This is the sample output from the **show performance-mgmt bgp** command:

```
RP/0/0/CPU0:router# show performance-mgmt monitor bgp 10.0.0.0 all-samples

BGP Neighbor: 10.0.0.0 Sample no: 1
-----
InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
ErrorsReceived: 0 ErrorsSent: 0 BGP Neighbor: 10.0.0.0 Sample no: 2
-----
InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
ErrorsReceived: 0 ErrorsSent: 0 BGP Neighbor: 10.0.0.0 Sample no: 3
-----
InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
ErrorsReceived: 0 ErrorsSent: 0
```

This table describes the significant fields in the display.

**Table 37: show performance-mgmt bgp Field Descriptions**

Field	Description
ConnDropped	Number of times the connection was dropped.
ConnEstablished	Number of times the connection was established.
ErrorsReceived	Number of error notifications received on the connection.
ErrorsSent	Number of error notifications sent on the connection.
InputMessages	Number of messages received.
InputUpdateMessages	Number of update messages received.
OutputMessages	Number of messages sent.
OutputUpdateMessages	Number of update messages sent.

# show performance-mgmt interface

To display performance management (PM) data from interface entity instance monitoring or statistics collections, use the **show performance-mgmt interface** command in EXEC mode.

**show performance-mgmt** {**monitor**|**statistics**} **interface** {**basic-counters**|**data-rates**|**generic-counters**} {*type interface-path-id*|**all**} {*sample-id*|**all-samples**|**last-sample**}

## Syntax Description

<b>monitor</b>	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle from one instance of an interface data entity collection template.  <b>Note</b> The data is available to be display only as the monitor data is collected.
<b>statistics</b>	Displays the data collected from statistics collection samples.
<b>basic-counters</b>	Displays data from interface basic counters entity collections.
<b>data-rates</b>	Displays data from interface data rates entity collections.
<b>generic-counters</b>	Displays data from interface generic counters entity collections.
<i>type</i>	(Optional) Interface type. For more information, use the question mark ( ? ) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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.
<b>all</b>	Displays all interface instances.  <b>Note</b> This option is available only with the <b>statistics</b> keyword. It is not available with the <b>monitor</b> keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle.
<i>sample-id</i>	Sample ID of the monitoring collection or statistics collection to be displayed.
<b>all-samples</b>	Displays all collected samples.
<b>last-sample</b>	Displays the last collected samples.

## Command Default

None

**Command Modes**

EXEC mode

**Command History**

Release	Modification
Release 3.2	This command was introduced.
Release 4.0.1	The basic-counters keyword was added to support basic counters entity collections.

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

Task ID	Operations
monitor	read

**Examples**This is sample output from the **show performance-mgmt interface** command:

```
RP/0/0/CPU0:router# show performance-mgmt monitor interface generic-counters pos 0/3/0/0 all-samples
```

```
Interface: POS0_3_0_0 Sample no: 1
```

```
-----
InPackets: 0 OutPackets: 0 InOctets: 0
OutOctets: 0 InUcastPkts: 0 OutUcastPkts: 0 InMulticastPkts: 0 OutMulticastPkts: 0
InBroadcastPkts: 0 OutBroadcastPkts: 0 InputTotalDrops: 0 OutputTotalDrops: 0
InputTotalErrors: 0 OutputTotalErrors: 0 InputOverrun: 0 OutputUnderrun: 0
InputQueueDrops: 0 InputUnknownProto: 0 InputCRC: 0 InputFrame: 0 Interface: POS0_3_0_0
Sample no: 2 ----- InPackets: 0 OutPackets: 0
InOctets: 0 OutOctets: 0 InUcastPkts: 0 OutUcastPkts: 0 InMulticastPkts: 0
OutMulticastPkts: 0 InBroadcastPkts: 0 OutBroadcastPkts: 0 InputTotalDrops: 0
OutputTotalDrops: 0 InputTotalErrors: 0 OutputTotalErrors: 0 InputOverrun: 0
OutputUnderrun: 0 InputQueueDrops: 0 InputUnknownProto: 0 InputCRC: 0 InputFrame: 0
```

```
RP/0/0/CPU0:router# show performance-mgmt monitor interface generic-counters hundredGigE 0/3/0/0 all-samples
```

```
Interface: HundredGigE0_3_0_0 Sample no: 1
```

```
-----
InPackets: 0 OutPackets: 0 InOctets: 0
OutOctets: 0 InUcastPkts: 0 OutUcastPkts: 0 InMulticastPkts: 0 OutMulticastPkts: 0
InBroadcastPkts: 0 OutBroadcastPkts: 0 InputTotalDrops: 0 OutputTotalDrops: 0
InputTotalErrors: 0 OutputTotalErrors: 0 InputOverrun: 0 OutputUnderrun: 0
InputQueueDrops: 0 InputUnknownProto: 0 InputCRC: 0 InputFrame: 0 Interface:
HundredGigE0_3_0_0
Sample no: 2 ----- InPackets: 0 OutPackets: 0
InOctets: 0 OutOctets: 0 InUcastPkts: 0 OutUcastPkts: 0 InMulticastPkts: 0
OutMulticastPkts: 0 InBroadcastPkts: 0 OutBroadcastPkts: 0 InputTotalDrops: 0
OutputTotalDrops: 0 InputTotalErrors: 0 OutputTotalErrors: 0 InputOverrun: 0
OutputUnderrun: 0 InputQueueDrops: 0 InputUnknownProto: 0 InputCRC: 0 InputFrame: 0
```

This table describes the significant fields shown in the display.

**Table 38: show performance-mgmt interface Field Descriptions**

Field	Description
InBroadcastPkts	Broadcast packets received.
InMulticast Pkts	Multicast packets received.
InOctets	Bytes received.
InPackets	Packets received.
InputCRC	Inbound packets discarded with incorrect CRC.
InputFrame	Inbound framing errors.
InputOverrun	Input overruns.
InputQueueDrops	Input queue drops.
InputTotalDrops	Inbound correct packets discarded.
InputTotalErrors	Inbound incorrect packets discarded.
InUcastPkts	Unicast packets received.
InputUnknownProto	Inbound packets discarded with unknown proto.
OutBroadcastPkts	Broadcast packets sent.
OutMulticastPkts	Multicast packets sent.
OutOctets	Bytes sent.
OutPackets	Packets sent.
OutputTotalDrops	Outbound correct packets discarded.
OutputTotalErrors	Outbound incorrect packets discarded.
OutUcastPkts	Unicast packets sent.
OutputUnderrun	Output underruns.



# show performance-mgmt mpls

To display performance management (PM) data for Multiprotocol Label Switching (MPLS) entity instance monitoring and statistics collections, use the **show performance-mgmt mpls** command in EXEC mode.

**show performance-mgmt** {**monitor**|**statistics**} **mpls ldp** {*ip-address*|**all**} {*first-sample-id*|**all-samples**|**last-sample**}

## Syntax Description

<b>monitor</b>	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle from one instance of an MPLS entity collection template.  <b>Note</b> The data is available to be displayed only as the monitor data is collected.
<b>statistics</b>	Displays the data collected from statistics collection samples.
<b>ldp</b>	Displays data from MPLS Label Distribution Protocol (LDP) collections.
<i>ip-address</i>	IP address of LDP session instance.
<b>all</b>	Displays data from all LDP session instances.  <b>Note</b> This option is available only with the <b>statistics</b> keyword. It is not available with the <b>monitor</b> keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle.
<i>first-sample-id</i>	Sample ID of the monitoring or statistics collection to be displayed.
<b>all-samples</b>	Displays all collected samples.
<b>last-sample</b>	Displays the last collected samples.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	Removed support for MPLS interfaces.

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

Task ID	Task ID	Operations
	monitor	read

**Examples** This is sample output from the **show performance-mgmt mpls** command:

```
RP/0/0/CPU0:router# show performance-mgmt monitor mpls ldp 192.0.2.45 last-sample
LDP Neighbor: 192.0.2.45 Sample no: 2
-----
TotalMsgsSent: 131,

TotalMsgsRcvd: 131 InitMsgsSent: 1, InitMsgsRcvd: 1 AddressMsgsSent: 1, AddressMsgsRcvd:
1 AddressWithdrawMsgsSent: 0, AddressWithdrawMsgsRcvd: 0 LabelMappingMsgsSent: 6,
LabelMappingMsgsRcvd: 7 LabelWithdrawMsgsSent: 0, LabelWithdrawMsgsRcvd: 0
LabelReleaseMsgsSent: 0, LabelReleaseMsgsRcvd: 0 NotificationMsgsSent: 0
NotificationMsgsRcvd: 0
```

This table describes the significant fields shown in the display.

Table 39: show performance-mgmt mpls Field Descriptions

Field	Description
InitMsgsSent	Initial messages sent.
InitMsgsRcvd	Initial messages received.
TotalMsgsSent	Total messages sent.
TotalMsgsRcvd	Total messages received.
AddressMsgsSent	Address messages sent.

## show performance-mgmt node

To display performance management (PM) data for node entity monitoring and statistics collections, use the **show performance-mgmt node** command in EXEC mode.

**show performance-mgmt** {**monitor**|**statistics**} **node** {**cpu**|**memory**|**process**} **location** {*node-id*|**all**}  
{*sample-id*|**all-samples**|**last-sample**}

### Syntax Description

<b>monitor</b>	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle from one instance of a node entity collection template.  <b>Note</b> The data is only available to be displayed as the monitor data is collected.
<b>statistics</b>	Displays the data collected from statistics collection samples.
<b>cpu</b>	Displays data from the central processing unit (CPU).
<b>memory</b>	Displays data from memory.
<b>process</b>	Displays data from processes.
<b>location</b>	Specifies the location of data origination.
<i>node-id</i>	Location of the node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>all</b>	Displays data from all LDP session instances.  <b>Note</b> This option is available only with the <b>statistics</b> keyword. It is not available with the <b>monitor</b> keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle.
<i>sample-id</i>	Sample ID of the monitoring or statistics collection to be displayed.
<b>all-samples</b>	Displays all collected samples.
<b>last-sample</b>	Displays the last collected samples.

### Command Default

None

### Command Modes

EXEC mode

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

This is sample output from the **show performance-mgmt node** command:

```
RP/0/0/CPU0:router# show performance-mgmt monitor node process location 0/RP1/CPU0 process
                               614587 last-sample
Node ID: 0_RP1_CPU0
Sample no: 1 ----- Process ID: 614587
----- PeakMemory: 908 AverageCPUUsed: 0
NoThreads: 5
```

This table describes the significant fields shown in the display.

Table 40: show performance-mgmt node Field Descriptions

Field	Description
PeakMemory	Maximum system memory (in MB) used since bootup.
AverageCPUUsed	Average system percent CPU utilization.
NoThreads	Number of threads.

# show performance-mgmt ospf

To display performance management (PM) data for Open Shortest Path First (OSPF) entity instance monitoring and statistics collections, use the **show performance-mgmt ospf** command in EXEC mode.

**show performance-mgmt** {**monitor**|**statistics**} **ospf** {**v2protocol**|**v3protocol**} *instance* {*sample-id*|**all-samples**|**last-sample**}

## Syntax Description

<b>monitor</b>	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle from one instance of an OSPF entity collection template.  <b>Note</b> The data is available to be displayed only as the monitor data is collected.
<b>statistics</b>	Displays the data collected from statistics collection samples.
<b>v2protocol</b>	Displays counters for an OSPF v2 protocol instance.
<b>v3protocol</b>	Displays counters for an OSPF v3 protocol instance.
<i>sample-id</i>	Sample ID of the monitoring or statistics collection to be displayed.
<b>all-samples</b>	Displays all collected samples.
<b>last-sample</b>	Displays the last collected samples.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.7.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

This is sample output from the **show performance-mgmt ospf** command:

```
RP/0/0/CPU0:router(config)# show performance-mgmt statistics ospf v2protocol 100 all-samples

Mon Aug 3 06:41:15.785 PST
OSPF Instance: 100 Sample no: 1
-----
InputPackets: 12323 OutputPackets: 12045
InputHelloPackets: 11281 OutputHelloPackets: 11276
InputDBDs: 18 OutputDBDs: 20
InputDBDsLSA: 508 OutputDBDsLSA: 530
InputLSRequests: 1 OutputLSRequests: 2
InputLSRequestsLSA: 11 OutputLSRequestsLSA: 0
InputLSAUpdates: 989 OutputLSAUpdates: 109
InputLSAUpdatesLSA: 28282 OutputLSAUpdatesLSA: 587
InputLSAacks: 34 OutputLSAacks: 638
InputLSAacksLSA: 299 OutputLSAacksLSA: 27995
ChecksumErrors: 0
```

# show running performance-mgmt

To display a list of configured templates and the template being applied, use the **show running performance-mgmt** command in EXEC mode.

**show running performance-mgmt** [**apply**| **resources**| **statistics**| **thresholds**]

## Syntax Description

<b>apply</b>	(Optional) Displays the list of apply template commands in the current configuration.
<b>resources</b>	(Optional) Displays the existing resource configuration commands applied.
<b>statistics</b>	(Optional) Displays the list of configured statistics templates.
<b>thresholds</b>	(Optional) Displays the list of configured threshold templates.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
monitor	read, write

## Examples

This example shows the list of statistic and threshold templates, the configuration of each template, and at the end, which templates are enabled for collection:

```
RP/0/0/CPU0:router(config)#show running performance-mgmt
```

```
performance-mgmt resources tftp-server 192.168.134.254 directory muckier/jagrello/pmtest
performance-mgmt statistics bgp template template3
  sample-size 5
  sample-interval 60
```

```
!  
performance-mgmt statistics node cpu template template4  
  sample-size 30  
  sample-interval 2  
!  
performance-mgmt statistics interface generic-counters template template2  
  sample-size 3  
  sample-interval 10  
!  
performance-mgmt statistics interface data-rates template template1  
  sample-size 10  
  sample-interval 5  
!  
performance-mgmt statistics node memory template template5  
  sample-size 30  
  sample-interval 2  
!  
performance-mgmt statistics node process template template6  
  sample-size 10  
  sample-interval 5  
!  
performance-mgmt thresholds node cpu template template20  
  AverageCpuUsed GT 75  
  sample-interval 5  
!  
performance-mgmt apply statistics interface generic-counters template2  
performance-mgmt apply statistics node memory global template5  
performance-mgmt apply statistics node process 0/0/CPU0 template6  
performance-mgmt apply thresholds node cpu global template20
```





## Statistics Service Commands

---

This module describes the Cisco IOS XR software commands related to the collection of interface statistics (StatsD) for system monitoring on the router. Interface statistics on the router are found in hardware (most of the time) and software (exception packets). The counters are always local (relative to the CPU) to the node on which the interface is homed. The Cisco IOS XR software provides an efficient mechanism to collect these counters from various application-specific integrated circuits (ASICs) or NetIO and assemble an accurate set of statistics for an interface. After the statistics are produced, they can be exported to interested parties (command-line interface [CLI], Simple Network Management Protocol [SNMP], and so forth).

The Cisco IOS XR software statistics collection system provides a common framework to be used by all interface owners to export the statistics for interfaces they own. The system also defines a common set of statistics that are relevant to all interfaces and thereby provides a consistent and constant set of counters that are always associated and maintained with any interface on the router.

The statistics collection system includes the statistics manager, the statistics server, one or more statistics collectors, and the necessary libraries. Each node on a router houses one statistics server.

In addition to the statistics server, each node (that has interfaces) has one or more statistics collectors. Statistics collectors are platform specific and can obtain various hardware and software counters to satisfy requests from the statistics server.

The statistics manager does not attempt to produce statistics for interfaces for which no statistics collector has registered. Requests for statistics on interfaces for which no statistics collector has registered results in an error returned to the requestor by the statistics manager.

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 counters](#), page 430
- [load-interval](#), page 432

# clear counters

To clear the interface counters, use the **clear counters** command in EXEC mode mode.

**clear counters** [**all**| *type interface-path-id*]

## Syntax Description

<b>all</b>	(Optional) Clears counters on all interfaces.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.  <b>Note</b> Use the <b>show interfaces</b> 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

Counters for all interfaces are cleared.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

Use the **clear counters** command to clear all the statistics counters displayed by the **show interfaces** command. If no optional arguments are supplied or if the **all** keyword is specified, then the counters for all interfaces are cleared. If an interface type is specified, then only the counters for that interface are cleared.

The **clear counters** command with the **all** option clears counters on all interfaces. When you enter this command, the system prompts you for confirmation. You must then press Enter or the *y* key for the **clear counters** command to take effect.



### Note

This command does not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those counters displayed with the **show interfaces** command.

**Task ID**

Task ID	Operations
interface	execute

**Examples**

This example shows how to clear counters on all interfaces:

```
RP/0/0/CPU0:router# clear counters all  
Clear "show interface" counters on all interfaces [confirm]
```

This example shows how to clear the interface counters for Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/0/CPU0:router# clear counters POS 0/1/0/0  
Clear "show interface" counters on this interface [confirm]
```

**Related Commands**

Command	Description
show interfaces	Displays statistics for all interfaces configured on the networking device.

# load-interval

To specify the interval for load calculation of an interface, use the **load-interval** command in interface configuration mode. To reset the load interval to the default setting, use the **no** form of this command.

**load-interval** *seconds*

**no load-interval** *seconds*

## Syntax Description

<i>seconds</i>	Number of seconds for load calculation of an interface. The value range is from 0 to 600 seconds and in increments of 30 (such as 30, 60, 90, and so on). The default is 300 seconds.
----------------	---

## Command Default

*seconds*: 300 seconds (5 minutes)

## Command Modes

Interface configuration

## Command History

Release	Modification
Release 3.2	This command was introduced.

## Usage Guidelines

When load interval is set to zero, load calculation is disabled. If you set the load interval, you must use a multiple of 30 (up to 600 seconds).

## Task ID

Task ID	Operations
interface	read/write

## Examples

This example shows how to configure the load interval to 30 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/0/CPU0:router(config-if)# load-interval 30
```



## Diagnostics Commands

---

This module provides command line interface (CLI) commands for configuring diagnostics 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.

- [diagnostic load, page 434](#)
- [diagnostic monitor, page 436](#)
- [diagnostic monitor interval, page 438](#)
- [diagnostic monitor syslog, page 440](#)
- [diagnostic monitor threshold, page 441](#)
- [diagnostic ondemand action-on-failure, page 443](#)
- [diagnostic ondemand iterations, page 445](#)
- [diagnostic schedule, page 446](#)
- [diagnostic start, page 448](#)
- [diagnostic stop, page 450](#)
- [diagnostic unload, page 451](#)
- [ping \(administration EXEC\), page 453](#)
- [show diag , page 458](#)
- [show diagnostic bootup level, page 463](#)
- [show diagnostic content, page 464](#)
- [show diagnostic ondemand settings, page 467](#)
- [show diagnostic result, page 468](#)
- [show diagnostic schedule, page 471](#)
- [show diagnostic status, page 473](#)
- [show run diagnostic monitor, page 474](#)

# diagnostic load

To load an offline diagnostic image for integrated field diagnostics, use the **diagnostic load** command in Admin EXEC mode.

**diagnostic load location** *node-id* [**autostart** {**all**|**basic**}]

Syntax Description

<b>location</b> <i>node-id</i>	Loads an offline diagnostic image for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. All modules in the specified slot are loaded with the offline diagnostic image.
<b>autostart</b> { <b>all</b>   <b>basic</b> }	(Optional) Starts running the diagnostic tests after the image has loaded. The following options are available: <ul style="list-style-type: none"><li>• <b>all</b>—Runs all tests.</li><li>• <b>basic</b>—Runs basic tests</li></ul>

Command Default

None

Command Modes

Admin EXEC mode

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

Use the **diagnostic load** command to load an offline diagnostic image used for integrated field diagnostics. Loading a diagnostic image places the specified card out of service.

The time it takes to load a diagnostic image varies depending on the card. Use the **show platform** command to determine if the image has been loaded and if the card has been placed out of service.



Note

The distributed route processor (DRP) does not support the automatic running of tests when the image is loaded for CPU0 and CPU1. After the diagnostic image is loaded, use the **diagnostic start location** *node-id* **test** {*id* | **all** | **basic** | **non-disruptive**} command to execute the tests.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

**Task ID**

Task ID	Operations
diag	execute

**Examples**

The following example shows how to load an offline diagnostic image:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# diagnostic load location 0/0/CPU0 autostart basic

diagnostic load will bring requested slot out of service. [confirm(y/n)] y
User has confirmed diagnostic load request
Preparing UUT for Diagnostics software.
Downloading IDS diagnostics image /pkg/ucode/hfr-diag-l3sp-fdiags
Downloading IDS diagnostics image /pkg/ucode/hfr-diag-l3-fdiags
Please wait for UUT image downloading ...
diagnostic load in progress.
```

**Related Commands**

Command	Description
show platform	Displays information and status of each node in the system.

# diagnostic monitor

To configure the health-monitoring diagnostic testing for a specified location, use the **diagnostic monitor** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**diagnostic monitor location** *node-id* **test** {*id* | *test-name*} [**disable**]

**no diagnostic monitor location** *node-id* **test** {*id* | *test-name*} [**disable**]

## Syntax Description

<i>node-id</i>	Location to enable diagnostic monitoring. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b> { <i>id</i>   <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <ul style="list-style-type: none"> <li>• <i>id</i>—Test ID .</li> <li>• <i>test-name</i>—Name of the test.</li> </ul> <p>Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs.</p>
<i>disable</i>	Disables diagnostic monitoring for a specified location.

## Command Default

To view the default value for each test, use the **show diagnostic content** command in administration EXEC mode when the diagnostic image is first installed. The default may be different for each test.

## Command Modes

Administration configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic monitor** command to enable or disable health-monitoring diagnostic testing for a specified test at the specified location.

Use the **disable** keyword to disable a health-monitoring diagnostic test that is enabled by default. For example, if test 1 is enabled by default, the **disable** keyword disables the diagnostic test. If the **no** form of the command is used, the test is set to the default condition, which is enabled.



**Task ID**

Task ID	Operations
diag	read, write

**Examples**

The following example shows how to enable health-monitoring diagnostic testing for 0/1/cpu0:

```
RP/0/0/CPU0:router(admin-config)# diagnostic monitor location 0/1/cpu0 test 1
```

**Related Commands**

Command	Description
<a href="#">show diagnostic content, on page 464</a>	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

# diagnostic monitor interval

To configure the health-monitoring diagnostic testing for a specified interval for a specified location, use the **diagnostic monitor interval** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**diagnostic monitor interval location** *node-id* **test** {*id* | *test-name*} *number-of-days* *hour* : *minutes* : *seconds* . *milliseconds*

**no diagnostic monitor interval location** *node-id* **test** {*id* | *test-name*} *number-of-days* *hour* : *minutes* : *seconds* . *milliseconds*

## Syntax Description

<b>location</b> <i>node-id</i>	Specifies a location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b> { <i>id</i>   <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <ul style="list-style-type: none"> <li>• <i>id</i>—Test ID.</li> <li>• <i>test-name</i>—Test name .</li> </ul> <p>Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs.</p>
<i>number-of-days</i> <i>hour:minutes:seconds.milliseconds</i>	Interval between each test run. <p>The <i>number-of-days</i> argument specifies the number of days between testing. The range is from 0 through 20.</p> <p>The <i>hour:minutes:seconds.milliseconds</i> argument specifies the interval, where <i>hour</i> is a number in the range from 0 through 23, <i>minutes</i> is a number in the range from 0 through 59, <i>seconds</i> is a number in the range from 0 through 59, and <i>milliseconds</i> is a number in the range from 0 through 999.</p>

## Command Default

To view the default value for each test, use the **show diagnostic content** command in administration EXEC mode when the diagnostic image is first installed. The default may be different for each test.

## Command Modes

Administration configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.

**Usage Guidelines**

Use the **diagnostic monitor interval** command to set the health-monitoring interval of a specified test at the specified location. The **no** version of the command resets the interval to the default setting. The **diagnostic monitor** command is used to enable health-monitoring.

**Task ID**

Task ID	Operations
diag	read, write

**Examples**

The following example shows how to set the health-monitoring diagnostic testing at an interval of 1 hour, 2 minutes, 3 seconds, and 4 milliseconds for 0/1/cpu0:

```
RP/0/0/CPU0:router(admin-config)# diagnostic monitor interval location 0/1/cpu0 test 1 0  
1:2:3.4
```

**Related Commands**

Command	Description
<a href="#">diagnostic monitor</a> , on page 436	Configures the health-monitoring diagnostic testing for a specified location.
<a href="#">show diagnostic content</a> , on page 464	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

# diagnostic monitor syslog

To enable the generation of a syslog message when any health monitoring test fails, use the **diagnostic monitor syslog** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**diagnostic monitor syslog**

**no diagnostic monitor syslog**

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

**Command Default** Syslog is disabled.

**Command Modes** Administration configuration

Command History	Release	Modification
	Release 3.4.0	This command was introduced.

**Usage Guidelines** Use the **diagnostic monitor syslog** command to enable the generation of a syslog message when a health-monitoring test fails.

Task ID	Task ID	Operations
	diag	read, write

**Examples** The following example shows how to enable the generation of syslog messages:

```
RP/0/0/CPU0:router(admin-config)# diagnostic monitor syslog
```

Related Commands	Command	Description
	<a href="#">show diagnostic content</a> , <a href="#">on page 464</a>	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

# diagnostic monitor threshold

To configure the health-monitoring diagnostic testing failure threshold, use the **diagnostic monitor threshold** command in administration configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**diagnostic monitor threshold location** *node-id* **test** {*id* | *test-name*} **failure count** *failures*

**no diagnostic monitor threshold location** *node-id* **test** {*id* | *test-name*} **failure count** *failures*

## Syntax Description

<b>location</b> <i>node-id</i>	Specifies a location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b> { <i>id</i>   <i>test-name</i> }	Specifies diagnostic test selection. The following test selections are available: <ul style="list-style-type: none"> <li>• <i>id</i>—Test ID.</li> <li>• <i>test-name</i>—Test name .</li> </ul> <p>Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs.</p>
<b>failure count</b> <i>failures</i>	Specifies the number of allowable test failures. Range is 1 to 99.

## Command Default

To view the default value for each test, use the **show diagnostic content** command in administration EXEC mode when the diagnostic image is first installed. The default can be different for each test.

## Command Modes

Administration configuration

## Command History

Release	Modification
Release 3.4.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic monitor threshold** command to specify health-monitoring diagnostic testing failure threshold.

## Task ID

Task ID	Operations
diag	read, write

## Examples

The following example shows how to set the failure threshold to 35 test failures for all tests for 0/1/cpu0:

```
RP/0/0/CPU0:router(admin-config)# diagnostic monitor threshold location 0/1/cpu0 test all  
failure count 35
```

## Related Commands

Command	Description
<a href="#">show diagnostic content</a> , <a href="#">on page 464</a>	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all components.

# diagnostic ondemand action-on-failure

To set when to stop test execution for a **diagnostic start** command, use the **diagnostic ondemand action-on-failure** command in Admin EXEC mode. This command is used in conjunction with the **diagnostic ondemand iteration** command.

**diagnostic ondemand action-on-failure** {**continue** [*failure-count* ]| **stop**}

## Syntax Description

<b>continue</b>	Specifies that test execution continues until all iterations are complete, no matter how many failures are encountered.
<b>failure-count</b>	(Optional) Specifies that test execution continues until the number of failures reaches the specified <i>failure-count</i> . Range is 0 to 65534. A <i>failure-count</i> of 0 indicates to not stop execution until all iterations are complete, no matter how many failures are encountered.
<b>stop</b>	Stops execution immediately when the first test failure occurs.

## Command Default

*failure-count*: 0

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic ondemand action-on-failure** command to specify whether or when to stop test execution if a test fails. This command is used in conjunction with the **diagnostic ondemand iterations** command.

## Task ID

Task ID	Operations
diag	execute

## Examples

The following example shows how to set the test failure action to stop:

```
RP/0/0/CPU0:router(admin)# diagnostic ondemand action-on-failure stop
```

**Related Commands**

Command	Description
<a href="#">diagnostic ondemand iterations, on page 445</a>	Sets the number of times to repeat execution of the diagnostic test.
<a href="#">diagnostic start, on page 448</a>	Runs a specified diagnostic test.



# diagnostic ondemand iterations

To set the number of times to repeat execution of the tests specified by the **diagnostic start** command, use the **diagnostic ondemand iterations** command in Admin EXEC mode.

**diagnostic ondemand iterations** *count*

## Syntax Description

<i>count</i>	Number of times to repeat the specified on-demand tests. Range is 1 to 999.
--------------	---

## Command Default

*count*: 1

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.5.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic ondemand iterations** command to specify the number of times the specified on-demand tests run. The on-demand tests are specified using the **diagnostic start** command.

## Task ID

Task ID	Operations
diag	execute

## Examples

The following example shows how to set the number of iterations to 12:

```
RP/0/0/CPU0:router(admin)# diagnostic ondemand iterations 12
```

## Related Commands

Command	Description
<a href="#">diagnostic ondemand action-on-failure</a> , <a href="#">on page 443</a>	Sets when to stop test execution for a diagnostic test.
<a href="#">diagnostic start</a> , <a href="#">on page 448</a>	Runs a specified diagnostic test.

# diagnostic schedule

To configure a diagnostic schedule, use the **diagnostic schedule** command in Admin Configuration mode. To disable the diagnostic schedule, use the **no** form of this command.

**diagnostic schedule location** *node-id* **test** {*id* | *test-name*} **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-device**} [**device number** | **all**] {**daily** | **on** *month day year* | **weekly** *day-of-week*} *hour:minute*

**no diagnostic schedule location** *node-id* **test** {*id* | *test-name*} **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-device**} [**device number** | **all**] {**daily** | **on** *month day year* | **weekly** *day-of-week*} *hour:minute*

## Syntax Description

<b>location</b> <i>node-id</i>	Schedules a diagnostic test for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b>	Specifies a specific diagnostic test, or all diagnostic tests.
<b>id</b>	Specifies a test ID or list of test IDs. Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs. Multiple tests can be listed if separated by semicolons (;) as follows: <ul style="list-style-type: none"> <li>• <i>x;y-z</i> (for example: 1; 3-4 or 1;3;4)</li> </ul>
<b>test-name</b>	Specifies the name of a test. Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names.
<b>all</b>	Specifies all tests.
<b>basic</b>	Specifies the basic on-demand test suite [Attribute = B].
<b>complete</b>	Specifies the complete bootup test suite [Attribute = C].
<b>minimal</b>	Specifies the minimal bootup test suite [Attribute = M].
<b>non-disruptive</b>	Specifies the non-disruptive test suite [Attribute = N].
<b>per-device</b>	Specifies the per-device test suite [Attribute = V].
<b>device number</b>   <b>all</b>	<p><b>Note</b> This string works only with the <b>all</b>, <b>basic</b>, <b>complete</b>, <b>minimal</b>, <b>non-disruptive</b>, and <b>per-device</b> keywords.</p> <p>(Optional) Specifies the devices on which the diagnostic tests should run. The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>number</i>—Runs tests on one or more devices. The range is 1 through 8. To specify multiple devices, you can use hyphens (-) and semicolons (;); for example, 1; 3-4 or 1;3;4).</li> <li>• <b>all</b>—Runs tests on all devices.</li> </ul>
<b>daily</b>	Specifies a daily schedule.

<b>on</b> <i>month day year</i>	Schedules an exact date.
<b>weekly</b> <i>day-of-week</i>	Specifies a weekly schedule with a set day of the week. Enter the name of a day of the week or a number that specifies a day of the week in the range from 0 through 6.
<i>hour:minute</i>	Scheduled start time, where <i>hour</i> is a number in the range from 0 through 23, and <i>minute</i> is a number in the range from 0 through 59.

**Command Default** No default behavior or values

**Command Modes** Admin Configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.3.0	This command was introduced.

**Usage Guidelines** For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	diag	read, write

**Examples** The following example shows how to schedule all diagnostic tests for location 0/0/CPU0 every day at 12:30 pm:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# configure
RP/0/0/CPU0:router(admin-config)# diagnostic schedule location 0/0/CPU0 test all daily 12:30
```

The following example shows how to schedule all bootup tests for device 1 every Sunday at 12:30 pm:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# configure
RP/0/0/CPU0:router(admin-config)# diagnostic schedule location 0/0/CPU0 test all daily
complete device 1 weekly 12:30
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show diagnostic schedule</a> , <a href="#">on page 471</a>	Displays the current scheduled diagnostic tasks.

# diagnostic start

To run a specified diagnostic test, use the **diagnostic start** command in Admin EXEC mode.

**diagnostic start location** *node-id* **test** {*id* | *test-name*} [**all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-device**] [*device number* | **all**]

## Syntax Description

<b>location</b> <i>node-id</i>	Runs diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b>	Specifies a specific diagnostic test, or all diagnostic tests.
<b>id</b>	Test ID or list of test IDs. Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs. Multiple tests can be listed if separated by semicolons (;) as follows: <ul style="list-style-type: none"> <li>• <i>x;y-z</i> (for example: 1; 3-4 or 1;3;4)</li> </ul>
<b>test-name</b>	Name of the test. Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names.
<b>all</b>	Specifies all tests.
<b>basic</b>	Specifies the basic on-demand test suite [Attribute = B].
<b>complete</b>	Specifies the complete bootup test suite [Attribute = C].
<b>minimal</b>	Specifies the minimal bootup test suite [Attribute = M].
<b>non-disruptive</b>	Specifies the nondisruptive test suite [Attribute = N].
<b>per-device</b>	Specifies the per-device test suite [Attribute = V].
<b>device</b> <i>number</i>   <b>all</b>	<p><b>Note</b> This string works only with the <b>all</b>, <b>basic</b>, <b>complete</b>, <b>minimal</b>, <b>non-disruptive</b>, and <b>per-device</b> keywords.</p> <p>(Optional) Specifies the devices on which the diagnostic tests should start. The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>number</i>—Start tests on one or more devices. The range is 1 through 8. To specify multiple devices, you can use hyphens (-) and semicolons (;); for example, 1; 3-4 or 1;3;4).</li> <li>• <b>all</b>—Starts tests on all devices.</li> </ul>

## Command Default

No default behavior or values

**Command Modes**

Admin EXEC mode

**Command History**

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	The <b>per-device</b> keyword was added.

**Usage Guidelines**

Use the **diagnostic start** command to run a diagnostic test on a specified card.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

**Task ID**

Task ID	Operations
diag	execute

**Examples**

The following example shows how to start a suite of basic diagnostic tests for a specified location:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# diagnostic start location 0/0/CPU0 test basic
```

The following example shows how to start a suite of minimal bootup tests for devices 1 through 7 at the specified location:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# diagnostic start location 0/0/CPU0 test minimal devices 1-7
```

**Related Commands**

Command	Description
<a href="#">diagnostic stop</a> , <a href="#">on page 450</a>	Stops the diagnostic testing in progress on a node.

# diagnostic stop

To stop the diagnostic testing in progress on a node, use the **diagnostic stop** command in Admin EXEC mode.

**diagnostic stop location** *node-id*

## Syntax Description

<b>location</b> <i>node-id</i>	Stops diagnostic testing for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
--------------------------------	--

## Command Default

No default behavior or values

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic stop** command to stop a diagnostic test on a specified node. The command is used for scheduled tests, a test that is causing errors, or a test that does not finish.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

## Task ID

Task ID	Operations
diag	execute

## Task ID

## Examples

The following example shows how to stop the diagnostic test process:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# diagnostic stop location 0/0/CPU0
```

## Related Commands

Command	Description
<a href="#">diagnostic start</a> , <a href="#">on page 448</a>	Runs a specified diagnostic test.

# diagnostic unload

To unload an offline diagnostic image, use the **diagnostic unload** command in Admin EXEC mode.

**diagnostic unload location** *node-id*

## Syntax Description

<b>location</b> <i>node-id</i>	Unloads an offline diagnostic image for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. The diagnostic image is unloaded for all modules in the specified slot.
--------------------------------	---

## Command Default

No default behavior or values

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

Use the **diagnostic unload** command to unload an offline diagnostic image used for integrated field diagnostics. Unloading the image returns the specified card to service.

Use the **show platform** command to determine if the card has been placed back into service.

For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

## Task ID

Task ID	Operations
diag	execute

## Examples

The following example shows how to unload a diagnostic image:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# diagnostic unload location 0/0/CPU0
```

## Related Commands

Command	Description
<a href="#">diagnostic load</a> , on page 434	Loads a diagnostic test.

Command	Description
show platform	Displays information and status of each node in the system.



## ping (administration EXEC)

To send internal echo messages from one node to another, use the **ping** command in administration EXEC mode.

**ping** {**control-eth**|**fabric**} {**fgid** *id*|**location** *node-id*} [**count** *pings*] [**debug**] [**interval** *milliseconds*] [**pattern** **random**] [**queue** *priority*] [**retries** *number*] [**size** *payload\_size*] [**timeout** *seconds*] [**tlate** *seconds*] [**uc**] [**via-egressq**] [**via-fabricq-1**]

### Syntax Description

<b>control-eth</b>	Specifies a control ethernet ping test.
<b>fabric</b>	Specifies a fabric ping test.
<b>fgid</b> <i>id</i>	Specifies that a multicast ping is sent over a fabric to nodes with the fabric group identifier (FGID) of 1024 through 1000000. Nodes that receive the ping respond with a unicast packet.
<b>location</b> <i>node-id</i>	Specifies that a unicast ping is sent a node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>count</b> <i>pings</i>	(Optional) Number of pings to send each time the command is run. The test reports results and statistics after all pings have been sent and received (or timed out). Range is from 0 through 4294967295. The default is 1.
<b>debug</b>	<b>Note</b> This keyword is available only if you specified the <b>fgid</b> keyword. (Optional) Specifies verbose debugging of the multicast ping utility.
<b>interval</b> <i>milliseconds</i>	(Optional) Hold-off time between each ping in milliseconds. Range is from 0 through 4294967295. The total test time is as follows: $(\text{count}-1) * (\text{RTT} + \text{interval}) + \text{RTT}$ RTT = Round Trip Time for the ping.
<b>pattern</b> <b>random</b>	(Optional) Specifies a data pattern for the ping packet payload.
<b>queue</b> <i>priority</i>	<b>Note</b> This keyword is available only if you specified the <b>fgid</b> keyword. (Optional) Specifies the priority of the queue. The priority can be 0 or 1.
<b>retries</b> <i>number</i>	(Optional) Maximum number of times a failed ping transmission is sent before the packet transmission is considered a failure. Range is from 0 through 4294967295. <b>Note</b> Packet transmission failure is usually an indication of a server software transient. In this case, we recommend that you run the <b>ping</b> command again.
<b>size</b> <i>payload_size</i>	(Optional) Specifies the payload size for each ping packet size. Range is from 0 through 4294967295 bytes. The maximum payload size allowed may be limited, depending on the transport type that is used (fabric or control-ethernet).

<b>timeout</b> <i>seconds</i>	<p>(Optional) Specifies the maximum time to wait for response to a ping. Range is from 0 through 4294967295 seconds.</p> <p>If a ping does not receive a response before the configured timeout expires, the ping statistics reflect it as a discrepancy between the “Sent:” and “Rec'd:” packet count, and the test is considered failed. Because of this, we recommend that you do not set the timeout to 0.</p>
<b>tlate</b> <i>seconds</i>	<p><b>Note</b> This keyword is available only if you specified the <b>fgid</b> keyword.</p> <p>(Optional) Specifies the amount of time to wait for a response to a multicast ping. The amount of time you specify must be less than the value of the <b>timeout</b> keyword. Range is from 0 through 4294967295 seconds.</p>
<b>uc</b>	<p><b>Note</b> This keyword is available only if you specified the <b>fgid</b> keyword.</p> <p>(Optional) Specifies that unicast pings (instead of multicast pings) are sent to nodes with the specified FGID.</p>
<b>via-egressq</b>	<p>(Optional) Specifies that a unicast or multicast ping packet is routed to the first fabricq ASIC (instance 0); then, to the egressq ASIC, and finally to the destination CPU.</p> <p>By default, a unicast ping is routed to the first fabricq ASIC (instance 0), then to the destination CPU. A multicast ping is routed to the constituent fabricq ASIC instances, then to the destination CPU.</p>
<b>via-fabricq-1</b>	<p><b>Note</b> This keyword is available if you specified the <b>location</b> keyword, or both the <b>fgid</b> and <b>uc</b> keywords.</p> <p>(Optional) Specifies that a unicast ping is routed to the current fabricq ASIC (instance 1), then to the egressq ASIC, and finally, to the destination CPU.</p> <p>By default, a unicast ping is routed to the first fabricq ASIC (instance 0), then to the destination CPU.</p>

**Command Default** No default behavior or values

**Command Modes** Administration EXEC

#### Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The <b>fgid</b> keyword was added.
Release 3.8.0	The <b>via-egressq</b> and <b>via-fabricq-1</b> keywords were added.

**Usage Guidelines**

When you enter the **ping** command, a ping is sent to the node at the specified location or to nodes with the specified FGID. The received response is compared byte-by-byte to the sent packet. If a ping response is not received before the specified time-out, or if the ping response does not match the transmitted ping, the ping is considered failed.

A node that is unreachable or intermittently working impacts the total run time for the test as follows:

```
(received_packet_count * RTT + lost_packet_count * timeout + (count-1) * interval)
```

Line cards have two fabricq ASICs and an egressq ASIC. From the first fabricq ASIC (instance 0), the CPU can be reached directly or via the egressq ASIC. From the second fabricq ASIC (instance 1), the CPU can be reached only via the egressq ASIC. In other words, no direct packet path exists between instance 1 and the CPU.

The route processor (RP) and distributed route processor (DRP) cards have only one fabricq ASIC per node (CPU) and no egressq ASIC. Therefore, a fabric ping on an RP or DRP destination specified with the **via-egressq** or **via-fabricq-1** keyword fails.

**Task ID**

Task ID	Operations
diag	execute

**Examples**

The following example shows sample output from a control-ethernet ping to an SP node in slot 0/0:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping control-eth location 0/0/SP count 5

Src node:      529 : 0/RP0/CPU0
Dest node:      0 : 0/0/SP
Local node:    529 : 0/RP0/CPU0
Packet cnt:     5  Packet size: 128  Payload ptn type: default (0)
Hold-off (ms): 300 Time-out(s): 2    Max retries: 5
Destination node has MAC addr 5246.4800.0000

Running CE node ping.
Please wait...
Src: 529:, Dest: 0, Sent: 5, Rec'd: 5, Mismatched: 0
Min/Avg/Max RTT: 0/200/1000
CE node ping succeeded for node: 0
```

The following example shows a fabric ping from the active RP to the active RP. In this example, the ping contains 72 packets of 1 kilobyte each. This command performs a good coverage test of the entire switch fabric:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping fabric location 0/RP0/CPU0 count 72 size 1024

Src node:      529 : 0/RP0/CPU0
Dest node:      529 : 0/RP0/CPU0
Local node:    529 : 0/RP0/CPU0
Packet cnt:     72  Packet size: 1024  Payload ptn type: default (0)
Hold-off (ms): 300 Time-out(s): 2    Max retries: 5

Running Fabric node ping.
Please wait...
```

```

Src: 529:, Dest: 529, Sent: 72, Rec'd: 72, Mismatched: 0
Min/Avg/Max RTT: 3000/3013/4000
Fabric node ping succeeded for node: 529

```

The following example shows a ping to a control Ethernet node that has a problem or does not exist:

```

RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping control-eth location 0/1/CPU0 count 3

Src node:      529 : 0/RP0/CPU0
Dest node:     17 : 0/1/CPU0
Local node:    529 : 0/RP0/CPU0
Packet cnt:    3   Packet size: 128   Payload ptn type: default (0)
Hold-off (ms): 300   Time-out(s): 2   Max retries: 5
Destination node has MAC addr 5246.4800.0011

Running CE node ping.
Please wait...
Src: 529:, Dest: 17, Sent: 3, Rec'd: 0, Mismatched: 0
Requested ping failed for node: 17

```

The following example shows how to send a multicast fabric ping to nodes with the FGID of 1024. The node that sent the multicast ping waits 1 second for a response from each node.

```

RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping fabric fgid 1024 tlate 1

Src node:      513 : 0/RP0/CPU0
fgid:          1024
Local node:    513 : 0/RP0/CPU0
Packet cnt:    1   Packet size: 128   Payload ptn type: default (0)
Hold-off (ms): 1   Time-out(s): 2   Max retries: 5
DelayTimeout: 1   Priority: High
Running Fabric node ping.
Please wait...

```

Multicast (Pinging fgid) ...

Node	Sent	Rcv.	Late	Lost
0/1/CPU0 (0x11:17)	1	1	0	0
0/4/CPU0 (0x41:65)	1	1	0	0
0/4/CPU1 (0x42:66)	1	1	0	0
0/6/CPU0 (0x61:97)	1	1	0	0
0/RP0/CPU0 (0x201:513)	1	1	0	0
0/RP1/CPU0 (0x211:529)	1	1	0	0

diag\_ping: All 6 nodes responded to all 1 pings

The following example shows how to send a multicast fabric ping to nodes with the FGID of 1024. The ping packets are routed from the first fabricq ASIC (instance 0) to the destination CPU via the egressq ASIC. The pings to the two line cards (0/1/CPU0 and 0/6/CPU0) succeeded, while the pings to the RPs (0/RP0/CPU0 and 0/RP1/CPU0) and DRPs (0/4/CPU0 and 0/4/CPU1) failed because they do not have an egressq ASIC.

```

RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping fabric fgid 1024 count 10 via-egressq

Src node:      513 : 0/RP0/CPU0
fgid:          1024
Local node:    513 : 0/RP0/CPU0
Packet cnt:    10   Packet size: 128   Payload ptn type: default (0)
Hold-off (ms): 1   Time-out(s): 2   Max retries: 5
DelayTimeout: 1   Priority: High
Reaching destination CPUs via egressq

Running Fabric node ping.
Please wait...

Multicast (Pinging fgid) ...

```

Node	Sent	Rcv.	Late	Lost
0/1/CPU0 (0x11:17)	10	10	0	0
0/4/CPU0 (0x41:65)	10	0	0	10
0/4/CPU1 (0x42:66)	10	0	0	10
0/6/CPU0 (0x61:97)	10	10	0	0
0/RP0/CPU0 (0x201:513)	10	0	0	10
0/RP1/CPU0 (0x211:529)	10	0	0	10

diag\_ping: Out of 6 node(s), 2 node(s) responded to all 10 pings, 4 node(s) hads

The following example shows how to send a unicast ping to nodes with the FGID of 1024. The ping packets are routed from the second fabricq ASIC (instance 1) to the destination CPU via the egressq ASIC. The pings to the two line cards (0/1/CPU0 and 0/6/CPU0) succeeded, while the pings to the RPs (0/RP0/CPU0 and 0/RP1/CPU0) and DRPs (0/4/CPU0 and 0/4/CPU1) failed because they do not have a second fabricq ASIC nor an egressq ASIC.

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# ping fabric fgid 1024 count 10 uc via-fabricq-1
```

```
Src node:      513 : 0/RP0/CPU0
fgid:          1024
Local node:    513 : 0/RP0/CPU0
Packet cnt:    10  Packet size: 128  Payload ptn type: default (0)
Hold-off (ms): 1   Time-out(s): 2   Max retries: 5
DelayTimeout: 1   Priority:      High
Using other fabricq instance
```

```
Running Fabric node ping.
Please wait...
```

```
Multicast (Pinging Individual Sponge Ids) ...
```

Node	Sent	Rcv.	Late	Lost
0/1/CPU0 (0x11:17)	10	10	0	0
0/4/CPU0 (0x41:65)	10	0	0	10
0/4/CPU1 (0x42:66)	10	0	0	10
0/6/CPU0 (0x61:97)	10	10	0	0
0/RP0/CPU0 (0x201:513)	10	0	0	10
0/RP1/CPU0 (0x211:529)	10	0	0	10

diag\_ping: Out of 6 node(s), 2 node(s) responded to all 10 pings, 4 node(s) hads

# show diag

To display details about the hardware and software on each node in a router, use the **show diag** command in the appropriate mode.

**show diag** [ *node-id* ] [ **chassis-info** | **details** | **summary** ]

## Syntax Description

details	(Optional) Displays detailed hardware and diagnostics information. <b>Note</b> Specifying the <b>details</b> keyword displays EEPROM information for the chassis or specified node.
summary	(Optional) Displays a summary of the installed hardware.
node-id	(Optional) Identifies the node for which you want to display information. The <i>node-id</i> argument is expressed in the <i>rack/slot/module</i> notation.
chassis-info	(Optional) Displays information about the chassis.

## Command Default

Hardware and software information for all nodes installed in the router is displayed

## Command Modes

EXEC  
Administration EXEC

## Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.3.0	The <b>chassis-info</b> keyword was introduced.

## Usage Guidelines

The **show diag** command displays detailed information on the hardware components for each node, and on the status of the software running on each node.

## Task ID

Task ID	Operations
sysmgr	read

## Examples

```
RP/0/5/CPU0:router# show diag details
```

```

SLOT 0 (RP/LC 0): Cisco 12000 Series - Multi-Service Blade
MAIN: type 150, 800-25972-02 rev A0 dev 0
HW config: 0x00 SW key: 00-00-00
PCA: 73-9289-04 rev A0 ver 3
HW version 1.0 S/N SAD11360218
MBUS: Embedded Agent
Test hist: 0x00 RMA#: 00-00-00 RMA hist: 0x00
DIAG: Test count: 0x00000000 Test results: 0x00000000
EEPROM contents (hex):
Release Modification
Release 3.3.0 The chassis-info keyword was added to the show diags command on the
Cisco XR 12000 Series Router.
Task ID Operations
sysmgr read
00: 01 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00
10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
40: 00 96 01 00 00 49 00 24 49 04 50 03 FE 01 00 03
50: 03 20 00 65 74 02 50 00 00 00 00 00 0A 01 00 00
60: 53 41 44 31 31 33 36 30 32 31 38 00 00 00 00 00
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 DA 00 00
C0: 58 52 2D 31 32 4B 2D 4D 53 42 00 00 00 00 00 00
D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E0: 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FRU: Linecard/Module: 12000-ServEngCard
L3 Engine: Service Engine - ISE OC192 (10 Gbps)
MBUS Agent Software version 4.4 (RAM) (ROM version is 4.4)
Using CAN Bus A
ROM Monitor version 1.3
Fabric Downloader version used 3.2 (ROM version is 3.2)
Primary clock is CSC0
Board State is IOS-XR RUN
Last Reset Reason: Card graceful reboot
Insertion time: Fri Oct 10 22:34:58 2008 (4w2d ago)
DRAM size: 2147483648 bytes
FrFab SDRAM size: 1610612736 bytes
ToFab SDRAM size: 268435456 bytes
0 resets since restart/fault forgive
...
SLOT 2 (RP/LC 2): Cisco 12000 Series SPA Interface Processor- 601
MAIN: type 149, 68-2647-01 rev A0 dev 85437
HW config: 0x20 SW key: 00-00-00
PCA: 73-9607-04 rev A0 ver 4
HW version 1.0 S/N SAD10330441
MBUS: Embedded Agent
Test hist: 0x00 RMA#: 00-00-00 RMA hist: 0x00
DIAG: Test count: 0x00000000 Test results: 0x00000000
EEPROM contents (hex):
00: 01 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00
10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
40: 00 95 01 00 00 49 00 25 87 04 50 04 FE 01 00 00
50: 00 44 00 0A 57 01 50 01 4D BD 20 09 01 00 00 00
60: 53 41 44 31 30 33 33 30 34 34 31 00 00 00 00 00
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A0: 00 01 40 98 00 00 00 00 00 00 00 00 00 00 00 00
B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 DA 00 00
C0: 31 32 30 30 30 2D 53 49 50 2D 36 30 31 00 00 00
D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
F0: B8 07 A4 1F 8A 52 6D 1F 9A CE AE CF BF F4 00 00
FRU: Linecard/Module: 12000-SIP-601
Route Memory: MEM-LC5-2048=
Packet Memory: MEM-LC5-PKT-512=

```

```

L3 Engine: 5 (MultiRate) - ISE OC192 (10 Gbps)
Operational rate mode: 10 Gbps
MBUS Agent Software version 4.4 (RAM) (ROM version is 4.2)
Using CAN Bus A
ROM Monitor version 17.1
Fabric Downloader version used 4.7 (ROM version is 4.7)
Primary clock is CSC0
Board State is IOS-XR RUN
Last Reset Reason: Reload initiated by user
Insertion time: Wed Nov 5 17:39:51 2008 (5d01h ago)
DRAM size: 2147483648 bytes
FrFab SDRAM size: 268435456 bytes
ToFab SDRAM size: 268435456 bytes
0 resets since restart/fault forgive
SPA Information:
subslot 0/2/0: SPA-4XOC3-POS-V2 (0x526), status is ok
subslot 0/2/1: SPA-IPSEC-2G-2 (0x549), status is ok
subslot 0/2/2: SPA-8X1FE (0x4c5), status is ok
subslot 0/2/3: Empty
...
SLOT 5 (RP/LC 5): Cisco 12000 Series Performance Route Processor 2
MAIN: type 96, 800-23469-06 rev A0 dev 84610
HW config: 0x10 SW key: 00-00-00
PCA: 73-8812-09 rev A0 ver 7
HW version 0.0 S/N SAD103003M7
MBUS: MBUS Agent (1) 73-8048-07 rev A0 dev 0
HW version 0.1 S/N SAL1026THV9
Test hist: 0x00 RMA#: 00-00-00 RMA hist: 0x00
DIAG: Test count: 0x00000000 Test results: 0x00000000
EEPROM contents (hex):
00: 01 00 01 00 49 00 1F 70 07 50 00 00 00 00 00 00
10: 53 41 4C 31 30 32 36 54 48 56 39 00 00 00 00 00
20: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
40: 00 60 00 00 00 49 00 22 6C 09 50 07 00 02 00 00
50: 03 20 00 5B AD 06 50 01 4A 82 10 00 01 00 00 00
60: 53 41 44 31 30 33 30 30 33 4D 37 00 00 00 00 00
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 32 DA 00 00
C0: 50 52 50 2D 32 00 00 00 00 00 00 00 00 00 00 00
D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E0: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FRU: Linecard/Module: PRP-2
Route Memory: MEM-PRP/LC-2048=
MBUS Agent Software version 4.4 (RAM) (ROM version is 4.2)
Using CAN Bus A
ROM Monitor version 1.16dev(0.1)
Primary clock is CSC0
Board State is IOS-XR RUN
Insertion time: Fri Oct 10 21:19:10 2008 (4w2d ago)
DRAM size: 2147483648 bytes
0 resets since restart/fault forgive

```

The output displayed for the **show diag details** command is the most comprehensive output displayed for **show diag** command variations. All other variations show a subset of the fields displayed except for the **show diag details chassis-info** and **show diag summary chassis-info** commands, which show different information.

**Table 41: show diags Field Descriptions**

Field	Description
SLOT	Physical slot number of the line card.
MAIN	General information about the hardware.



Field	Description
PCA	Cisco Protection Channel Access (PCA) hardware and revision number.
MBUS	Provides version information for the Mbus agent.
DIAG	Results of the last diagnostics test, in hexadecimal format.
EEPROM contents	EEPROM contents, in hexadecimal, of the component.
FRU	Information about the Field-replaceable Units (FRUs) associated with the nodes that are installed in the router.
MBUS Agent Software version	Mbus agent software version currently running on the router.
ROM Monitor version	Version of monitor library used by ROMMON.
Fabric Downloader version	Version of fabric downloader used.
Primary clock	Primary clock source configured on the router.
Board State	Current software on the board, and whether or not the board is running.
Last Reset Reason	Reason the card was last reset.
Insertion time	Time at which the last diagnostics test was executed.
DRAM size	Dynamic Random-Access Memory (DRAM) size in bytes.
<i>number</i> resets since restart/fault forgive	Number of resets since the card was last restarted.
SPA Information	Subslot in which SPA is installed, name of SPA, and current status of SPA.

The following example shows how to display detailed information for a chassis:

```
RP/0/5/CPU0:router# show diag details chassis-info

Backplane NVRAM [version 0x20] Contents -
  Chassis: type 12406 Fab Ver: 2
    Chassis S/N: TBM10421465
  PCA: 73-5796-2 rev: C0 dev: 0 HW ver: 1.0
    Backplane S/N: TBM10402356
  MAC Addr: base 0019.aaa3.3a00 block size: 1024
  RMA Number: 0x00-0x00-0x00 code: 0x00 hist: 0x00
```

```

Backplane NVRAM (hex)
00: 20 00 00 49 16 a4 00 02 00 60 00 02 01 00 00 07
10: 54 42 4d 31 30 34 30 32 33 35 36 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
30: 54 42 4d 31 30 34 32 31 34 36 35 00 00 00 00 00
40: 00 19 aa a3 3a 00 04 00 00 00 00 00 00 00 00 00
50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

**Table 42: show diags details chassis-info Field Descriptions**

Field	Description
Chassis	Type and fabrication version of the chassis.
Chassis S/N	Serial number of the chassis.
PCA	Cisco Protection Channel Access (PCA) hardware and revision number.
Backplane S/N	Serial number of the backplane.
MAC Addr	MAC address and block size of the chassis.
RMA Number	RMA information for the chassis.
Backplane NVRAM	Contents of the backplane NVRAM, in hexadecimal.

**Related Commands**

Command	Description
show platform	Displays information and status for each node in the system.
show version	Displays details on the hardware and software status of the system.

# show diagnostic bootup level

To display the current diagnostic bootup level, use the **show diagnostic bootup level** command in Admin EXEC mode.

**show diagnostic bootup level location** *node-id*

## Syntax Description

<b>location</b> <i>node-id</i>	Specifies a card. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
--------------------------------	---

## Command Default

No default behavior or values.

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.4.0	This command was introduced.

## Usage Guidelines

Use the **show diagnostic bootup level** command to display the current diagnostic bootup level for a specified card.

## Task ID

Task ID	Operations
diag	read

## Examples

The following example shows how to display the current diagnostic bootup level for 0/1/cpu0:

```
RP/0/0/CPU0:router(admin)# show diagnostic bootup level location 0/1/cpu0
Current bootup diagnostic level for LC 0/1/CPU0: minimal
```

# show diagnostic content

To display test information including test ID, test attributes, and supported coverage test levels for each test and for all components, use the **show diagnostic content** command in Admin EXEC mode.

**show diagnostic content location** *node-id*

Syntax Description	location <i>node-id</i>	Displays the diagnostic content for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
--------------------	-------------------------	---

Command Default	No default behavior or values
-----------------	-------------------------------

Command Modes	Admin EXEC mode
---------------	-----------------

Command History	Release	Modification
	Release 3.3.0	This command was introduced.

Usage Guidelines	Use the <b>show diagnostic content</b> command to display diagnostic test information for a specific location. The test information includes the supported tests and attributes.  For more information about running Cisco IOS XR diagnostics, refer to <i>Cisco IOS XR Diagnostics</i> .
------------------	---

Task ID	Task ID	Operations
	diag	read

Examples	The following example shows how to display the test information for a specified location:  For a route processor:
----------	---

```
RP/0/0/CPU0:router(admin): show diagnostic content
location 0/0/cpu0
```

```
Diagnostics test suite attributes:
  M/C/* - Minimal bootup level test / Complete bootup level test / NA
  B/*   - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
```

S/\* - Only applicable to standby unit / NA  
 X/\* - Not a health monitoring test / NA  
 F/\* - Fixed monitoring interval test / NA  
 E/\* - Always enabled monitoring test / NA  
 A/I - Monitoring is active / Monitoring is inactive

ID	Test Name	Attributes	Test Interval (day hh:mm:ss.ms)	Thre- shold
1)	ControlEthernetPingTest	*B*N*X**I	001 00:00:00.000	1
2)	SelfPingOverFabric	*B*N*X**I	001 00:00:00.000	1
3)	FabricPingTest	*B*N*X**I	001 00:00:00.000	1
4)	ControlEthernetInactiveLinkTest	*B*NS**I	001 00:00:00.000	1
5)	RommonRevision	*B*N*X**I	001 00:00:00.000	1
6)	FabricDiagnosisTest	*B*NS**I	000 00:02:00.000	1
7)	FilesystemBasicDisk0	*B*N****I	003 00:00:00.000	1
8)	FilesystemBasicDisk1	*B*N****I	003 00:00:00.000	1
9)	FilesystemBasicHarddisk	*B*N****I	003 00:00:00.000	1
10)	ScratchRegisterTest	CBVN****I	001 00:00:00.000	1
11)	FabricMcastTest	*B*NS**I	000 00:02:00.000	1
12)	ControlEthernetIntraSwitchTest	*B*N****I	000 00:00:02.000	3
13)	FabricUcastMcastTest	*B*N****A	000 00:01:00.000	1

RP/0/0/CPU0:router(admin)# **show diagnostic content location 0/1/cpu0**

Wed Feb 16 09:27:01.424 PST

MSC 0/1/CPU0:

Diagnostics test suite attributes:  
 M/C/\* - Minimal bootup level test / Complete bootup level test / NA  
 B/\* - Basic ondemand test / NA  
 P/V/\* - Per port test / Per device test / NA  
 D/N/\* - Disruptive test / Non-disruptive test / NA  
 S/\* - Only applicable to standby unit / NA  
 X/\* - Not a health monitoring test / NA  
 F/\* - Fixed monitoring interval test / NA  
 E/\* - Always enabled monitoring test / NA  
 A/I - Monitoring is active / Monitoring is inactive

ID	Test Name	Attributes	Test Interval (day hh:mm:ss.ms)	Thre- shold
1)	ControlEthernetPingTest	*B*N*X**I	001 00:00:00.000	1
2)	SelfPingOverFabric	*B*N*X**I	001 00:00:00.000	1
3)	RommonRevision	*B*N*X**I	001 00:00:00.000	1
4)	ScratchRegisterTest	CBVN****I	001 00:00:00.000	1
5)	TcamFullScanTest	*BVN****I	001 00:00:00.000	1
6)	EgressqMemoryBISTTest	**VD*X**I	001 00:00:00.000	1
7)	IngressqMemoryBISTTest	**VD*X**I	001 00:00:00.000	1
8)	FabricqMemoryBISTTest	**VD*X**I	001 00:00:00.000	1

Table 43: show diagnostic content Field Descriptions, on page 465 describes the significant fields shown in the display.

**Table 43: show diagnostic content Field Descriptions**

Field	Description
M/C/* - Minimal bootup level test / Complete bootup level test / NA	Minimal bootup test or complete bootup test.
B/* - Basic ondemand test / NA	Basic on-demand test.

Field	Description
P/V/* - Per port test / Per device test / NA	Test is per port or device.
D/N/* - Disruptive test / Non-disruptive test / NA	Test is disruptive or nondisruptive.
S/* - Only applicable to standby unit / NA	Test is available for standby node only.
X/* - Not a health monitoring test / NA	Test is not a health-monitoring test.
F/* - Fixed monitoring interval test / NA	Test is a fixed monitoring interval test.
E/* - Always enabled monitoring test / NA	Test is an always enabled monitoring test.
A/I - Monitoring is active / Monitoring is inactive	Test is active or inactive.
ID	ID of the test.
Test Name	Name of the test.
Attributes	Attributes for the test.
Test Interval	Interval of the test.
Threshold	Failure threshold of the text.

**Related Commands**

Command	Description
<a href="#">diagnostic load, on page 434</a>	Loads an offline diagnostic image for integrated field diagnostics.
<a href="#">diagnostic monitor interval, on page 438</a>	Configures the health-monitoring diagnostic testing for a specified interval for a specified location.
<a href="#">diagnostic schedule, on page 446</a>	Configures a diagnostic schedule.
<a href="#">diagnostic start, on page 448</a>	Runs a specified diagnostic test.
<a href="#">diagnostic unload, on page 451</a>	Unloads an offline diagnostic image.

# show diagnostic ondemand settings

To display the current on-demand settings, use the **show diagnostic ondemand settings** command in Admin EXEC mode .

**show diagnostic ondemand settings**

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

**Command Default** No default behavior or values

**Command Modes** Admin EXEC mode

Command History	Release	Modification
	Release 3.5.0	This command was introduced.

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

Task ID	Task ID	Operations
	diag	read

**Examples** The following example shows how to display the on-demand settings:

```
RP/0/0/CPU0:router(admin)# show diagnostic ondemand settings

Test iterations = 45
Action on test failure = continue until test failure limit reaches 25
```

# show diagnostic result

To display diagnostic test results, use the **show diagnostic result** command in Admin EXEC mode.

**show diagnostic result location** *node-id*[**test** {*id* | *test-name* | **all**}] [**detail**]

Syntax Description

<b>location</b> <i>node-id</i>	Displays the diagnostic test results for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>test</b> { <i>id</i>   <i>test-name</i>   <b>all</b> }	(Optional) Specifies diagnostic test selection. The following test selections are available: <ul style="list-style-type: none"><li>• <i>id</i>—Test ID or list of test IDs . Multiple tests can be listed if separated by semicolons (;) as follows:<ul style="list-style-type: none"><li>◦ x;y-z (for example: 1; 3-4 or 1;3;4)</li></ul></li><li>• <i>test-name</i>—Test name.</li><li>• <b>all</b>—Specifies all tests.</li></ul> <p>Use the <b>show diagnostic content</b> command in administration EXEC mode to see a list of test names and their associated IDs.</p>
<b>detail</b>	(Optional) Specifies detailed results.

Command Default

No default behavior or values

Command Modes

Admin EXEC mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

Use the **show diagnostic result** command to display diagnostic results for a specific location. For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

Task ID

Task ID	Operations
diag	read



## Examples

The following example shows how to display detailed diagnostic test results:

```
RP/0/0/CPU0:router(admin)# show diagnostic result location 0/3/CPU0 test 1 detail
```

Test results: (. = Pass, F = Fail, U = Untested)

```
1 ) Control Ethernet Ping Test -----> .
Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 1
Last test execution time ----> Thu Aug 11 18:13:38.918 2005
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> Thu Aug 11 18:13:38.918 2005
Total failure count -----> 0
Consecutive failure count ---> 0
```

**Table 44: show diagnostic result Field Descriptions**

Field	Description
Test results :	Test result options: <ul style="list-style-type: none"> <li>• .—Pass</li> <li>• F—Fail</li> <li>• U—Untested</li> </ul>
Error code	Code for the error. DIAG_SUCCESS is indicated if there were no code errors. DIAG_FAILURE is indicated for any failure. DIAG_SKIPPED is indicated if the test was stopped.
Total run count	Number of times the test has run.
Last test execution time	Last time the test was run.
First test failure time	First time the test failed.
Last test failure time	Last time the test failed.
Last test pass time	Last time the test passed.
Total failure count	Number of times the test has failed.
Consecutive failure count	Number of consecutive times the test has failed.

**Related Commands**

Command	Description
<a href="#">diagnostic load, on page 434</a>	Loads an offline diagnostic image for integrated field diagnostics.
<a href="#">diagnostic schedule, on page 446</a>	Configures a diagnostic schedule.
<a href="#">diagnostic start, on page 448</a>	Runs a specified diagnostic test.

# show diagnostic schedule

To display the current scheduled diagnostic tasks, use the **show diagnostic schedule** command in Admin EXEC mode.

**show diagnostic schedule location** *node-id*

## Syntax Description

<b>location</b> <i>node-id</i>	Displays the diagnostic schedule for a specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
--------------------------------	--

## Command Default

No default behavior or values

## Command Modes

Admin EXEC mode

## Command History

Release	Modification
Release 3.3.0	This command was introduced.

## Usage Guidelines

Use the **show diagnostic schedule** command to display scheduled diagnostic tasks for a specific location. For more information about running Cisco IOS XR diagnostics, refer to *Cisco IOS XR Diagnostics*.

## Task ID

Task ID	Operations
diag	read

## Examples

The following example shows how to display scheduled diagnostic tasks:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# show diagnostic schedule location 0/3/CPU0

Current Time = Tue Sep 27 12:41:24 2005
Diagnostic for LC 0/3/CPU0:

Schedule #1:
  To be run daily 14:40
  Test ID(s) to be executed: 1 .
```

**Table 45: show diagnostic schedule Field Descriptions**

Field	Description
Current Time	Current system time.
Diagnostic for	Card for which the diagnostic is scheduled.
Schedule	Schedule number.
To be run	Time at which the diagnostics are scheduled to run.
Test ID(s) to be executed	Tests to be run at scheduled time.

**Related Commands**

Command	Description
<a href="#">diagnostic schedule</a> , on page 446	Configures a diagnostic schedule.

# show diagnostic status

To display the current running tests, use the **show diagnostic status** command in Admin EXEC mode.

**show diagnostic status**

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

**Command Default** No default behavior or values

**Command Modes** Admin EXEC mode

Release	Modification
Release 3.5.0	This command was introduced.

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

Task ID	Task ID	Operations
	diag	read

# show run diagnostic monitor

To display the card type of a line card or a Shared Port Adapter (SPA), use the **show run diagnostic monitor** command in the Admin Configuration mode.

**show run diagnostic monitor**

## Syntax Description

This command has no keywords or arguments.

## Command Default

No default behavior or values

## Command Modes

Admin Configuration mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

You need to be aware of the card type when you configure a slot or swap a card, and the configuration must re-apply. If the card type is different, the configuration does not re-apply. You can display the card type using the **show run diagnostic monitor** command in the administration configuration mode.

## Task ID

Task ID	Operations
diag	read, write

## Examples

```
RP/0/0/CPU0:router#admin
RP/0/0/CPU0:router(admin)# config
RP/0/0/CPU0:router(admin-config)# diagnostic monitor location 0/RP1/CPU0 test
FabricDiagnosisTest
RP/0/0/CPU0:router(admin-config)# commit
RP/0/0/CPU0:router(admin-config)# end
RP/0/0/CPU0:router(admin)# show run diagnostic monitor

diagnostic monitor location 0/RP1/CPU0 test FabricDiagnosisTest card-type 100006
```



## INDEX

### A

access-list command [117](#)  
action (IP SLA) command [119](#)  
ageout command [121](#)  
alarm command [3](#)  
all-alarms command [4](#)  
all-of-router command [5](#)  
archive-length command [311](#)  
archive-size command [312](#)

### B

buckets (history) command [123](#)  
buckets (statistics hourly) command [125](#)  
buckets (statistics interval) command [127](#)

### C

clear counters command [430](#)  
clear logging command [313](#)  
clear logging correlator delete command [6](#)  
clear logging events delete command [7](#)  
clear logging events reset command [11](#)  
clear logging onboard command [369](#)  
context-correlation command [13](#)  
control disable command [128](#)

### D

datasize request command [130](#)  
destination address (IP SLA) command [132](#)  
destination port command [134](#)  
device command [315](#)  
diagnostic load command [434](#)  
diagnostic monitor command [436](#)  
diagnostic monitor interval command [438](#)  
diagnostic monitor syslog command [440](#)

diagnostic monitor threshold command [441](#)  
diagnostic ondemand action-on-failure command [443](#)  
diagnostic ondemand iterations command [445](#)  
diagnostic schedule command [446](#)  
diagnostic start command [448](#)  
diagnostic stop command [450](#)  
diagnostic unload command [451](#)  
distribution count command [136](#)  
distribution interval command [138](#)

### E

event manager directory user command [79](#)  
event manager environment command [81](#)  
event manager policy command [83](#)  
event manager refresh-time command [87](#)  
event manager run command [88](#)  
event manager scheduler suspend command [90](#)  
exp command [140](#)

### F

file-size command [316](#)  
filter command [142](#)  
force explicit-null command [144](#)  
frequency (IP SLA) command [146](#)  
frequency (logging) command [317](#)

### H

history command [148](#)  
hw-module logging onboard command [371](#)

### I

interval command [150](#)  
ipsla command [152](#)

**K**

key-chain command [154](#)

**L**

life command [156](#)  
 lives command [158](#)  
 load-interval command [432](#)  
 logging archive command [320](#)  
 logging buffered command [322](#)  
 logging command [318](#)  
 logging console command [324](#)  
 logging console disable command [326](#)  
 logging correlator apply rule command [15](#)  
 logging correlator apply ruleset command [18](#)  
 logging correlator buffer-size command [20](#)  
 logging correlator rule command [22](#)  
 logging correlator ruleset command [25](#)  
 logging events buffer-size command [27](#)  
 logging events display-location command [29](#)  
 logging events level command [31](#)  
 logging events link-status (interface) command [329](#)  
 logging events link-status command [327](#)  
 logging events threshold command [33](#)  
 logging facility command [332](#)  
 logging history command [335](#)  
 logging history size command [337](#)  
 logging hostnameprefix command [339](#)  
 logging localfilesize command [344](#)  
 logging monitor command [345](#)  
 logging source-interface [341](#)  
 logging source-interface command [347](#)  
 logging suppress apply rule command [35](#)  
 logging suppress deprecated command [349](#)  
 logging suppress duplicates command [350](#)  
 logging suppress rule command [37](#)  
 logging trap command [352](#)  
 low-memory command [160](#)  
 lsp selector ipv4 command [162](#)  
 lsr-path command [164](#)

**M**

maximum hops command [166](#)  
 maximum paths (IP SLA) command [168](#)  
 monitor command [170](#)  
 monitor controller fabric command [377](#)  
 monitor controller sonet command [379](#)  
 monitor interface command [381](#)  
 mpls discovery vpn command [172](#)

mpls lsp-monitor command [174](#)

**N**

nonrootcause command [39](#)

**O**

operation command [176](#)  
 output interface command [177](#)  
 output nexthop command [179](#)

**P**

packet count command [181](#)  
 packet interval command [183](#)  
 path discover command [185](#)  
 path discover echo command [186](#)  
 path discover path command [188](#)  
 path discover scan command [190](#)  
 path discover session command [192](#)  
 performance-mgmt apply monitor command [386](#)  
 performance-mgmt apply statistics command [389](#)  
 performance-mgmt apply thresholds command [392](#)  
 performance-mgmt regular-expression command [395](#)  
 performance-mgmt resources dump local command [396](#)  
 performance-mgmt resources memory command [397](#)  
 performance-mgmt resources tftp-server command [399](#)  
 performance-mgmt statistics command [401](#)  
 performance-mgmt thresholds command [404](#)  
 ping (administration EXEC) command [453](#)

**R**

react command [194](#)  
 react lpd command [197](#)  
 reaction monitor command [199](#)  
 reaction operation command [201](#)  
 reaction trigger command [203](#)  
 recurring command [206](#)  
 reissue-nonbistate command [41](#)  
 reparent command [43](#)  
 reply dscp command [207](#)  
 reply mode command [209](#)  
 responder command [205](#)  
 rootcause command [45](#)



## S

scan delete-factor command [212](#)  
 scan interval command [214](#)  
 schedule monitor command [216](#)  
 schedule operation command [218](#)  
 schedule period command [220](#)  
 service timestamps command [354](#)  
 severity command [356](#)  
 show diag command [458](#)  
 show diagnostic bootup level command [463](#)  
 show diagnostic content command [464](#)  
 show diagnostic ondemand settings command [467](#)  
 show diagnostic result command [468](#)  
 show diagnostic schedule command [471](#)  
 show diagnostic status command [473](#)  
 show event manager directory user command [92](#)  
 show event manager environment command [94](#)  
 show event manager metric hardware command [96](#)  
 show event manager metric process command [98](#)  
 show event manager policy available command [102](#)  
 show event manager policy registered command [104](#)  
 show event manager refresh-time command [107](#)  
 show event manager statistics-table command [109](#)  
 show ipsla application command [223](#)  
 show ipsla history command [225](#)  
 show ipsla mpls discovery vpn command [228](#)  
 show ipsla mpls lsp-monitor lpd command [230](#)  
 show ipsla mpls lsp-monitor scan-queue command [232](#)  
 show ipsla mpls lsp-monitor summary command [234](#)  
 show ipsla responder statistics ports command [237](#)  
 show ipsla statistics aggregated command [242](#)  
 show ipsla statistics command [239](#)  
 show ipsla statistics enhanced aggregated command [251](#)  
 show logging command [357](#)  
 show logging correlator buffer command [47](#)  
 show logging correlator info command [50](#)  
 show logging correlator rule command [52](#)  
 show logging correlator ruleset command [55](#)  
 show logging events buffer command [57](#)  
 show logging events info command [62](#)  
 show logging history command [361](#)  
 show logging onboard command [366](#)  
 show logging suppress rule command [64](#)  
 show performance-mgmt bgp command [416](#)  
 show performance-mgmt interface command [418](#)  
 show performance-mgmt mpls command [421](#)  
 show performance-mgmt node command [423](#)

show performance-mgmt ospf command [425](#)  
 show run diagnostic monitor command [474](#)  
 show running performance-mgmt command [427](#)  
 show snmp correlator buffer command [66](#)  
 show snmp correlator info command [68](#)  
 show snmp correlator rule command [69](#)  
 show snmp correlator ruleset command [70](#)  
 source address command [257](#)  
 source command [71](#)  
 source port command [259](#)  
 start-time command [261](#)  
 statistics command [264](#)

## T

tag (IP SLA) command [267](#)  
 target ipv4 command [269](#)  
 target pseudowire command [271](#)  
 target traffic-eng command [273](#)  
 terminal monitor command [363](#)  
 threshold command [275](#)  
 threshold type average command [277](#)  
 threshold type consecutive command [279](#)  
 threshold type immediate command [281](#)  
 threshold type xofy command [283](#)  
 timeout command [72, 285](#)  
 timeout-rootcause command [74](#)  
 tos command [287](#)  
 ttl command [289](#)  
 type icmp echo command [291](#)  
 type icmp path-echo command [292](#)  
 type icmp path-jitter command [293](#)  
 type mpls lsp ping command [294](#)  
 type mpls lsp trace command [296](#)  
 type udp echo command [298](#)  
 type udp ipv4 address command [300](#)  
 type udp jitter command [299](#)

## V

verify-data command [302](#)  
 vrf (IP SLA MPLS LSP monitor) command [306](#)  
 vrf (IP SLA) command [304](#)

