

# System Monitoring Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers

**First Published:** 2016-05-20

**Last Modified:** 2026-09-11

**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

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

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

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

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

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

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

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

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

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

© 2016–2026 Cisco Systems, Inc. All rights reserved.



# CONTENTS


PREFACE

**Preface** xi

Changes to This Document xi

Communications, Services, and Additional Information xii

CHAPTER 1

**Alarm Management and Logging Correlation Commands** 1

alarm 4

all-alarms 5

all-of-router 6

clear logging correlator delete 7

clear logging events delete 8

clear logging events reset 12

context-correlation 13

logging correlator apply rule 14

logging correlator apply ruleset 16

logging correlator buffer-size 18

logging correlator rule 19

logging correlator ruleset 21

logging events buffer-size 22

logging events display-location 23

logging events level 25

logging events threshold 27

logging suppress apply rule 28

logging suppress rule 29

nonrootcause 30

reissue-nonbistate 32

reparent 33

rootcause 35
show alarms 36
show alarms brief 41
show alarms detail 43
show logging correlator buffer 46
show logging correlator info 48
show logging correlator rule 49
show logging correlator ruleset 51
show logging events buffer 53
show logging events info 57
show logging suppress rule 58
show snmp correlator buffer 60
show snmp correlator info 61
show snmp correlator rule 62
show snmp correlator ruleset 63
source 64
timeout 65
timeout-rootcause 66

CHAPTER 2 Embedded Event Manager Commands 67
event manager directory user 69
event manager environment 71
event manager policy 72
event manager refresh-time 75
event manager run 76
event manager scheduler suspend 78
show event manager directory user 79
show event manager environment 80
show event manager policy available 82
show event manager policy registered 84
show event manager refresh-time 87

CHAPTER 3 Logging Services Commands 89
archive-length 91

archive-size 92
clear logging 93
device 94
file-size 95
logging 96
logging archive 99
logging buffered 101
logging console 103
logging console disable 105
logging container all 106
logging events link-status 108
logging facility 109
logging file 111
logging format bsd 114
logging hostnameprefix 115
logging source-interface 116
logging suppress duplicates 117
logging trap 118
login-history 119
process shutdown pam_manager 120
process start pam_manager 121
service timestamps 122
show logging 124
enable-pam process-monitoring 129
disable-pam process-monitoring 130
show pam process-monitoring-status 131
show syslog persistent status 132

CHAPTER 4 **Onboard Failure Logging Commands** 133
show logging onboard 135

CHAPTER 5 **Performance Management Commands** 137
monitor interface 139
performance-mgmt apply monitor 146

performance-mgmt apply statistics 149
performance-mgmt apply thresholds 152
performance-mgmt regular-expression 154
performance-mgmt resources dump local 155
performance-mgmt resources memory 156
performance-mgmt resources tftp-server 157
performance-mgmt statistics 159
performance-mgmt thresholds 161
show performance-mgmt bgp 170
show performance-mgmt interface 172
show performance-mgmt mpls 175
show performance-mgmt node 177
show performance-mgmt ospf 179
show health sysdb 181
show running performance-mgmt 183

CHAPTER 6 **Statistics Service Commands** 185
clear counters 187
load-interval 189
show environment 190

CHAPTER 7 **System Health Check Commands** 197
healthcheck 198
healthcheck metric 199
show healthcheck metric 201
show healthcheck report 203
show healthcheck status 204
use-case 206

CHAPTER 8 **IP Service Level Agreement Commands** 209
access-list 213
action (IP SLA) 215
ageout 217
buckets (history) 218

buckets (statistics hourly) 220
buckets (statistics interval) 221
control disable 222
datasize request 224
destination address (IP SLA) 226
destination port 227
distribution count 228
distribution interval 230
exp 232
filter 234
force explicit-null 236
frequency (IP SLA) 238
history 240
hw-timestamp disable 242
interval 243
ipsla 244
key-chain 245
life 246
lives 247
local-ip 249
low-memory 250
lsp selector ipv4 251
lsr-path 253
maximum hops 254
maximum paths (IP SLA) 256
monitor 258
mpls discovery vpn 259
mpls lsp-monitor 260
operation 261
output interface 262
output nexthop 264
packet count 266
packet interval 267
path discover 268

path discover echo 269
path discover path 271
path discover scan 273
path discover session 275
react 277
react lpd 281
reaction monitor 283
reaction operation 285
reaction trigger 286
recurring 287
reply dscp 288
reply mode 290
responder 292
responder twamp light 293
samples 295
scan delete-factor 297
scan interval 299
schedule monitor 301
schedule operation 302
schedule period 304
server twamp 306
show ipsla application 307
show ipsla history 309
show ipsla mpls discovery vpn 311
show ipsla mpls lsp-monitor lpd 313
show ipsla mpls lsp-monitor scan-queue 315
show ipsla mpls lsp-monitor summary 317
show ipsla responder statistics 320
show ipsla statistics 322
show ipsla statistics aggregated 325
show ipsla statistics enhanced aggregated 334
show ipsla twamp connection 337
show ipsla twamp session 338
show ipsla twamp standards 340

source address 341
source port 343
start-time 344
statistics 346
tag (IP SLA) 348
target ipv4 350
target pseudowire 352
target traffic-eng 354
threshold 356
threshold type average 358
threshold type consecutive 360
threshold type immediate 362
threshold type xofy 364
timeout (IP SLA) 366
tos 368
ttl 370
type icmp echo 372
type icmp path-echo 373
type icmp path-jitter 374
type mpls lsp ping 375
type mpls lsp trace 377
type udp echo 379
type udp jitter 380
type udp ipv4 address 381
verify-data 382
vrf (IP SLA) 383
vrf (IP SLA MPLS LSP monitor) 385

CHAPTER 9 **Out Of Resource Handling Commands** 387
oor hw 388
hw-module profile qos free-buffer-int-threshold 389
show controllers npu resources 390
show controllers npu resources qos 394
show grid pool 397

CHAPTER 10 Tech-Support Commands 399

show tech-support custom 400

show tech-support mgbl 413

show tech-support mgbl grpc 415

show tech-support mgbl netconf 417

show tech-support mgbl telemetry 419

show tech-support multicast address-family 421

show tech-support ztp brief 423

CHAPTER 11 Traffic Monitoring Commands 425

show controllers npu exttcamipv4 426

show controllers npu exttcamipv6 428

show drops all 430

show controllers npu stats counters-all 433

show controllers npu stats traps-all 436

show controllers npu stats voq 439

show fwd statistics 443

show spp client 446

show spp node-counters 449

show controllers fia diagshell 453

show controllers fia statistics 455

show netio drops 459

CHAPTER 12 Audit Monitoring Commands 461

linux security audit 462

show linux security audit 467



# Preface

This preface contains these sections:


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


## Changes to This Document

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

***Table 1: Changes to This Document***

| Date | Summary |
|---|---|
| September 2025 | Republished with documentation updates for Release 25.3.1. |
| December 2024 | Republished with documentation updates for Release 24.4.1. |
| January 2024 | Republished with documentation updates for Release 7.3.6. |
| August 2023 | Republished with documentation updates for Release 7.3.5. |
| February 2021 | Republished with documentation updates for Release 7.3.1. |
| May 2019 | Republished with documentation updates for Release 6.6.25. |
| March 2019 | Republished with documentation updates for Release 6.5.3. |
| September 2017 | Republished with documentation updates for Release 6.3.1. |
| July 2016 | Republished with documentation updates for Cisco IOS XR Release 6.0.2. |

| Date | Summary |
|---|---|
| May 2016 | Initial release of this document. |

# Communications, Services, and Additional Information

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

### Cisco Bug Search Tool

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



# 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.

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

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 *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.

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

For system logging concepts, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- alarm, on page 4
- all-alarms, on page 5
- all-of-router, on page 6
- clear logging correlator delete, on page 7
- clear logging events delete, on page 8
- clear logging events reset, on page 12
- context-correlation, on page 13
- logging correlator apply rule, on page 14
- logging correlator apply ruleset, on page 16
- logging correlator buffer-size, on page 18
- logging correlator rule, on page 19

- logging correlator ruleset, on page 21
- logging events buffer-size, on page 22
- logging events display-location, on page 23
- logging events level, on page 25
- logging events threshold, on page 27
- logging suppress apply rule, on page 28
- logging suppress rule, on page 29
- nonrootcause, on page 30
- reissue-nonbistate, on page 32
- reparent, on page 33
- rootcause, on page 35
- show alarms, on page 36
- show alarms brief, on page 41
- show alarms detail, on page 43
- show logging correlator buffer, on page 46
- show logging correlator info, on page 48
- show logging correlator rule, on page 49
- show logging correlator ruleset, on page 51
- show logging events buffer, on page 53
- show logging events info, on page 57
- show logging suppress rule, on page 58
- show snmp correlator buffer, on page 60
- show snmp correlator info, on page 61
- show snmp correlator rule, on page 62
- show snmp correlator ruleset, on page 63
- source, on page 64
- timeout, on page 65
- timeout-rootcause, on page 66

# 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

| | |
|---|---|
| *msg-category* | Message category of the root message. |
| *group-name* | Group name of the root message. |
| *msg-code* | 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 6.0 | 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/RP0/CPU0:router(config)# logging suppress rule commit
RP/0/RP0/CPU0:router(config-suppr-rule)# alarm MBGL COMMIT SUCCEEDED
```

# 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 6.0 | 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/RP0/CPU0:router(config)# logging suppress rule commit
RP/0/RP0/CPU0:router(config-suppr-rule)# all-alarms
```

# 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 6.0 | 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/RP0/CPU0:router(config)# logging suppress apply rule commit
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# all-of-router
```

# 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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **all-in-buffer** | Clears all messages in the logging correlator buffer. |
| *correlation-id* | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

Use the show logging correlator buffer, on page 46 command to confirm that records have been cleared.

Use the logging correlator buffer-size, on page 18 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/RP0/CPU0:router# clear logging correlator delete all-in-buffer
```

# clear logging events delete

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

**clear logging events delete**

## Syntax Description

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

| | |
|---|---|
| **severity** | Severity level. Valid values are:<br>• **alerts**<br>• **critical**<br>• **emergencies**<br>• **errors**<br>• **informational**<br>• **notifications**<br>• **warnings**<br>**Note**<br>Settings for the severity levels and their respective system conditions are listed under the "Usage Guidelines" section for the **logging events level** command. Events of lower severity level represent events of higher importance. |
| **severity-lo-limit** | Deletes events with a severity level equal to or higher than the severity level specified with the *severity* argument. |
| **timestamp-hi-limit** | 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.<br>Ranges for the *hh* **:** *mm* **:** *ss month day year* arguments are as follows:<br>• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.<br>• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.<br>• *ss*—Seconds. Range is 00 to 59.<br>• *month*—(Optional) The month of the year. The values for the *month* argument are:<br>• january<br>• february<br>• march<br>• april<br>• may<br>• june<br>• july<br>• august<br>• september<br>• october<br>• november<br>• december<br>• *day*—(Optional) Day of the month. Range is 01 to 31.<br>• *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37. |
| **timestamp-lo-limit** | 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**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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 53 command to verify that events have been cleared from the logging events buffer.

Use the logging events buffer-size, on page 22 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/RP0/CPU0:router# clear logging events delete all-in-buffer
```

# clear logging events reset

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

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

## Syntax Description

| | |
|---|---|
| **all-in-buffer** | Resets all bi-state alarm messages in the event logging buffer. |
| *event-id* | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 a change in component temperature.

Use the show logging events buffer, on page 53 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/RP0/CPU0:router# clear logging events reset all-in-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

## Command History

| Release | Modification |
|---|---|
| Release 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 49 command to show the current setting for the context-correlation flag.

## Task ID

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

## Examples

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

```
RP/0/RP0/CPU0:router(config)# logging correlator rule stateful_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# context-correlation
```

# 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 XR Config 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

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

## Command Default

No correlation rules are applied.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 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 49 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/RP0/CPU0:router(config)# logging correlator apply rule stateful1
RP/0/RP0/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 XR Config mode
  show           Show contents of configuration
RP/0/RP0/CPU0:router(config-corr-apply-rule)#
```

While in the submode, you can negate keyword options:

```
RP/0/RP0/CPU0:router(config-corr-apply-rule)# no all-of-router
RP/0/RP0/CPU0:router(config-corr-apply-rule)# no context
RP/0/RP0/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/RP0/CPU0:router(config)# logging correlator apply rule rule1
RP/0/RP0/CPU0:router(config-corr-apply-rule)# location 0/2/CPU0
```

# 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 XR Config 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

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

## Command Default

No correlation rule sets are applied.

## Command Modes

XR Config mode

## Command History

| | |
|---|---|
| **location** *node-id* | (Optional) Displays location information for the specified node ID. |

## 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 51 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/RP0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/RP0/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 XR Config mode
  show           Show contents of configuration
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)#
```

While in the submode, you can negate keyword options:

```
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)# no all-of-router
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)# no context
RP/0/RP0/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/RP0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/RP0/CPU0:router(config-corr-apply-rule)# all-of-router
```

# logging correlator buffer-size

To configure the logging correlator buffer size, use the **logging correlator buffer-size** command in XR Config 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*

## Syntax Description

| | |
|---|---|
| *bytes* | The size, in bytes, of the logging correlator buffer. Range is 1024 to 52428800 bytes. |

## Command Default

*bytes*: 81920 bytes

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

The **logging correlator buffer-size** 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:

- First, remove the oldest nonstateful correlation records from the buffer.
- Then, if there are no more nonstateful correlations present; remove the oldest stateful correlation records.

Use the show logging correlator info, on page 48 command to confirm the size of the buffer and the percentage of buffer space that is currently used. The show logging events buffer, on page 53 **all-in-buffer** command can be used to show the details of the buffer contents.

## Task ID

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

## Examples

This example shows how to set the logging correlator buffer size to 90000 bytes:

```
RP/0/RP0/CPU0:router(config)# logging correlator buffer-size 90000
```

# logging correlator rule

To define the rules for correlating messages, use the **logging correlator rule** command in XR Config 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

| | |
|---|---|
| *correlation-rule* | Name of the correlation rule to be applied. |
| **type** | Specifies the type of rule. |
| **stateful** | Enters stateful correlation rule configuration mode. |
| **nonstateful** | Enters nonstateful correlation rule configuration mode. |

## Command Default

No rules are defined.

## Command Modes

XR Config mode

## Syntax Description

| | |
|---|---|
| **location** *node-id* | (Optional) Displays location information for the specified node ID. |

## 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/RP0/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/RP0/CPU0:router(config-corr-rule-st)#
```

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

```
RP/0/RP0/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/RP0/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 46 to display messages stored in the logging correlator buffer.

Use the show logging correlator rule, on page 49 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/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout 50000
```

# logging correlator ruleset

To enter correlation rule set configuration mode and define a correlation rule set, use the **logging correlator ruleset** command in XR Config 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

| | |
|---|---|
| *correlation-ruleset* | Name of the correlation rule set to be applied. |
| **rulename** | Specifies the correlation rule name. |
| *correlation-rulename* | Name of the correlation rule name to be applied. |

## Command Default

No rule sets are defined.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 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 16 command.

## Examples

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

```
RP/0/RP0/CPU0:router(config)# logging correlator ruleset ruleset_1
RP/0/RP0/CPU0:router(config-corr-ruleset)# rulename state_rule
RP/0/RP0/CPU0:router(config-corr-ruleset)# rulename state_rule2
```

# logging events buffer-size

To configure the size of the logging events buffer, use the **logging events buffer-size** command in XR Config 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

| | |
|---|---|
| *bytes* | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 57 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/RP0/CPU0:router(config)# logging events buffer-size 50000
```

# 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 XR Config 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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

| 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/RP0/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/RP0/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/RP0/CPU0/0, changed state to Administratively Down
RP/0/RP0/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
 on Interface MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/RP0/CPU0/0, changed state to Up
RP/0/RP0/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
 on Interface MgmtEth0/RP0/CPU0/0, changed state to Up

RP/0/RP0/CPU0:router# config
Wed Aug 13 01:31:32.517 UTC

RP/0/RP0/CPU0:router(config)# logging events display-location

RP/0/RP0/CPU0:router(config)# commit

RP/0/RP0/CPU0:router(config)# exit

RP/0/RP0/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/RP0/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/RP0/CPU0/0, changed state to Administratively Down
RP/0/RP0/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/RP0/CPU0/0: Interface MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/RP0/CPU0/0: Line protocol on Interface MgmtEth0/RP0/CPU0/0, changed state to Down

RP/0/RP0/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/RP0/CPU0/0: Interface MgmtEth0/RP0/CPU0/0, changed state to Up
RP/0/RP0/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/RP0/CPU0/0: Line protocol on Interface MgmtEth0/RP0/CPU0/0, changed state to Up
```

# logging events level

To specify a severity level for logging alarm messages, use the **logging events level** command in XR Config 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 25lists severity levels and their respective system conditions. |

## Command Default

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

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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. |
| 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/RP0/CPU0:router(config)# logging events level warnings
```

# logging events threshold

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

**logging events threshold** *percent*
**no logging events threshold**

## Syntax Description

| | |
|---|---|
| *percent* | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 57 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/RP0/CPU0:router(config)# logging events threshold 95
```

# logging suppress apply rule

To apply and activate a logging suppression rule, use the **logging suppress apply rule** command in XR Config 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

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

## Command Default

No logging suppression rules are applied.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)#logging suppress apply rule infobistate
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# all-of-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 XR Config 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

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

## Command Default

No logging suppression rules exist by default.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)# logging suppress rule infobistate
RP/0/RP0/CPU0:router(config-suppr-rule)#
```

# 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

| | |
|---|---|
| **alarm** | Non-root-cause alarm. |
| *msg-category* | (Optional) Message category assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space. |
| *group-name* | (Optional) Message group assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space. |
| *msg-code* | (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 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 57 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/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# nonrootcause
 (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 XR Config mode
show      Show contents of configuration
```

# 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 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/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# 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 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/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# reparent
```

# 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

| | |
|---|---|
| *msg-category* | Message category of the root message. |
| *group-name* | Group name of the root message. |
| *msg-code* | 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 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 57 command to display the root-cause and non-root-cause alarms for a correlation rule.

## Task ID

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

# show alarms

To display alarms related to System Monitoring, use the **show alarms** command in the System Monitoring mode.

**show alarms**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

System Monitoring EXEC

## Command History

| Release | Modification |
|---|---|
| Release 3.9.0 | This command was introduced. |

## Usage Guidelines

Use the show alarms brief, on page 41 to view the router alarms in brief.

Use the show alarms detail, on page 43 to view the router alarms in detail.

## Task ID

| Task ID | Operations |
|---|---|
| logging | read |

This example displays the output of the **show alarms** command:

```
RP/0/RSP0/CPU0:router#show alarms
------------------------------------------------------------------------
Active Alarms (Brief) for 1/0
------------------------------------------------------------------------
Location    Severity   Group     Set time               Description

------------------------------------------------------------------------
0/1/CPU0   Critical   Fabric   11/11/2022 10:34:22 IST  LC Bandwidth Insufficient To Support
 Line Rate Traffic
1/0/CPU0    Major    Software  11/11/2022 10:43:36 IST   Optics1/0/0/20 - hw_optics:  RX
LOS LANE-0 ALARM
1/0/CPU0    Major    Software  11/11/2022 10:43:36 IST   Optics1/0/0/20 - hw_optics:  RX
LOS LANE-1 ALARM
------------------------------------------------------------------------------------
History Alarms (Brief) for 1/0
------------------------------------------------------------------------------------
No entries.

------------------------------------------------------------------------------------
Suppressed Alarms (Brief) for 1/0
------------------------------------------------------------------------------------
No entries.

------------------------------------------------------------------------------------
Conditions (Brief) for 1/0
```

```
------------------------------------------------------------------------------
No entries.
------------------------------------------------------------------------------
System Scoped Active Alarms (Brief)
------------------------------------------------------------------------------
Location    Severity    Group     Set Time                 Description

------------------------------------------------------------------------------
D1           Major      Environ   11/16/2022 11:37:41 IST  Power Group redundancy lost.

D1/PM1       Major      Environ   11/16/2022 11:37:41 IST  Power Module Output Disabled
(PM_OUTPUT_EN_PIN_HI).
------------------------------------------------------------------------------
System Scoped History Alarms (Brief)
------------------------------------------------------------------------------
Location   Severity     Group       Set Time                 Description

                                    Clear Time
------------------------------------------------------------------------------
7/0        Major        Fabric      07/14/2022 11:51:38 IST  7/0/1/6 - hw_optics:  RX LOS
LANE-0 ALARM
7/0        Major        Fabric      07/18/2022 12:29:02 IST
                                    07/14/2022 11:51:38 IST  7/0/1/6 - hw_optics:  RX LOS
LANE-1 ALARM
7/0/CPU0  Critical      Fabric      09/13/2022 11:40:53 IST
                                    09/09/2022 21:50:13 IST  LC Bandwidth Insufficient To
Support Line Rate Traffic
------------------------------------------------------------------------------
Active Alarms (Brief) for EDT
------------------------------------------------------------------------------
Location   Severity     Group        Set Time                   Description

------------------------------------------------------------------------------
D1          Major      Environ      11/16/2022 11:37:41 IST    Power Group redundancy lost.

D1/PM1      Major      Environ      11/16/2022 11:37:41 IST    Power Module Output Disabled
 (PM_OUTPUT_EN_PIN_HI).
E0          Major      Environ      11/16/2022 11:37:42 IST    Power Group redundancy lost.

------------------------------------------------------------------------------
Active Alarms (Brief) for EDT
------------------------------------------------------------------------------
Location   Severity     Group         Set Time                   Description


------------------------------------------------------------------------------
D1           Major       Environ       11/16/2022 11:37:41 IST    Power Group redundancy
lost.

D1/PM1      Major       Environ      11/16/2022 11:37:41 IST    Power Module Output Disabled
 (PM_OUTPUT_EN_PIN_HI).
E0           Major       Environ       11/16/2022 11:37:42 IST    Power Group redundancy
lost.
------------------------------------------------------------------------------
History Alarms (Detail) for 1/0
------------------------------------------------------------------------------
No entries.

------------------------------------------------------------------------------
Suppressed Alarms (Detail) for 1/0
------------------------------------------------------------------------------
No entries.

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

```
Conditions (Detail) for 1/0
--------------------------------------------------------------------------------
No entries.

--------------------------------------------------------------------------------
Clients for 1/0
--------------------------------------------------------------------------------
Agent Name:              optics_fm.xml
Agent ID:                196678
Agent Location:          1/0/CPU0
Agent Handle:            93827323237168
Agent State:             Registered
Agent Type:              Producer
Agent Filter Display:    false
Agent Subscriber ID:     0
Agent Filter Severity:   Unknown
Agent Filter State:      Unknown
Agent Filter Group:      Unknown
Agent Connect Count:     1
Agent Connect Timestamp: 11/16/2022 20:40:18 IST
Agent Get Count:         0
Agent Subscribe Count:   0
Agent Report Count:      8
--------------------------------------------------------------------------------
Statistics for 1/0
--------------------------------------------------------------------------------
Alarms Reported:               9
Alarms Dropped:                0
Active (bi-state set):         9
History (bi-state cleared):    0
Suppressed:                    0
Dropped Invalid AID:           0
Dropped No Memory:             0
Dropped DB Error:              0
Dropped Clear Without Set:     0
Dropped Duplicate:             0
Cache Hit:                     0
Cache Miss:                    0
Active Alarms (Detail) for 7/0
--------------------------------------------------------------------------------
Description:             LC Bandwidth Insufficient To Support Line Rate Traffic


Location:                7/0/CPU0
AID:                     XR_FABRIC/SW_MISC_ERR/18
Tag String:              FAM_FAULT_TAG_HW_FIA_LC_BANDWIDTH
Module Name:             N/A
EID:                     MODULE/MSC/1:MODULE/SLICE/1:MODULE/PSE/1
Reporting Agent ID:      524365
Pending Sync:            false
Severity:                Critical
Status:                  Set
Group:                   Fabric
Set Time:                11/16/2022 20:42:41 IST
Clear Time:              -
Service Affecting:       NotServiceAffecting
Transport Direction:     NotSpecified
Transport Source:        NotSpecified
Interface:               N/A
Alarm Name:              LC-BW-DEG
--------------------------------------------------------------------------------
History Alarms (Detail) for 7/0
--------------------------------------------------------------------------------
No entries.
```

```
------------------------------------------------------------------------------
Suppressed Alarms (Detail) for 7/0
------------------------------------------------------------------------------
No entries.
------------------------------------------------------------------------------
Conditions (Detail) for 7/0
------------------------------------------------------------------------------
No entries.
------------------------------------------------------------------------------
Clients for 7/0
------------------------------------------------------------------------------
Agent Name:              optics_fm.xml
Agent ID:                196678
Agent Location:          7/0/CPU0
Agent Handle:            94180835316528
Agent State:             Registered
Agent Type:              Unknown
Agent Filter Display:    false
Agent Subscriber ID:     0
Agent Filter Severity:   Unknown
Agent Filter State:      Unknown
Agent Filter Group:      Unknown
Agent Connect Count:     1
Agent Connect Timestamp: 11/16/2022 20:40:11 IST
Agent Get Count:         0
Agent Subscribe Count:   0
Agent Report Count:      0
------------------------------------------------------------------------------
Agent Name:              fia_fm.xml
Agent ID:                524365
Agent Location:          7/0/CPU0
Agent Handle:            94180835313792
Agent State:             Registered
Agent Type:              Producer
Agent Filter Display:    false
Agent Subscriber ID:     0
Agent Filter Severity:   Unknown
Agent Filter State:      Unknown
Agent Filter Group:      Unknown
Agent Connect Count:     1
Agent Connect Timestamp: 11/16/2022 20:39:59 IST
Agent Get Count:         0
Agent Subscribe Count:   0
Agent Report Count:      1
Statistics for 7/0
------------------------------------------------------------------------------
Alarms Reported:               1
Alarms Dropped:                0
Active (bi-state set):         1
History (bi-state cleared):    0
Suppressed:                    0
Dropped Invalid AID:           0
Dropped No Memory:             0
Dropped DB Error:              0
Dropped Clear Without Set:     0
Dropped Duplicate:             0
Cache Hit:                     0
Cache Miss:                    0
```

## Related Commands

| Command | Description |
|---|---|
| show alarms brief, on page 41 | Displays router alarms in brief. |

| Command | Description |
| --- | --- |
| show alarms detail, on page 43 | Displays router alarms in detail. |

# show alarms brief

To display alarms related to System Monitoring, use the **show alarms brief** command in the System Monitoring mode.

**show alarms brief** [ **aid** [ **active** { * } ] | **card** [ **location** *location-ID* [ **active** | **conditions** | **history** | **suppressed** ] ] | **system** [ **active** | **conditions** | **history** | **suppressed** ] ]

## Syntax Description

| | |
|---|---|
| **brief** | Displays alarms in brief. |
| **aid** | Displays system scope alarms related data. |
| **card** | Displays card scope alarms related data. |
| **system** | Displays brief system scope related data. |
| **active** | Displays the active alarms at this scope. |
| **conditions** | Displays the conditions present at this scope. |
| **history** | Displays the history alarms at this scope. |
| **suppressed** | Displays the suppressed alarms at this scope. |

## Command Default

None

## Command Modes

System Monitoring EXEC

## Command History

| Release | Modification |
|---|---|
| Release 3.9.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| logging | read |

This example displays the output of the **show alarms brief** command:

```
RP/0/RSP0/CPU0:router#show alarms brief

------------------------------------------------------------------------
Active Alarms for 1/0
------------------------------------------------------------------------
Location    Severity   Group     Set time              Description

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

```
0/1/CPU0   Critical   Fabric   11/11/2022 10:34:22 IST  LC Bandwidth Insufficient To Support
 Line Rate Traffic
1/0/CPU0    Major    Software  11/11/2022 10:43:36 IST   Optics1/0/0/20 - hw_optics:  RX
LOS LANE-0 ALARM
1/0/CPU0    Major    Software  11/11/2022 10:43:36 IST   Optics1/0/0/20 - hw_optics:  RX
LOS LANE-1 ALARM
------------------------------------------------------------------------------
History Alarms for 1/0
------------------------------------------------------------------------------
No entries.

------------------------------------------------------------------------------
Suppressed Alarms for 1/0
------------------------------------------------------------------------------
No entries.

------------------------------------------------------------------------------
Conditions for 1/0
------------------------------------------------------------------------------
No entries.
```

## Related Commands

| Command | Description |
|---|---|
| show alarms, on page 36 | Displays router alarms in brief and detail. |
| show alarms detail, on page 43 | Displays router alarms in detail. |

# show alarms detail

To display alarms related to System Monitoring, use the **show alarms detail** command in the System Monitoring mode.

**show alarms detail** [ **aid** [ **active** { * } ] | **card** [ **location** *location-ID* [ **active** | **conditions** | **history** | **suppressed** ] ] | **system** [ **active** | **clients** | **conditions** | **history** | **stats** | **suppressed** ] ]

## Syntax Description

| | |
|---|---|
| **detail** | Displays alarms in detail. |
| **aid** | Displays system scope alarms related data. |
| **card** | Displays card scope alarms related data. |
| **system** | Displays system scope alarms related data. |
| **active** | Displays the active alarms at this scope. |
| **clients** | Displays the clients associated with this service. |
| **conditions** | Displays the conditions present at this scope. |
| **history** | Displays the history alarms at this scope. |
| **stats** | Displays the service statistics. |
| **suppressed** | Displays the suppressed alarms at this scope. |

## Command Default

None

## Command Modes

System Monitoring EXEC

## Command History

| Release | Modification |
|---|---|
| Release 3.9.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| logging | read |

This example displays the output of the **show alarms detail** command:

```
RP/0/RSP0/CPU0:router#show alarms detail

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

```
Active Alarms for 1/0
------------------------------------------------------------------------
Description:            LC Bandwidth Insufficient To Support Line Rate Traffic


Location:               1/0/CPU0
AID:                    XR_FABRIC/SW_MISC_ERR/18
Tag String:             FAM_FAULT_TAG_HW_FIA_LC_BANDWIDTH
Module Name:            N/A
EID:                    MODULE/MSC/1:MODULE/SLICE/1:MODULE/PSE/1
Reporting Agent ID:     524365
Pending Sync:           false
Severity:               Critical
Status:                 Set
Group:                  Fabric
Set Time:               11/11/2022 10:34:22 IST
Clear Time:             -
Service Affecting:      NotServiceAffecting
Transport Direction:    NotSpecified
Transport Source:       NotSpecified
Interface:              N/A
Alarm Name:             LC-BW-DEG
------------------------------------------------------------
History Alarms for 1/0
--------------------------------------------------------------------------------
No entries.

--------------------------------------------------------------------------------
Suppressed Alarms for 1/0
--------------------------------------------------------------------------------
No entries.

--------------------------------------------------------------------------------
Conditions for 1/0
--------------------------------------------------------------------------------
No entries.
------------------------------------------------------------
Clients for 1/0
------------------------------------------------------------
Agent Name:             optics_fm.xml
Agent ID:               196678
Agent Location:         1/0/CPU0
Agent Handle:           94374612126576
Agent State:            Registered
Agent Type:             Producer
Agent Filter Display:   false
Agent Subscriber ID:    0
Agent Filter Severity:  Unknown
Agent Filter State:     Unknown
Agent Filter Group:     Unknown
Agent Connect Count:    1
Agent Connect Timestamp: 11/11/2022 10:30:04 IST
Agent Get Count:        0
Agent Subscribe Count:  0
Agent Report Count:     8
------------------------------------------------------------
Statistics for 1/0
------------------------------------------------------------
Alarms Reported:               9
Alarms Dropped:                0
Active (bi-state set):         9
History (bi-state cleared):    0
Suppressed:                    0
Dropped Invalid AID:           0
```

```
Dropped No Memory:              0
Dropped DB Error:               0
Dropped Clear Without Set:      0
Dropped Duplicate:              0
Cache Hit:                      0
Cache Miss:                     0
```

## Related Commands

| Command | Description |
|---|---|
| show alarms, on page 36 | Displays router alarms in brief and detail. |
| show alarms brief, on page 41 | Displays router alarms in brief. |

# show logging correlator buffer

To display messages in the logging correlator buffer, use the **show logging correlator buffer** command in XR 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

| | |
|---|---|
| **all-in-buffer** | Displays all messages in the correlation buffer. |
| **ruletype** | (Optional) Displays the ruletype filter. |
| **nonstateful** | (Optional) Displays the nonstateful rules. |
| **stateful** | (Optional) Displays the stateful rules. |
| **rulesource** | (Optional) Displays the rulesource filter. |
| **internal** | (Optional) Displays the internally defined rules from the rulesource filter. |
| **user** | (Optional) Displays the user-defined rules from the rulesource filter. |
| **rule-name** *correlation-rule1...correlation-rule14* | Displays a messages associated with a correlation rule name. Up to 14 correlation rules can be specified, separated by a space. |
| **correlationID** *correlation-id1..correlation-id14* | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# show logging correlator buffer all-in-buffer

#C_id.id:Rule Name:Source :Context: Time : Text
#14.1 :Rule1:RP/0/RP0/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]: %PKT_INFRA-LINK-3-UPDOWN
 : Interface MgmtEth0/RP0/CPU0/0, changed state to Down
#14.2 :Rule1:RP/0/RP0/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]:
%PKT_INFRA-LINEPROTO-3-UPDOWN : Line protocol on Interface MgmtEth0/RP0/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. |
| 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. |

# 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 XR EXEC mode.

**show logging correlator info**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 18 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/RP0/CPU0:router# show logging correlator info

Buffer-Size     Percentage-Occupied
      81920                   0.00
```

# show logging correlator rule

To display defined correlation rules, use the **show logging correlator rule** command in XR 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

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

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 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 keywords are not specified, then detailed information is displayed as the default.

**Task ID**

| Task ID | Operations |
|---|---|
| logging | read |

# show logging correlator ruleset

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

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

## Syntax Description

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

## Command Default

Detail is the default, if nothing is specified.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 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/RP0/CPU0:router# show logging correlator RuleSetOne RuleSetTwo

Rule Set Name : RuleSetOne
Rules: Rule1 : Applied
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/RP0/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/RP0/CPU0:router# show logging correlator ruleset all summary
RuleSetOne
RuleSetTwo
RuleSetThree
```

This table describes the significant fields shown in the display.

***Table 4: 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. |

# show logging events buffer

To display messages in the logging events buffer, use the **show logging events buffer** command in XR 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

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

| | |
|---|---|
| **severity** | Severity level. Valid values are:<br>• **emergencies**<br>• **alerts**<br>• **critical**<br>• **errors**<br>• **warnings**<br>• **notifications**<br>• **informational**<br>**Note**<br>Settings for the severity levels and their respective system conditions are listed under the "Usage Guidelines" section for the **logging events level** command. Events of lower severity level represent events of higher importance. |
| **severity-lo-limit** | Displays events with a severity level equal to or higher than the specified severity level. |
| **timestamp-hi-limit** | 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.<br>Ranges for the *hh* **:** *mm* **:** *ss month day year* arguments are as follows:<br>• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.<br>• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.<br>• *ss*—Seconds. Range is 00 to 59.<br>• *month*—(Optional) The month of the year. The values for the *month* argument are:<br>  • january<br>  • february<br>  • march<br>  • april<br>  • may<br>  • june<br>  • july<br>  • august<br>  • september<br>  • october<br>  • november<br>  • december<br>• *day*—(Optional) Day of the month. Range is 01 to 31.<br>• *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37. |
| **timestamp-lo-limit** | Displays events with a time stamp equal to or higher than the specified time stamp. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# show logging events buffer all-in-buffer

#ID    :C_id:Source  :Time                :%CATEGORY-GROUP-SEVERITY-MESSAGECODE: Text

#1     :    :RP/0/RPO/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/RP0/CPU0:Jan  9 08:58:21 2004:psarb[238]: %PLATFORM-PSARB-5-GO_BID : Card

 is going to bid state.
#3     :    :RP/0/RP0/CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-5-GO_ACTIVE :
Card is becoming active.
#4     :    :RP/0/RP0/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/RP0/CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-GO_ACTIVE : this
 card going active
#6     :    :RP/0/RP0/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 5: 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. |
| Text | Message string that delineates the event. |

# show logging events info

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

**show logging events info**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 6: 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 logging events buffer-size, on page 22 command. |
| #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 logging events threshold, on page 27 command. |
| Filter | The lowest severity level for events that will be displayed. This field is controlled by the logging events level, on page 25 command. |

# show logging suppress rule

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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:  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/RP0/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/RP0/CPU0:router# show logging suppression rule all summmary
Rule Name                                :Number of Suppressed Alarms
Mike1                                    0
Mike2                                    0
Mike3                                    0
Real1                                    4
```

# show snmp correlator buffer

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

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

## Syntax Description

| | |
|---|---|
| **all** | Displays all messages in the correlator buffer. |
| **correlation** *id* | Displays a message identified by correlation ID. Range is 0 to 4294967294. Up to 14 correlation rules can be specified, separated by a space. |
| **rule-name** *name* | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| snmp | read |

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

```
RP/0/RP0/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 = hundredGigE0/1/0/8
       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 = 10.1.1.1
           ospfNbrIpAddr = 10.0.28.2
           ospfNbrAddressLessIndex = 0
           ospfNbrRtrId = 10.3.3.3
           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 XR EXEC mode.

**show snmp correlator info**

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

**Command Default** None

**Command Modes** XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

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

**Task ID**

| Task ID | Operation |
|---|---|
| snmp | read |

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/RP0/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 XR EXEC mode.

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

**Syntax Description**

| | |
|---|---|
| **all** | Displays all rule sets. |
| *rule-name* | 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**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operation |
|---|---|
| snmp | read |

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

```
RP/0/RP0/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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **all** | Displays all rule set names. |
| *ruleset-name* | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| snmp | read |

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

```
RP/0/RP0/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

| | |
|---|---|
| **location** *node-id* | Specifies a node. The *node-id* argument is entered in the *rack/slot/module* notation. |

## Command Default

No scope is configured by default.

## Command Modes

Logging suppression apply rule configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)# logging suppress apply rule infobistate
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# source location 0/RP0/CPU0
```

# 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 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/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout 60000
```

# 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

| | |
|---|---|
| *milliseconds* | Range is 1 to 600000 milliseconds.<br>Range is 1 to 7200000 milliseconds. |

## Command Default

Root-cause alarm timeout period is not specified.

## Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

When a root-cause timeout is configured and a non-root-cause message is received first, the following occurs:

- 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.
- 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.

## Task ID

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

## Examples

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

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout-rootcause 50000
```



# 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.

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

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.

For detailed information about the EEM concepts, configuration tasks, and examples, see the *Configuring and Managing Embedded Event Manager Policies* module in *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- event manager directory user, on page 69
- event manager environment, on page 71
- event manager policy, on page 72
- event manager refresh-time, on page 75
- event manager run, on page 76
- event manager scheduler suspend, on page 78
- show event manager directory user, on page 79
- show event manager environment, on page 80
- show event manager policy available, on page 82
- show event manager policy registered, on page 84
- show event manager refresh-time, on page 87

# 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 XR Config 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

| | |
|---|---|
| **library** | Specifies a directory name for storing user library files. |
| *path* | Absolute pathname to the user directory on the flash device. |
| **policy** | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 XR 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 XR 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/RP0/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/RP0/CPU0:router(config)# event manager directory user policy disk0:/usr/fm_policies
```

# event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in XR Config 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

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

## Command Default

None

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 uptil the end of the line in order to be a part of the *var-value* argument.

Use the event manager environment, on page 71 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/RP0/CPU0:router(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
RP/0/RP0/CPU0:router(config)# event manager environment _show_cmd show eem manager policy
registered
RP/0/RP0/CPU0:router(config)# event manager environment _email_server alpha@cisco.com
RP/0/RP0/CPU0:router(config)# event manager environment _email_from beta@cisco.com
RP/0/RP0/CPU0:router(config)# event manager environment _email_to beta@cisco.com
RP/0/RP0/CPU0:router(config)# event manager environment _email_cc
```

# event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in XR Config 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*]

## Syntax Description

| | |
|---|---|
| *policy-name* | Name of the policy file. |
| **username** *username* | 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.<br>In addition, the username that runs the script must have access privileges to the commands issued by the EEM policy being registered. |
| **persist-time** [*seconds* \| **infinite**] | (Optional) The length of the username authentication validity, in seconds. The default time is 3600 seconds (1 hour). The *seconds* range is 0 to 4294967294. Enter 0 to stop the username authentication from being cached. Enter the **infinite** keyword to stop the username from being marked as invalid. |
| **type** | (Optional) Specifies the type of policy. |
| **system** | (Optional) Registers a system policy defined by Cisco. |
| **user** | (Optional) Registers a user-defined policy. |

## Command Default

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

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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* module of *System Security Configuration Guide for Cisco NCS 5500 Series RoutersSystem Security Configuration Guide for Cisco NCS 540 Series RoutersSystem Security Configuration Guide* 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 75 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/RP0/CPU0:router(config)# event manager policy cron.tcl username joe
```

# 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 XR Config 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

| | |
|---|---|
| *seconds* | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| *policy* | Name of the policy file. |
| [*argument*[...[*argument15*]]] | 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 run, on page 76 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/RP0/CPU0:router# event manager run policy-manual.tcl parameter1 parameter2 parameter3

RP/0/RP0/CPU0:Sep 20 10:26:31.169 : user-plocy.tcl[65724]: The reqinfo of arg2 is parameter2.

RP/0/RP0/CPU0:Sep 20 10:26:31.170 : user-plocy.tcl[65724]: The reqinfo of argc is 3.
RP/0/RP0/CPU0:Sep 20 10:26:31.171 : user-plocy.tcl[65724]: The reqinfo of arg3 is parameter3.

RP/0/RP0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_type_string
 is none.
RP/0/RP0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_pub_sec is
```

```
 1190283990.
RP/0/RP0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_pub_time
is 1190283990.
RP/0/RP0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_id is 3.
RP/0/RP0/CPU0:Sep 20 10:26:31.174 : user-plocy.tcl[65724]: The reqinfo of arg1 is parameter1.

RP/0/RP0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_type is 16.

RP/0/RP0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_pub_msec
is 830
```

# event manager scheduler suspend

To suspend the Embedded Event Manager (EEM) policy scheduling execution immediately, use the **event manager scheduler suspend** command in XR Config 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/CPU0:router(config)# event manager scheduler suspend
```

This example shows how to enable policy scheduling:

```
RP/0/RP0/CPU0:router(config)# no event manager scheduler suspend
```

# 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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **library** | Specifies the user library files. |
| **policy** | Specifies the user-defined EEM policies. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# show event manager directory user library
disk0:/fm_user_lib_dir

RP/0/RP0/CPU0:router# show event manager directory user policy
disk0:/fm_user_pol_dir
```

# 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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Specifies all the environment variables. |
| *environment-name* | (Optional) Environment variable for which data is displayed. |

## Command Default

All environment variables are displayed.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# show event manager environment

No.  Name                           Value
1    _email_cc
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 7: show event manager environment Field Descriptions***

| Field | Description |
|---|---|
| No. | Number of the EEM environment variable. |
| Name | Name of the EEM environment variable. |

| Field | Description |
|---|---|
| Value | Value of the EEM environment variable. |

# 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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **system** | (Optional) Displays all the available system policies. |
| **user** | (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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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 8: 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. |

# 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 XR EXEC mode.

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

## Syntax Description

| | |
|---|---|
| **event-type** *type* | (Optional) Displays the registered policies for a specific event type, where the valid *type* options are as follows:<br>• **application**—Application event type<br>• **cli**—CLI event type<br>• **config**—Conf event type<br>• **counter**—Counter event type<br>• **hardware**—Hardware event type<br>• **none**—None event type<br>• **oir**—Online insertion and removal (OIR) event type<br>• **process-abort**—Event type for abnormal termination of process<br>• **process-start**—Process start event type<br>• **process-term**—Process termination event type<br>• **process-user-restart**—Process user restart event type<br>• **process-user-shutdown**—Process user shutdown event type<br>• **snmp**—SNMP event type<br>• **snmp-proxy**—SNMP PROXY event type<br>• **statistics**—Statistics event type<br>• **syslog**—Syslog event type<br>• **timer-absolute**—Absolute timer event type<br>• **timer-countdown**—Countdown timer event type<br>• **timer-cron**—Clock daemon (cron) timer event type<br>• **timer-watchdog**—Watchdog timer event type<br>• **track**—Track event type<br>• **wdsysmon**—Watchdog system monitor event type |
| **system** | (Optional) Displays the registered system policies. |
| **user** | (Optional) Displays the registered user policies. |
| **time-ordered** | (Optional) Displays the policies according to registration time. |
| **name-ordered** | (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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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}
 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 table describes the significant fields displayed in the example.

***Table 9: show event manager policy registered Field Descriptions***

| Field | Description |
|---|---|
| No. | Number of the policy. |

| Field | Description |
|---|---|
| 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. |

# 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 XR EXEC mode.

**show event manager refresh-time**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# show event manager refresh-time
Output:
1800 seconds
```



# Logging Services Commands

This module describes the Cisco IOS XR software commands to configure system logging (syslog) for system monitoring on the router.

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- archive-length, on page 91
- archive-size, on page 92
- clear logging, on page 93
- device, on page 94
- file-size, on page 95
- logging, on page 96
- logging archive, on page 99
- logging buffered, on page 101
- logging console, on page 103
- logging console disable, on page 105
- logging container all, on page 106
- logging events link-status, on page 108
- logging facility, on page 109
- logging file, on page 111
- logging format bsd, on page 114
- logging hostnameprefix, on page 115
- logging source-interface, on page 116
- logging suppress duplicates, on page 117
- logging trap, on page 118
- login-history, on page 119
- process shutdown pam_manager, on page 120
- process start pam_manager, on page 121
- service timestamps, on page 122
- show logging, on page 124
- enable-pam process-monitoring, on page 129
- disable-pam process-monitoring, on page 130
- show pam process-monitoring-status, on page 131
- show syslog persistent status, on page 132

# 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

| | |
|---|---|
| *weeks* | 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 6.0 | 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/RP0/CPU0:router(config)# logging archive
RP/0/RP0/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

| | |
|---|---|
| *size* | 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 6.0 | 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/RP0/CPU0:router(config)# logging archive
RP/0/RP0/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 XR EXEC mode.

**clear logging**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 101 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 124 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/RP0/CPU0:router# clear logging

Clear logging buffer [confirm] [y/n] :y
```

# 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

| | |
|---|---|
| **disk0** | Uses disk0 as the archive device. |
| **disk1** | Uses disk1 as the archive device. |
| **harddisk** | Uses the harddisk as the archive device. |

## Command Default

None

## Command Modes

Logging archive configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)# logging archive
RP/0/RP0/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

| | |
|---|---|
| *size* | 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 6.0 | 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/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# file-size 10
```

# logging

To specify a system logging (syslog) server host as the recipient of syslog messages, use the **logging** command in XR Config 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** *vrf_name* } } { **archive** | **buffered** | **console** | **correlator** | **disable** | **events** | **facility** | **history** | **hostnameprefix** | **localfilesize** | **monitor** | **source-address** | **source-interface** | **suppress** | **trap** | **severity** }
**no logging** { *ip-address hostname* | { **vrf** *vrf_name* } } { **archive** | **buffered** | **console** | **correlator** | **disable** | **events** | **facility** | **history** | **hostnameprefix** | **localfilesize** | **monitor** | **source-address** | **source-interface** | **suppress** | **trap** | **severity** }

## Syntax Description

| | |
|---|---|
| *ip-address* \| *hostname* | IP address or hostname of the host to be used as a syslog server. |
| **vrf** *vrf-name* | Name of the VRF. Maximum length is 32 alphanumeric characters. |
| **archive** | Specifies logging to a persistent device(disk/harddisk). |
| **buffered** | Sets buffered logging parameters. |
| **console** | Sets console logging. |
| **correlator** | Configures properties of the event correlator |
| **disable** | Disables console logging. |
| **events** | Configures event monitoring parameters. |
| **facility** | Modifies message logging facilities. |
| **history** | Sets history logging. |
| **hostnameprefix** | Adds the hostname prefix to messages on servers. |
| **localfilesize** | Sets size of the local log file. |
| **monitor** | Sets monitor logging |
| **source-address** | Specifies source address of the logging host. |
| **source-interface** | Specifies interface for source address in logging transactions. |
| **suppress** | Configures properties for the event suppression. |
| **trap** | Sets trap logging. |
| **severity** | Set severity of messages for particular remote host/vrf. |

| | |
|---|---|
| {**all**\|**none**} [**port** *number*] [**vrf** *name*] | All or no severity logs are logged to the syslog server, respectively.<br>This set of options is added under **severity**.<br>• **port** *number* - For the *number* argument, you can use **default** option or the port number. |

## Command Default

No syslog server hosts are configured as recipients of syslog messages.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |
| Release 7.4.1 | The **all** and **none** keywords were added under the **logging severity** command form. |
| Release 7.10.1 | The **facility** and **source-address** options per remote syslog server were introduced. |

## Usage Guidelines

command form.

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 118 command to limit the messages sent to snmp server.

Amongst other options, **all** and **none** are provided under the **logging severity** command form. If you enable **all** or **none**, all or no severity logs are logged to the syslog server, respectively. This configuration persists even when you enable a specific operator type.

The configurations for **facility** and **source-address** per remote syslog server takes priority over global configuration.

## Examples

This example shows how to log messages to a host named host1:

```
RP/0/RP0/CPU0:router(config)# logging host1

RP/0/RP0/CPU0:router(config)#logging A.B.C.D
  severity  Set severity of  messages for particular remote host/vrf
  vrf       Set VRF option

RP/0/RP0/CPU0:router(config)#logging A.B.C.D
RP/0/RP0/CPU0:router(config)#commit
Wed Nov 14 03:47:58.976 PST
```

```
RP/0/RP0/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.

### Configuration Example for Facility and Source-address Per Remote Syslog Server

This example shows how to configure **facility** and **source-address** per remote syslog server:

```
Router#configure
Router(config)#
Router(config)#logging 209.165.201.1 source-address 209.165.201.2
Router(config)#logging 209.165.201.1 facility local2
Router(config)#commit
```

# logging archive

To configure attributes for archiving syslogs, use the **logging archive** command in XR Config mode. To exit the **logging archive** submode, use the **no** form of this command.

**logging archive**
**no logging archive**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 in the table:

**Note** The configuration attributes must be explicitly configured in order to use the logging archive feature.

*Table 10: Configuring Command Attributes For Archiving Syslogs*

| Command | Range | Description | Recommended Setting |
|---|---|---|---|
| archive-length | <0-4294967295> | Number of weeks | 4 weeks |
| archive-size | <1-2047> | Size in MB | 20 MB |
| device | <disk0 \| disk1 \| harddisk> | Use configured devices as the archive device. | harddisk |
| file-size | <1-2047> | Size in MB | 1 MB |
| frequency | <daily \| weekly> | | daily |
| severity | <alerts \| critical \| debugging \| emergencies \| errors \| informational \| notifications \| warnings> | | informational |

## 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/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# device disk1
```

# logging buffered

To send system logging (syslog) messages to logging buffer, use the **logging buffered** command in XR Config mode. To return to the default, use the **no** form of the **logging buffered** command.

**logging buffered** { *buffer-size* | **alerts** | **critical** | **debugging** | **discriminator** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **entries-count** *count* | **backup-period** }

## Syntax Description

| | |
|---|---|
| *buffer-size* | Size of the buffer, in bytes. Range is 2097152-125000000 bytes. The default is 2097152 bytes. |
| **entries-count** *count* | Specifies the buffer entries-count of syslog messages you want to see. The default value is 2545. The range is 2545-151699. |
| **alerts** | Specifies if any immediate action is needed |
| **critical** | Specifies critical conditions |
| **debugging** | Specifies debugging messages |
| **discriminator** | Sets logging buffer discriminator |
| **emergencies** | Specifies system is unusable |
| **informational** | Specifies informational messages |
| **notifications** | Specifies normal but significant conditions |
| **warnings** | Specifies warning conditions |
| **backup-period** | Sets how often the system flushes buffered syslog messages to persistent storage |

## Command Default

None

## Command Modes

XR Config mode

XR Config Mode

## Command History

| Release | Modification |
|---|---|
| Release 26.3.1 | A new keyword, **backup-period**, was added to the command. |
| Release 7.11.1 | This command was modified to include **entries-count** option. |
| Release 6.0 | This command was introduced. |

## 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 specify the size of the buffer. Use the **logging buffer entries-count** command to specify the count of syslog entries.

If both the **logging buffered** *bytes* and **logging buffered entries-count** commands are present, then the maximum configured value is taken to display the number of system log messages.

## Task ID

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

## Examples

This example shows the configuration for sending syslog messages to the logging buffer:

```
RP/0/RP0/CPU0:router(config)# logging buffered 3000000
```

This example shows how to specify the count of syslog entries.

```
Router# configure
Router(config)# logging buffered entries-count 3000
Router(config)# commit
```

This example shows how often the system flushes buffered syslog messages to persistent storage based on the specified backup period.

```
Router(config)# logging buffered backup-period 30
Router(config)# commit
```

# logging console

To enable logging of system logging (syslog) messages logged to the console by severity level, use the **logging console** command in XR Config 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

| | |
|---|---|
| *severity* | Severity level of messages logged to the console, 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 in the table under the "Usage Guidelines" section. |
| **disable** | Removes the **logging console** 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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** command to display syslog messages stored in the logging 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 the table 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 11: Severity Levels for Messages***

| Level Keywords | Level | Description | Syslog Definition |
|---|---|---|---|
| emergencies | 0 | Unusable system | LOG_EMERG |
| alerts | 1 | Need for immediate action | LOG_ALERT |

| Level Keywords | Level | Description | Syslog Definition |
|---|---|---|---|
| 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 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/RP0/CPU0:router(config)# logging console alerts
```

This example shows how to disable console logging:

```
RP/0/RP0/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/RP0/CPU0:router# no logging console
```

# logging console disable

To disable logging of system logging (syslog) messages logged to the console, use the **logging console disable** command in XR Config mode. To return logging to the default setting, use the **no** form of this command.

**logging consoledisable**
**no logging consoledisable**

## Syntax Description

This command has no keywords or arguments.

## Command Default

By default, logging is enabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)# logging console disable
```

# logging container all

To enable logging of messages from third-party software containers, use the **logging container all** command in XR Config mode. To disable logging messages from third-party containers, use the **no** form of this command.

**logging container all**
**no logging container all**

## Syntax Description

| | |
|---|---|
| **container** | Enables the logging of messages from third-party software containers. |
| **all** | Specifies all running containers in the device. |

## Command Default

By default, logging is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.6.4 | This command was introduced. |

## Usage Guidelines

None.

## Task ID

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

## Examples

This example shows how to enable third-party software container logging and how to view the logs for the third-party software named **docker**:

```
Router(config)# logging container all
Router(config)# commit
Router(config)# do show running-config logging
logging container all\
Router(config)# do show logging | inc DOCKER
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 5 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 148 messages logged

Log Buffer (2097152 bytes):

RP/0/RP0/CPU0:Jul  5 06:56:11.913 UTC: exec[66927]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS :
Successfully authenticated user 'lab' from 'console' on 'con0_RP0_CPU0'
RP/0/RP0/CPU0:Jul  5 06:58:13.053 UTC: config[66985]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Jul  5 06:59:04.775 UTC: ubuntu-1[67232]: %OS-SYSLOG-6-DOCKER_APP :
^[]0;root@c382b2e7bed6: /^Groot@c382b2e7bed6:/# testlog
```

```
RP/0/RP0/CPU0:Jul  5 06:59:04.830 UTC: config[67139]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
 committed by user 'lab'. Use 'show configuration commit changes 1000000012' to view the
changes.
RP/0/RP0/CPU0:Jul  5 06:59:45.028 UTC: config[67139]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Jul  5 06:59:48.552 UTC: run_cmd[67780]: %INFRA-INFRA_MSG-5-RUN_LOGIN : User
 lab logged into shell from con0/RP0/CPU0
RP/0/RP0/CPU0:Jul  5 06:59:56.073 UTC: ubuntu-1[67976]: %OS-SYSLOG-6-DOCKER_APP : testlog-123

RP/0/RP0/CPU0:Jul  5 07:00:12.471 UTC: ubuntu-1[68099]: %OS-SYSLOG-6-DOCKER_APP : testlog-new1

RP/0/RP0/CPU0:Jul  5 07:01:55.747 UTC: ubuntu-1[68245]: %OS-SYSLOG-6-DOCKER_APP : testlog-new1

RP/0/RP0/CPU0:Jul  5 07:02:02.869 UTC: run_cmd[67780]: %INFRA-INFRA_MSG-5-RUN_LOGOUT : User
 lab logged out of shell from con0/RP0/CPU0
```

# 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 XR Config 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

| | |
|---|---|
| **disable** | Disables the logging of link-status messages for all interfaces, including physical links. |
| **software-interfaces** | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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.

When you administratively shut down the parent bundle interface, the system generates Admin Down syslog messages for the main bundle interface but does not generate them for its subinterfaces.

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.

## 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/RP0/CPU0:router(config)# logging events link-status disable
```

# 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 XR Config 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 1 in the "Usage Guidelines" section. |

## Command Default

*type*: **local7**

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

This table describes the acceptable options for the *type* argument.

***Table 12: 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 |
| 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 |

| Facility Type | Description |
|---|---|
| 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 #unique_73 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/RP0/CPU0:router(config)# logging facility kern
```

# logging file

To specify the file to store system logs on the router, use the **logging file** command in XR Config Mode.

**logging file** *filename* **path** *pathname* [ **local-accounting** [ **maxfilesize** *max-file-size* | **severity** *severity* | **send-to-remote** **facility** *facility-type* ] ]

## Syntax Description

| | |
|---|---|
| *filename* | Specifies the filename of the log file. |
| **path** *pathname* | Specifies the location to save the logging file. |
| **local-accounting** | (optional) Enables the storage of the AAA command-accounting logs directly on the router, in the file specified in *pathname* |
| **maxfilesize** *max-file-size* | (optional) Specifies the maximum file size of the logging file in bytes. Range is from 1 to 2097152 (in KB). Default is 2 GB. |
| **severity** *severity* | (optional) Specifies the severity level for the logging file. Default is informational.<br>• alerts - Immediate action needed (severity=1)<br>• critical - Critical conditions (severity=2)<br>• debugging - Debugging messages (severity=7)<br>• emergencies - System is unusable (severity=0)<br>• errors - Error conditions (severity=3)<br>• informational - Informational messages (severity=6)<br>• notifications - Normal but significant conditions (severity=5)<br>• warnings - Warning conditions (severity=4) |
| **send-to-remote** | (optional) Enables the command accounting logs to be sent to the syslog server |
| **facility** *facility-type* | (optional) Specifies the facility from which the command accounting logs are generated. Facility is the identifier used by the remote logging server to identify the application or process that generated the log message. The available facility-types are listed under **Usage Guidelines**. |

## Command Default

This feature is disabled by default.

## Command Modes

XR Config Mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |
| Release 7.4.1 | The **local-accounting** option is introduced. |

## Usage Guidelines

If the logs generated exceeds the maximum file size, then the router over-writes the existing file contents.

The following table describes the available options for *facility-type*:

***Table 13: Facility Types***

| 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 |
| 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 |

**Task ID**

| Task ID | Operation |
|---|---|
| logging | read, write |

### Example

This example shows how to enable local command accounting after configuring the AAA command accounting feature:

```
Router#conf t
Router(config)#aaa accounting commands default start-stop group tacacs+ local
Router(config)#logging file cmdacctfile path /disk0: maxfilesize 1024 severity info
local-accounting send-to-remote facility local7
Router(config)#commit
```

# logging format bsd

To send system logging messages to a remote server in Berkeley Software Distribution (BSD) format, use the **logging format bsd** command in XR Config mode. To return console logging to the default setting, use the **no** form of this command.

**logging format bsd**

## Syntax Description

| | |
|---|---|
| **format** | Specifies the format of the syslog messages sent to the server. |
| **bsd** | Configures the format of the syslog messages according to the BSD format. |

## Command Default

By default, this feature is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.2 | This command was introduced. |

## Usage Guidelines

None.

## Task ID

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

## Examples

This example shows how to log messages to a server, in the BSD format:

```
Router(config)#logging 209.165.200.225 vrf default severity info
Router(config)#logging format bsd
Router(config)#commit

Router(config)#do show run logging
logging format bsd
logging 209.165.200.225 vrf default severity info
```

# logging hostnameprefix

To append a hostname prefix to system logging (syslog) messages logged to syslog servers, use the **logging hostnameprefix** command in XR Config 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

| | |
|---|---|
| *hostname* | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 #unique_73 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/RP0/CPU0:router(config)# logging hostnameprefix host1
```

# 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 XR Config 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

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark (**?**) online help function. |
| *interface-path-id* | Physical interface or virtual interface.<br>**Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br>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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 #unique_73 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 HundredGigE interface 0/1/0/0 be set as the source IP address for all messages:

```
RP/0/RP0/CPU0:router(config)# logging source-interface HundredGigE interface 0/1/0/0
```

# 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 XR Config 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)# logging suppress duplicates
```

# logging trap

To specify the severity level of messages logged to snmp server, use the **logging trap** command in XR Config 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 1 in the "Usage Guidelines" section for the **logging buffered** command. |

## Command Default

*severity*: **informational**

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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.

#unique_61 unique_61_Connect_42_tab_1365648 under the "Usage Guidelines" section for the logging buffered, on page 101 command lists the syslog definitions that correspond to the debugging message levels.

Use the #unique_73 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/RP0/CPU0:router(config)# logging trap notifications
```

# login-history

To enable the display of the login banner in compliance with US DoD login notification requirements, use the **login-history enable** command in the XR Config mode. To disable the display of the login banner, use the **login-history disable** command in the XR Config mode.

**login-history** { **enable** | **disable** }

## Command Default

The display of the login banner is not enabled.

## Command History

| Release | Modification |
|---|---|
| Release 7.3.1 | This command was introduced. |

## Task ID

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

## Examples

This example shows how to enable and disable the display of the login banner in compliance with the US DoD login notification requirements:

```
Router(config-un)# login-history enable
Router(config-un)# login-history disable
```

If you enable the login banner, you can display the login notification banner that conforms to the US (DOD) requirements:

```
Username: user1
Password:
User root : login failed 2 time(s) successful 5 time(s).
Most recent Failure Thu Mar 19 2020 21:12:00 UTC
to con0_RP0_CPU0 from console

User user1 last logged in successfully Thu Mar 19 2020 21:11:50 UTC
to con0_RP0_CPU0 from console
```

# process shutdown pam_manager

To disable platform automated monitoring (PAM) by shutting down the required process agents, use the **process shutdown pam_manager** command in XR EXEC mode.

**process shutdown pam_manager** [**location** {*node-id* | **all**}]

## Syntax Description

| | |
|---|---|
| **location all** | Disables PAM agents for all RPs. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.1.2 | This command was introduced. |

## Usage Guidelines

Because PAM tool process (pam_manager) is not a mandatory process, it does not restart automatically if it was manually disabled (unless in the case of a system reload). You can re-enable PAM using the **process start pam_manager** command.

If you use **process shutdown pam_manager** without any keywords, it disables PAM agents for the local RP.

## Task ID

| Task ID | Operation |
|---|---|
| network | read, write |

This example shows how to disable PAM for all RPs:

```
RP/0/RP0/CPU0:router# process shutdown pam_manager location all
```

## Related Commands

| Command | Description |
|---|---|
| process start pam_manager, on page 121 | Re-enables platform automated monitoring (PAM) by restarting the required process agents. |

# process start pam_manager

To re-enable platform automated monitoring (PAM) by restarting the required process agents, use the **process start pam_manager** command in XR EXEC mode.

**process start pam_manager** [**location** {*node-id* | **all**}]

## Syntax Description

| | |
|---|---|
| **location all** | Restarts PAM agents for all RPs. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.1.2 | This command was introduced. |

## Usage Guidelines

If you use **process start pam_manager** without any keywords, it restarts PAM agents for the local RP.

You can use these commands to check if PAM is installed in the router:

- **show processes pam_manager location all** (from Cisco IOS XR command line interface):
- **run ps auxw | egrep perl** (from router shell prompt)

## Task ID

| Task ID | Operation |
|---|---|
| network | read, write |

This example shows how to re-enable PAM for all RPs:

```
RP/0/RP0/CPU0:router# process start pam_manager location all
```

## Related Commands

| Command | Description |
|---|---|
| process shutdown pam_manager, on page 120 | |

# service timestamps

To modify the time-stamp format for system logging (syslog) and debug messages, use the **service timestamps** command in XR Config mode. To revert to the default timestamp format, use the **no** form of this command.

**service timestamps** [[**debug**|**log**] {**datetime** [**localtime**] [**msec**] [**show-timezone**] |**disable**|**uptime**}]
**no service timestamps** [[**debug**|**log**] {**datetime** [**localtime**] [**msec**] [**show-timezone**] |**disable**|**uptime**}]

## Syntax Description

| | |
|---|---|
| **debug** | (Optional) Specifies the time-stamp format for debugging messages. |
| **log** | (Optional) Specifies the time-stamp format for syslog messages. |
| **datetime** | (Optional) Specifies that syslog messages are time-stamped with date and time. |
| **localtime** | (Optional) When used with the **datetime** keyword, includes the local time zone in time stamps. |
| **msec** | (Optional) When used with the **datetime** keyword, includes milliseconds in the time stamp. |
| **show-timezone** | (Optional) When used with the **datetime** keyword, includes time zone information in the time stamp. |
| **disable** | (Optional) Causes messages to be time-stamped in the default format. |
| **uptime** | (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 log datetime localtime** and **service timestamps debug datetime localtime** forms of the command with no additional keywords is to format the time in the local time zone, without milliseconds and time zone information.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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/RP0/CPU0:router(config)# service timestamps log datetime localtime show-timezone
```

# show logging

To display the contents of the logging buffer, use the **show logging** command in XR EXEC mode.

**show logging** [[**alarm-location location** *location*] | [**correlator** *options*] | **local location** *node-id* | [**location** *node-id*] [**start** *month day hh* **:** *mm* **:** *ss*] [**process** *name*] [**string** *string*] [**end** *month day hh* **:** *mm* **:ss**][**events** *options*][**history**][**last** *entries*][**suppress rule** {*rule_name* | **all**}]]

## Syntax Description

| | |
|---|---|
| **alarm-location trace** *location* | (Optional) Displays the alarm-location information. The **trace** option shows trace data for the alarm location components. |
| **correlator***options* | (Optional) Displays the content and information about correlation buffer. The various options available are:<br>• buffer: Displays the content of the correlation buffer.<br>• info: Displays information about event correlation.<br>• trace: Displays trace data for the alarm_logger component. |

| | |
|---|---|
| **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.<br>The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are as follows:<br>• *month*—The month of the year. The values for the *month* argument are:<br>• january<br>• february<br>• march<br>• april<br>• may<br>• june<br>• july<br>• august<br>• september<br>• october<br>• november<br>• december<br>• *day*—Day of the month. Range is 01 to 31.<br>• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.<br>• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.<br>• *ss*—Seconds. Range is 00 to 59. |
| **events** *options* | Displays the content and information about event buffer.The various options available are:<br>• buffer: Displays the content of the event buffer.<br>• info: Displays information about events buffer.<br>• rule: Displays specified rules.<br>• ruleset: Displays rulesets.<br>• trace: Displays trace data for the correlation component. |
| **history** | Displays the contents of logging history. |
| **last** *entries* | Displays last <n> entries. The number of entries can range from 1 to 500. |

| | |
|---|---|
| **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/modul e* notation. |
| **location** *node-id* | (Optional) Displays syslog messages from the designated node. The *node-id* argument is entered in the *rack/slot/modul e* notation. |
| **start** *month day hh* **:** *mm* **:** *ss* | (Optional) Displays syslog messages with a time stamp equal to or higher than the time stamp specified with the *month day mm* **:** *hh* **:** *ss* argument.<br>The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are as follows:<br>• *month*—The month of the year. The values for the *month* argument are:<br>• january<br>• february<br>• march<br>• april<br>• may<br>• june<br>• july<br>• august<br>• september<br>• october<br>• november<br>• december<br>• *day*—Day of the month. Range is 01 to 31.<br>• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.<br>• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.<br>• *ss*—Seconds. Range is 00 to 59. |
| **process** *name* | (Optional) Displays syslog messages related to the specified process. |
| **string** *string* | (Optional) Displays syslog messages that contain the specified string. |
| **suppress rule**{*rule_name*\|**all**} | Displays the content and information about log suppression. The **rule** option shows specified rules. |

**Command Default** None

**Command Modes** XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 **process***name* keyword argument pair and **location** *node-id* keyword argument pair. Syslog messages related to the “init” process emitted from node 0/RP0/CPU0 are displayed in the sample output.

```
RP/0/RP0/CPU0:router# show logging process init location 0/RP0/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 14: 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.” |

# enable-pam process-monitoring

To detect the blocked processes on all nodes in the system, use the **enable-pam process-monitoring** command in EXEC mode to enable the Platform Automated Monitoring process blockage monitoring feature.

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.5.2 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, it automatically collects logs and saves these logs (along with the core file in applicable cases) as a *.tgz* file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/ directory`. PAM also generates a system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

## Task ID

| Task ID | Operations |
|---|---|
| monitor | read |
| basic-services or cisco-support | read |

## Examples

```
Router# enable-pam process-monitoring
PAM "Monitoring Process Blockage" Feature is enabled
```

# disable-pam process-monitoring

To disable the Platform Automated Monitoring process blockage monitoring feature, use the **disable-pam process-monitoring** command in EXEC mode. To re-enable the feature, use the **enable** form of this command.

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.5.2 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, it automatically collects logs and saves these logs (along with the core file in applicable cases) as a *.tgz* file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/ directory`. PAM also generates a system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

## Task ID

| Task ID | Operations |
|---|---|
| monitor | read |
| basic-services or cisco-support | read |

## Examples

```
Router# disable-pam process-monitoring
PAM "Monitoring Process Blockage" Feature has been disabled
```

# show pam process-monitoring-status

To see if the Platform Automated Monitoring (PAM) process blockage monitoring is enabled or disabled, use the **show pam process-monitoring-status** command in EXEC mode.

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.5.2 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, it automatically collects logs and saves these logs (along with the core file in applicable cases) as a *.tgz* file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/ directory`. PAM also generates a system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

## Task ID

| Task ID | Operations |
|---|---|
| monitor | read |
| basic-services or cisco-support | read |

## Examples

```
Router# show pam process-monitoring-status
PAM "Monitoring Process Blockage" Feature is disabled
```

# show syslog persistent status

To display the status of persistent logging buffers, use the **show syslog persistent status** command in EXEC mode.

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 26.3.1 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| cisco-support | read |

## Examples

This example shows the status of persistent logging file details.

```
Router# show syslog persistent status
Thu Aug 6 11:14:32.464 UTC
node: node0_RP0_CPU0
Persistent file details:
Filename: /var/log/xr_syslog/persistent/messages.log
Maximum Size: 2731 messages (2097432 bytes)
Message Write Index: 260 messages (199704 bytes)
Dropped Messages: 0
Invalid Messages: 14
No of Wraps: 0
Backup Period: 10000 milliseconds
```



# Onboard Failure Logging Commands

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

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, and environmental factors 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.

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

**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 *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.

- show logging onboard, on page 135

# show logging onboard

To display the onboard failure logging (OBFL) messages, use the **show logging onboard** command in System Admin EXEC mode.

**show logging onboard** {**diag_log** | **diag_result** | **fabric** | **fmea** | **fpd** | **inventory** | **temperature** | **uptime** | **voltage**}[**location** *node-id*] [**verbose**]

## Syntax Description

| | |
|---|---|
| **diag_log** | Displays the OBFL diag logs data information. |
| **diag_result** | Displays the OBFL diag test results information. |
| **fabric** | Displays the OBFL fabric data information. |
| **fmea** | Displays the OBFL FMEA data information. |
| **fpd** | Displays the OBFL FPD data information. |
| **inventory** | Displays the OBFL inventory data information. |
| **temperature** | Displays temperature information. |
| **uptime** | Displays the OBFL uptime. |
| **voltage** | Displays voltage information. |

## Command Default

None

## Command Modes

System Admin EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 keyword.

Use the **location** *node-id* keyword and argument to display OBFL messages for a specific node.

## Task ID

| Task ID | Operations |
|---|---|
| logging | read |

## Examples

This example displays uptime information from the OBFL feature:

```
sysadmin-vm:0_RP0# show logging onboard uptime location 0/7
```



# 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.

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D



**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

For detailed information about performance management concepts, configuration tasks, and examples, see the *Implementing Performance Management* module in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- monitor interface, on page 139
- performance-mgmt apply monitor, on page 146
- performance-mgmt apply statistics, on page 149
- performance-mgmt apply thresholds, on page 152
- performance-mgmt regular-expression, on page 154
- performance-mgmt resources dump local, on page 155
- performance-mgmt resources memory, on page 156
- performance-mgmt resources tftp-server, on page 157
- performance-mgmt statistics, on page 159
- performance-mgmt thresholds, on page 161
- show performance-mgmt bgp, on page 170
- show performance-mgmt interface , on page 172
- show performance-mgmt mpls, on page 175
- show performance-mgmt node, on page 177
- show performance-mgmt ospf, on page 179
- show health sysdb, on page 181
- show running performance-mgmt, on page 183

# monitor interface

To monitor interface counters in real time, use the **monitor interface** command in XR EXEC mode or System Admin EXEC mode.

**monitor interface** [ *type1 interface-path-id1* [ . . . [ *type32 interface-path-id32* ] ] [ *wide* ] [ *full-name* ] [ *filter physical* ] ]

## Syntax Description

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark ( **?** ) online help function. |
| *interface-path-id* | Physical interface or virtual interface.<br>**Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br>For more information about the syntax for the router, use the question mark ( **?** ) online help function. |
| *wide* | Display detailed statistics of the interfaces. |
| *full-name* | Display full name of the interfaces.<br>For more information, use the question mark ( **?** ) online help function. |
| *filter physical* | Filters the output to display only physical interface. |

## Command Default

Use the **monitor interface** command without an argument to display statistics for all interfaces in the system.

## Command History

| Release | Modification |
|---|---|
| Release 24.4.1 | This command was modified to introduce the *filter physical* keyword.<br>New columns InDrops and OutDrops are added to the output. |
| Release 7.5.4 | The argument *full-name* was introduced. |
| Release 7.0.12 | This command was introduced. |

## Usage Guidelines

The argument *full-name* is applicable only for Release 7.5.4

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**

To display more than one selected interface, enter the **monitor interface** command with multiple *type interface-path-id* arguments. For example: **monitor interface**

To display a range of interfaces, enter the **monitor interface** command with a wildcard. For example: **monitor**

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.

Use the **monitor interface** command with the *wide* argument to display detailed statistics of the interfaces. For example: **monitor interface** *HundredGigE0/0/0/0 HundredGigE0/0/0/1 HundredGigE0/0/0/2 wide*

Use the **monitor interface** command with the *full-name* argument to display full name of the interfaces. Full name is more useful especially for Named interfaces, which has large character lengths. For example: **monitor interface** *HundredGigE0/0/0/0 HundredGigE0/0/0/1 tunnel-te FROM-INDBGL-AAA-TO-USASJC-BBB-TO-CANAD-CCC full-name*

Use the **monitor interface** command with the *wide* and *full-name* arguments to display detailed statistics of the interfaces with its full name. For example: **monitor interface** *HundredGigE0/0/0/0 HundredGigE0/0/0/1 tunnel-te FROM-INDBGL-AAA-TO-USASJC-BBB-TO-CANAD-CCC wide full-name*

From Release 24.4.1 onwards, new columns InDrops and OutDrops are displayed in the **monitor interface** command output.

***Table 15: Interactive Commands Available for the monitor interface Command (Functional Summary)***

| Command | Description |
|---|---|
| **Use the following keys to suspend or resume the counter refresh:** | |
| **f** | Freezes the display screen, thereby suspending the display of fresh counters. |
| **t** | Thaws the display screen, thereby resuming the display of fresh counters. |
| **Use the following key to reset the counters:** | |
| **c** | Resets interface counters to 0. |
| **Use the following keys when displaying statistics for a single interface. These keys display counters in normal or detailed view**. | |
| **d** | Changes the display mode for the interface monitoring session to display detailed counters. Use the **b** interactive command to return to the regular display mode. |
| **r** | Displays the protocol divided by IPv4 or IPv6, and multicast and unicast. When the statistics are displayed using the **r** option, you can also use the **k**, **y**, or **o** keys to display statistics in packets ("**k**"), bytes("**y**") or packets and ("**o**"). |
| **b** | Returns the interface monitoring session to the regular display mode for counters. Statistics are not divided by protocol. |
| 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.** | |

| | |
|---|---|
| **k** | Displays statistics in packets ("**k**"). |
| **y** | (Default) Displays statistics in bytes ("**y**"). |
| **o** | Displays statistics in both bytes and packets ("**o**"). |
| **Use the following keys to display statistics for a different interface:** | |
| **i** | Enables you to jump to a nonsequential interface. You are prompted to enter the interface type and interface path ID to be monitored. |
| **p** | Displays the previous sequential interface in the list of available interfaces. |
| **n** | Displays the next sequential interface in the list of available interfaces. |
| **q** | 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 HundredGigE interface, enter the command and wildcard **monitor interface HundredGigE *** .
- To display statistics for three specified interfaces, enter the command **monitor interface HundredGigE 0/0/0/0 HundredGigE 0/0/0/1 HundredGigE 0/0/0/0** .

This is the sample output for the **monitor interface** command entered without an argument. This command displays statistics for all interfaces in the system.

Before Release 24.4.1, the following output is displayed.

```
Router# monitor interface
Fri Aug 23 14:47:13.474 UTC
Protocol:General
Interface             In(bps)       Out(bps)      InBytes/Delta  OutBytes/Delta
Fo0/0/0/0              1.7M/  0%    740000/  0%    89.3M/0          37.2M/0
Fo0/0/0/1                 0/  0%         0/  0%        0/0              0/0
Mg0/RSP0/CPU0/0           0/  0%         0/  0%   764213/0           7686/0
Mg0/RSP1/CPU0/0           0/  0%         0/  0%   752405/0              0/0
Te0/0/1/0              1.7M/  0%      1.7M/  0%    89.3M/0          88.9M/0
Te0/0/1/1                 0/  0%         0/  0%        0/0              0/0
Te0/0/1/10                0/  0%         0/  0%        0/0              0/0
Te0/0/1/11                0/  0%         0/  0%        0/0              0/0
Te0/0/1/12                0/  0%         0/  0%        0/0              0/0
Te0/0/1/13                0/  0%         0/  0%        0/0              0/0
```

```
Te0/0/1/14                0/  0%        0/  0%        0/0             0/0
Te0/0/1/15                0/  0%        0/  0%        0/0             0/0
Te0/0/1/16                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')
```

From Release 24.4.1 onwards, new columns InDrops and OutDrops are added to the output. The new columns are displayed for all **monitor interface** command outputs.

```
Router# monitor interface
Fri Aug 23 14:47:13.474 UTC
Monitor Time: 00:00:00          SysUptime: 04:26:12
Protocol:General
Interface       In(bps)   Out(bps)    InBytes/Delta  OutBytes/Delta  InDrops/Delta
OutDrops/Delta
Fo0/0/0/0       1.7M/ 0%  740000/ 0%  89.3M/0        37.2M/0          1511/0
 26502/0
Fo0/0/0/1       0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Mg0/RSP0/CPU0/0 0/ 0%     0/  0%      764213/0       7686/0           0/0
 0/0
Mg0/RSP1/CPU0/0 0/ 0%     0/  0%      752405/0        0/0             0/0
 0/0
Te0/0/1/0       1.7M/ 0%  1.7M/ 0%    89.3M/0        88.9M/0         12044/0
 0/0
Te0/0/1/1       0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/10      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/11      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/12      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/13      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/14      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/15      0/ 0%     0/ 0%        0/0            0/0             0/0
 0/0
Te0/0/1/16      0/ 0%     0/ 0%        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')
```

This is the sample output for the **monitor interface** command entered with single *type interface-path-id* argument. This command displays statistics for the entered single interface.

```
Router# monitor interface hundredGigE 0/0/0/0 hundredGigE 0/0/0/1
Mon Sep 2 21:18:02.547 UTC

ios Monitor Time: 00:00:02 SysUptime: 93:53:03

Protocol:General
Interface In(bps) Out(bps) InBytes/Delta OutBytes/Delta InDrops/Delta OutDrops/Delta
Hu0/0/0/0  0/ 0%    0/ 0%      0/0           0/0              0/0            0/0
Hu0/0/0/1  0/ 0%    0/ 0%      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')
```

This is the sample output for the **monitor interface** command entered with multiple *type interface-path-id* arguments. This command displays statistics for all entered interfaces.

```
Router# monitor interface fourHundredGigE 0/0/0/0  fourHundredGigE 0/0/0/1 tunnel-te
FROM-BGL-AA-BB-TO-SJC-CC-DD-1 tunnel-te FROM-BGL-AA-BB-TO-SJC-CC-DD-2
 Mon Jan 16 11:11:03.775 UTC

 R1                   Monitor Time: 00:00:12          SysUptime: 00:45:03

 Protocol:General
 Interface            In(bps)      Out(bps)     InBytes/Delta  OutBytes/Delta  InDrops/Delta
 OutDrops/Delta
 FH0/0/0/0                 0/  0%         0/  0%         0/0             0/0        0/0
     0/0
 FH0/0/0/1                 0/  0%         0/  0%         0/0             0/0        0/0
     0/0
 FROM-BGL-AA-              0/ --%         0/ --%         0/0             0/0        0/0
     0/0
 FROM-BGL-AA-              0/ --%         0/ --%         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')
```

This is the sample output for the **monitor interface** command entered with *type interface-path-id* and *wide* arguments. This command displays detailed statistics of the interfaces.

```
Router# monitor interface fourHundredGigE 0/0/0/0  fourHundredGigE 0/0/0/1 tunnel-te
FROM-BGL-AA-BB-TO-SJC-CC-DD-1 tunnel-te FROM-BGL-AA-BB-TO-SJC-CC-DD-2 wide
 Mon Jan 16 11:12:48.388 UTC

 R1                   Monitor Time: 00:00:04          SysUptime: 00:46:40

 Protocol:General
 Interface             In(bps)      Out(bps)     InBytes/Delta  OutBytes/Delta  ErrIn/Delta
  ErrCRC/Delta  ErrFr/Delta   ErrOvr/Delta   ErrOut/Delta   ErrUnd/Delta
 FH0/0/0/0                 0/  0%         0/  0%         0/0             0/0            0/0
         0/0           0/0           0/0         0/0           0/0
 FH0/0/0/1                 0/  0%         0/  0%         0/0             0/0            0/0
         0/0           0/0           0/0         0/0           0/0
 FROM-BGL-AA-              0/ --%         0/ --%         0/0             0/0            0/0
         0/0           0/0           0/0         0/0           0/0
 FROM-BGL-AA-              0/ --%         0/ --%         0/0             0/0            0/0
         0/0           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')
```

This is the sample output for the **monitor interface** command entered with *full-name* argument. This command displays statistics of all interfaces in the system with their full name.

```
Router# monitor interface full-name
Fri Aug 23 14:50:22.970 UTC
Monitor Time: 00:00:00          SysUptime: 04:29:21
Protocol:General
In(bps)  Out(bps)  InBytes/Delta  OutBytes/Delta  InDrops/Delta  OutDrops/Delta  Interface
2.7M/ 0% 1.1M/ 0%  88.6M/0        36.9M/0          0/0            26479/0
FortyGigE0/0/0/0
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
FortyGigE0/0/0/1
0/ 0%    0/ 0%     7397/0         42/0             0/0            0/0
MgmtEth0/RSP0/CPU0/0
```

```
0/ 0%    0/ 0%     7337/0          0/0             0/0            0/0
MgmtEth0/RSP1/CPU0/0
2.7M/ 0% 2.7M/ 0%  88.6M/0        88.6M/0         10527/0        0/0
TenGigE0/0/1/0
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/1
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/10
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/11
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/12
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/13
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/14
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/15
0/ 0%    0/ 0%      0/0            0/0             0/0            0/0
TenGigE0/0/1/16

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 the **monitor interface** command entered with the *type interface-path-id* and *full-name* arguments. This command displays statistics of the interfaces with their full name.

```
Router# monitor interface fourHundredGigE 0/0/0/0  fourHundredGigE 0/0/0/1 tunnel-te
FROM-BGL-AA-BB-TO-SJC-CC-DD-1 tunnel-te FROM-BGL-AA-BB-TO-SJC-CC-DD-2 full-name
 Mon Jan 16 11:16:30.346 UTC

 R1                   Monitor Time: 00:00:04          SysUptime: 00:50:22

 Protocol:General
 In(bps)      Out(bps)     InBytes/Delta  OutBytes/Delta  InDrops/Delta OutDrops/Delta
Interface
 0/  0%        0/  0%        0/0             0/0            0/0           0/0
 FourHundredGigE0/0/0/0
 0/  0%        0/  0%        0/0             0/0            0/0           0/0
 FourHundredGigE0/0/0/1
 0/ --%        0/ --%        0/0             0/0            0/0           0/0
 FROM-BGL-AA-BB-TO-SJC-CC-DD-1
 0/ --%        0/ --%        0/0             0/0            0/0           0/0
 FROM-BGL-AA-BB-TO-SJC-CC-DD-2

 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 the **monitor interface** command entered with the *type interface-path-id wide* and *full-name* arguments. This command displays detailed statistics of the interfaces with their full name.

```
Router# monitor interface HundredGigE 0/0/0/0 HundredGigE0/0/0/1 tunnel-te
FROM-BGL-AA-BB-TO-SJC-CC-DD-1 tunnel-te FROM-BGL-AA-BB-TO-SJC-CC-DD-2 wide full-name
Mon Sep 2 22:34:17.826 UTC
ios Monitor Time: 00:00:02 SysUptime: 95:09:18

Protocol:General
In(bps) Out(bps) InBytes/Delta OutBytes/Delta InDrops/Delta OutDrops/Delta ErrIn/Delta
ErrCRC/Delta ErrFr/Delta ErrOvr/Delta ErrOut/Delta ErrUnd/Delta
Interface : HundredGigE0/0/0/0
0/ 0%   0/ 0%    0/0            0/0                0/0         0/0          0/0
```

```
0/0          0/0        0/0           0/0          0/0
Interface : HundredGigE0/0/0/1
0/ 0%   0/ 0%    0/0           0/0                 0/0         0/0          0/0
0/0          0/0        0/0           0/0          0/0
Interface : FROM-BGL-AA-BB-TO-SJC-CC-DD-1
0/ --%   0/ 0%    0/0           0/0                   0/0         0/0         0/0
0/0          0/0        0/0           0/0          0/0
Interface : FROM-BGL-AA-BB-TO-SJC-CC-DD-2
0/ --%   0/ 0%    0/0           0/0                   0/0         0/0         0/0
0/0          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')
```

From Release 24.4.1 onwards, you can use the *filter physical* keyword with the **monitor interface** command, to filter the output to display details of only the physical interfaces.

```
Router# monitor interface filter physical
Fri Aug 23 15:18:16.185 UTC
Monitor Time: 00:00:00          SysUptime: 04:57:14
Protocol:General
Interface       In(bps)  Out(bps) InBytes/Delta OutBytes/Delta InDrops/Delta OutDrops/Delta
Fo0/0/0/0        3.6M/ 0% 1.5M/ 0% 88.5M/0       36.9M/0         0/0           26456/0
Fo0/0/0/1        0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Mg0/RSP0/CPU0/0  0/ 0%    0/ 0%    7817/0        42/0            0/0             0/0
Mg0/RSP1/CPU0/0  0/ 0%    0/ 0%    7757/0        0/0             0/0             0/0
Te0/0/1/0        3.6M/ 0% 3.6M/ 0% 88.5M/0       88.5M/0         10518/0         0/0
Te0/0/1/1        0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/10       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/11       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/12       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/13       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/14       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/15       0/ 0%    0/ 0%    0/0           0/0             0/0             0/0
Te0/0/1/16       0/ 0%    0/ 0%    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')
```

# 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 XR Config 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

| | |
|---|---|
| *entity* | Specifies an entity for which you want to apply the statistics template:<br>• **bgp**—Applies a template for monitoring a Border Gateway Protocol (BGP) neighbor.<br>• **interface basic-counters**—Applies a template for monitoring basic counters on an interface. If you enter this keyword, supply values for the *type* and *interface-path-id* arguments.<br>• **interface data-rates**—Applies a template for monitoring data rates on an interface. If you enter this keyword, supply values for the *type* and *interface-path-id* arguments.<br>• **interface generic-counters**—Applies a template for monitoring generic counters on an interface. If you enter this keyword, supply values for the *type* and *interface-path-id* arguments.<br>• **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.<br>• **node cpu**—Applies a template for monitoring the central processing unit (CPU) on a node. Use the *node-id* argument with this entity.<br>• **node memory** —Applies a template for monitoring memory utilization on a node. Use the **location** keyword and *node-id* argument with this entity.<br>• **node process**—Applies a template for monitoring a process on a node. Use the *node-id* and *process-id* arguments with this entity.<br>• **ospf v2protocol**—Applies a template for monitoring an Open Shortest Path First v2 (OSPFv2) process instance.<br>• **ospf v3protocol**—Applies a template for monitoring an OSPFv3 process instance. |
| *ip-address* | IP or neighbor address. Used with the **bgp** or **ldp** keyword. |
| *type* | Interface type. For more information, use the question mark (**?**) online help function. |
| *interface-path-id* | Physical interface or virtual interface.<br>**Note**<br>Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br><br>For more information about the syntax for the router, use the question mark (**?**) online help function. |
| *node-id* | Designated node. Used with the **node cpu** or **node memory** keyword. The *node-id* argument is entered in the *rack/slot/module* notation. |

| | |
|---|---|
| *node-id process-id* | Designated node and process ID. Used with the **node process** keyword. The *node-id* argument is entered in the *rack/slot/module* notation. |
| *process-name* | Process name of the OSPF instance. Used with the **ospfv2protocol** and **ospfv3protocol** keywords. |
| *template-name* | 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 **show running performance-mgmt** command to display a list of available templates. |
| **default** | Applies the default template. |

## Command Default

Monitoring is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 149 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/RP0/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/RP0/CPU0:router(config)#performance-mgmt apply monitor interface data-rates hundredGigE
 0/2/0/0 default
```

This example shows how to enable memory monitoring based on the criterion set in the default template:

```
RP/0/RP0/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/RP0/CPU0:router(config)#performance-mgmt apply monitor interface basic-counters
hundredGigE 0/2/0/0 default
```

# performance-mgmt apply statistics

To apply a statistics template and enable statistics collection, use the **performance-mgmt apply statistics** command in XR Config 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

| | |
|---|---|
| *entity* | Specifies an entity for which you want to apply a statistics template:<br>• **bgp**—Applies a statistics collection template for Border Gateway Protocol (BGP).<br>• **interface basic-counters**—Applies a statistics collection template for basic counters.<br>• **interface data-rates**—Applies a statistics collection template for data rates.<br>• **interface generic-counters**—Applies a statistics collection template for generic counters.<br>• **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.<br>• **node cpu**—Applies a statistics collection template for the central processing unit (CPU). Use the **location** keyword with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **node memory**—Applies a statistics collection template for memory utilization. Use the **location** keyword with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **node process**—Applies a statistics collection template for processes. Use the **location** keyword with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **ospf v2protocol**—Applies a statistics collection template for Open Shortest Path First v2 (OSPFv2) process instances.<br>• **ospf v3protocol**—Applies a statistics collection template for OSPFv3 process instances. |
| **location** {**all** \| *node-id*} | Specifies all nodes or a particular node.<br>Specify the **location all** keywords for all nodes, or the *node-id* argument to specify a particular node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation. You must specify either the **location all** keywords or the **location** keyword and *node-id* argument with the **node cpu**, **node memory**, or **node process** entity. |
| *template-name* | 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 show running performance-mgmt, on page 183 command to display a list of available templates. |
| **default** | Applies the default template. |

## Command Default

Statistics collection is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 157 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 146 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 159 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/RP0/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/RP0/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/RP0/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:

```
RP/0/RP0/CPU0:router(config)#performance-mgmt apply statistics interface basic-counters
default
```

# performance-mgmt apply thresholds

To apply a thresholds template and enable threshold collection, use the **performance-mgmt apply thresholds** command in XR Config 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

| | |
|---|---|
| *entity* | Specifies an entity for which you want to apply a threshold template:<br>• **bgp**—Applies a threshold monitoring template for Border Gateway Protocol (BGP).<br>• **interface basic-counters**—Applies a threshold monitoring template for basic counters.<br>• **interface data-rates**—Applies a threshold monitoring template for data rates.<br>• **interface generic-counters**—Applies a threshold monitoring template for generic counters.<br>• **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.<br>• **node cpu**—Applies a threshold monitoring template for central processing unit (CPU) utilization. Use the **location** keyword in conjugation with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **node memory**—Applies a threshold monitoring template for memory utilization. Use the **location** keyword in conjugation with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **node process**—Applies a threshold monitoring template for processes. Use the **location** keyword in conjugation with the **all** keyword or *node-id* argument when enabling a statistics collection template for this entity.<br>• **ospf v2protocol**—Applies a threshold monitoring template for OSPFv2.<br>• **ospf v3protocol**—Applies a threshold monitoring template for OSPFv3. |
| **location** {**all** \| *node-id*} | Specifies all nodes or a particular node.<br>Specify the **location all** keywords for all nodes, or the *node-id* argument to specify a particular node. The *node-id* argument is entered in the *rack/slot/module* notation. You must specify either the **location all** keywords or the **location** keyword and *node-id* argument with the **node cpu**, **node memory**, or **node process** entity. |
| **template-name** | 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 show running performance-mgmt, on page 183 command to display a list of available templates. |
| **default** | Applies the default template. |

## Command Default

Threshold collection is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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 161 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/RP0/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/RP0/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/RP0/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/RP0/CPU0:router(config)#performance-mgmt apply thresholds interface basic-counters
stats3
```

# 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 XR Config 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

| | |
|---|---|
| *regular-expression-string* | Specifies a defined regular expression group to one or more statistics or threshold template. |
| **index** | Specifies a regular expression index. Range is 1 to 100. |

## Command Default

No regular expression is configured by default.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| monitor | read, write |

This is the sample output from the **performance-mgmt regular-expression** command:

```
RP/0/RP0/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 XR Config 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

| | |
|---|---|
| **dump** | Configures data dump parameters. |
| **local** | Sets the local filesystem on which statistics data is dumped.<br>**Note**<br>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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| monitor | read, write |

This is the sample output for the **performance-mgmt resources dumplocal** command:

```
RP/0/RP0/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 XR Config 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

| | |
|---|---|
| **max-limit** *kilobytes* | Specifies the maximum amount of memory (specified with the *kilobytes* argument) that the PM statistics collector can use for serving data collection requests. Range is 0 to 4294967295 kilobytes.The default is 50000 kilobytes. |
| **min-reserved** *kilobytes* | Specifies a minimum amount of memory (specified with the *kilobytes* 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 XR Config 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

| | |
|---|---|
| **tftp-server** *ip-address* | Specifies the IP address of the TFTP server. |
| **directory** *dir-name* | Specifies the directory where performance management statistics will be copied. |
| **vrf** *vrf_name* | Specifies the name of the VRF instance. |
| **default** | 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router(config)#performance-mgmt resources tftp-server 192.168.134.254 directory
 /user/perfmgmt/tftpdump
```

# performance-mgmt statistics

To create a template to use for collecting performance management statistics, use the **performance-mgmt statistics** command in XR Config 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:<br>• **bgp**—Creates a statistics collection template for Border Gateway Protocol (BGP).<br>• **interface basic-counters**—Creates a statistics collection template for basic counters.<br>• **interface data-rates**—Creates a statistics collection template for data rates.<br>• **interface generic-counters**—Creates a statistics collection template for generic counters.<br>• **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.<br>• **node cpu**—Creates a statistics collection template for the central processing unit (CPU).<br>• **node memory**—Creates a statistics collection template for memory utilization.<br>• **node process**—Creates a statistics collection template for processes.<br>• **ospf v2protocol**—Creates a statistics template for Open Shortest Path First v2 (OSPFv2) protocol instances.<br>• **ospf v3protocol**—Creates a statistics template for OSPFv3 protocol instances. |
| **template** | Specifies that a template will be used for collection. |
| *template-name* | A template name can be any combination of alphanumeric characters, and may include the underscore character (_).<br>Use the show running performance-mgmt, on page 183 to display information about templates, and to display the templates that are being used. |

| | |
|---|---|
| **default** | Applies the settings of the default template. The default template contains the following statistics and values. Values are in minutes.<br>Each entity has a default template. In each default template, the sample interval is 10 minutes, and the default sample count is 5. |
| **sample-size** *size* | (Optional) Sets the number of samples to be taken. |
| **sample-interval** *minutes* | (Optional) Sets the frequency of each sample, in minutes. |
| **history-persistent** | (Optional) Maintains the history of statistics collections persistently. |
| **regular-expression***regular-expression-group-name* | (Optional) Sets instance filtering by regular expression. |

## Command Default

Statistics collections for all entities is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

If you have not yet created a directory for the statistics, use the performance-mgmt resources tftp-server, on page 157 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 149 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/RP0/CPU0:router(config)#performance-mgmt statistics interface data-rates int_data_rates
RP/0/RP0/CPU0:router(config_stats-if-rate)# sample-size 25
RP/0/RP0/CPU0:router(config_stats-if-rate)# sample-interval 5
```

# performance-mgmt thresholds

To configure a template for threshold checking, use the **performance-mgmt thresholds** command in XR Config 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*}] [ *delta* ]
**no performance-mgmt thresholds**

## Syntax Description

| | |
|---|---|
| *entity* | Specify an entity for which you want to create a template:<br>• **bgp** —Creates a template for threshold collection for Border Gateway Protocol (BGP).<br>• **interface basic-counters** —Creates a threshold monitoring template for basic counters.<br>• **interface data-rates** —Creates a threshold monitoring template for data rates.<br>• **interface generic-counters** —Creates a threshold monitoring template for generic counters.<br>• **mpls ldp** —Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor.<br>• **node cpu** —Creates a threshold monitoring template for the central processing unit (CPU).<br>• **node memory** —Creates a threshold monitoring template for memory utilization.<br>• **node process** —Creates a threshold monitoring template for processes.<br>• **ospf v2protocol** —Creates a threshold monitoring template for Open Shortest Path First v2 (OSPFv2) process instances.<br>• **ospf v3protocol** —Creates a threshold monitoring template for OSPFv3 process instances. |
| **template** | Specifies that a template will be used for collection. |
| *template-name* | 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 show running performance-mgmt, on page 183 to display information about templates, and to display the templates that are being used. |
| **default** | Applies the settings of the default template. |
| *attribute* | The attributes for the entity. See Table 17: Attribute Values, on page 163for a list of attributes. |

| | |
|---|---|
| *operation* | A limiting operation for thresholding that includes:<br>• **EQ** —Equal to.<br>• **GE** —Greater than or equal to.<br>• **GT** —Greater than.<br>• **LE** —Less than or equal to.<br>• **LT** —Less than.<br>• **NE** —Not equal to.<br>• **RG** —Not in range. |
| *value* | The base value against which you want to sample. |
| *value2* | (Optional) This value can only be used with the operator **RG** . For example, if you use **RG** for the operation argument value, you create a range between *value* and *value2* . |
| *percent* | (Optional) Specifies a value relative to the previous sample interval value. See the "Usage Guidelines" section for more information. |
| **rearm** {**toggle** \| **window**} | (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 **toggle** 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.<br>Use the **window** 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 **window** 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. |
| *window-size* | The number of intervals to use with the **rearm** keyword. |

## Command Default

None

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.7.1 | The argument *delta* was introduced. |
| Release 6.0 | This command was introduced. |

## 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) GT 50% 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 16: 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 17: 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). |

| Entity | Attributes | Description |
|---|---|---|
| | 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). |
| 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. |
| 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. |
| | 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/RP0/CPU0:router(config)# performance-mgmt thresholds bgp template bgp_thresh1
RP/0/RP0/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/RP0/CPU0:router(config)# performance-mgmt thresholds node cpu template cpu_thresh1
RP/0/RP0/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/RP0/CPU0:router(config)# performance-mgmt thresholds interface generic_ctr template
intf_crc_thresh1
RP/0/RP0/CPU0:router(config-threshold-bgp)# InputCRC GE 1000
```

This example shows how to create a template for monitoring interface generic counters. The template named **ge_delta** is configured to check if the value of InPackets counter exceeds 10.

```
RP/0/0/CPU0:ios(config)#performance-mgmt thresholds interface generic-counters template
ge_delta InPackets ge 10 delta
RP/0/0/CPU0:ios(config)#commit
```

# 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 XR EXEC mode.

**show performance-mgmt** {**monitor** | **statistics**} **bgp** {*ip-address* | **all**} {*sample-id* | **all-samples** | **last-sample**}

## Syntax Description

| | |
|---|---|
| **monitor** | 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. |
| **statistics** | Displays the data collected from statistics collection samples. |
| *ip-address* | IP address of a BGP peer. |
| **all** | Displays all BGP peer instances.<br>**Note** This option is available only with the **statistics** keyword. It is not available with the **monitor** keyword because an entity instance monitoring collection captures data from an entity instance for one sampling cycle. |
| *sample-id* | Sample ID of the monitoring or statistics collection to be displayed. |
| **all-samples** | Displays all collected samples. |
| **last-sample** | Displays the last collected samples. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 18: 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 XR 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

| | |
|---|---|
| **monitor** | 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.<br>**Note** The data is available to be display only as the monitor data is collected. |
| **statistics** | Displays the data collected from statistics collection samples. |
| **basic-counters** | Displays the data collected from interface basic counters entity collections.<br>**Note** Use only for subscriber interfaces and layer 2 transport interfaces |
| **data-rates** | Displays data from interface data rates entity collections. |
| **generic-counters** | Displays data from interface generic counters entity collections.<br>**Note** Use for all interfaces, except subscriber interfaces and layer 2 transport interfaces. |
| *type* | (Optional) Interface type. For more information, use the question mark ( **?** ) online help function. |
| *interface-path-id* | (Optional) Physical interface or virtual interface.<br>**Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br>For more information about the syntax for the router, use the question mark ( **?** ) online help function. |
| **all** | Displays all interface instances.<br>**Note** This option is available only with the **statistics** keyword. It is not available with the **monitor** keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle. |
| *sample-id* | Sample ID of the monitoring collection or statistics collection to be displayed. |
| **all-samples** | Displays all collected samples. |
| **last-sample** | Displays the last collected samples. |

**Command Default** None

**Command Modes** XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

**Usage Guidelines** Use **interface basic-counters** for subscriber interfaces and layer 2 transport interfaces. For all other instances, use **interface generic-counters**.

**Task ID**

| Task ID | Operations |
|---|---|
| monitor | read |

**Examples** This is sample output from the **show performance-mgmt interface** command:

```
RP/0/RP0/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


RP/0/RP0/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 19: 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 XR EXEC mode.

**show performance-mgmt** {**monitor** | **statistics**} **mpls ldp** {*ip-address* | **all**} {*first-sample-id* | **all-samples** | **last-sample**}

## Syntax Description

| | |
|---|---|
| **monitor** | 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.<br>**Note** The data is available to be displayed only as the monitor data is collected. |
| **statistics** | Displays the data collected from statistics collection samples. |
| **ldp** | Displays data from MPLS Label Distribution Protocol (LDP) collections. |
| *ip-address* | IP address of LDP session instance. |
| **all** | Displays data from all LDP session instances.<br>**Note** This option is available only with the **statistics** keyword. It is not available with the **monitor** keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle. |
| *first-sample-id* | Sample ID of the monitoring or statistics collection to be displayed. |
| **all-samples** | Displays all collected samples. |
| **last-sample** | Displays the last collected samples. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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 mpls** command:

```
 RP/0/RP0/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 20: 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 XR EXEC mode.

**show performance-mgmt** {**monitor** | **statistics**} **node** {**cpu** | **memory** | **process**} **location** {*node-id* | **all**} {*sample-id* | **all-samples** | **last-sample**}

## Syntax Description

| | |
|---|---|
| `monitor` | 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.<br>**Note**<br>The data is only available to be displayed as the monitor data is collected. |
| **statistics** | Displays the data collected from statistics collection samples. |
| **cpu** | Displays data from the central processing unit (CPU). |
| **memory** | Displays data from memory. |
| **process** | Displays data from processes. |
| **location** | Specifies the location of data origination. |
| *node-id* | Location of the node. The *node-id* argument is entered in the *rack/slot/module* notation. |
| **all** | Displays data from all LDP session instances.<br>**Note**<br>This option is available only with the **statistics** keyword. It is not available with the **monitor** keyword because a entity instance monitoring collection captures data from an entity instance for one sampling cycle. |
| *sample-id* | Sample ID of the monitoring or statistics collection to be displayed. |
| **all-samples** | Displays all collected samples. |
| **last-sample** | Displays the last collected samples. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# show performance-mgmt monitor node process location 0/RP0/CPU0 process
 13542 last-sample
Node ID:
Sample no: 1 ------------------------------------------- Process ID: 13542
------------------------------------------- PeakMemory: 908 AverageCPUUsed: 0
NoThreads: 5
```

This table describes the significant fields shown in the display.

***Table 21: 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 XR EXEC mode.

**show performance-mgmt** {**monitor** | **statistics**} **ospf** {**v2protocol** | **v3protocol**} *instance* {*sample-id* | **all-samples** | **last-sample**}

## Syntax Description

| | |
|---|---|
| **monitor** | 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.<br>**Note** The data is available to be displayed only as the monitor data is collected. |
| **statistics** | Displays the data collected from statistics collection samples. |
| **v2protocol** | Displays counters for an OSPF v2 protocol instance. |
| **v3protocol** | Displays counters for an OSPF v3 protocol instance. |
| *sample-id* | Sample ID of the monitoring or statistics collection to be displayed. |
| **all-samples** | Displays all collected samples. |
| **last-sample** | Displays the last collected samples. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 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

This is sample output from the **show performance-mgmt ospf** command:

```
RP/0/RP0/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 health sysdb

To display the abstract view of the overall health of the system database (SysDB), use the **show health sysdb** command in XR EXEC mode.

XML schema is supported for the CLI commands.

- SysDB
  - ConfigurationSpace
  - IPCSpace
  - CPU
  - Memory
- SysdbConnections
  - NodeTable
  - Node

**show health sysdb** | **location** <*node-id*> | **memory** | **cpu** | **ipc** | **config** | **conn location** <*node-id*>

## Syntax Description

| | |
|---|---|
| **location** *node-id* | Displays the SysDB health information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation. |
| **memory** | Displays the amount of memory consumed by the SysDB processes. |
| **cpu** | Displays the health of CPU consumed by the SysDB processes. |
| **ipc** | Displays an abstract view of the health of SysDB interprocess communication (IPC) operational space. |
| **config** | Displays an abstract view of the health of SysDB configurational space. |
| **con location** <*node-id*> | Displays an internal breakdown of Lightweight Messaging (LWM) connections for the node. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.4.1 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| cisco-support | read |
| interface | read |

## Examples

The following is sample output from the **show health sysdb** command to display the health of the SysDB:

```
RP/0/RP0/CPU0:router# show health sysdb location 0/2/cpu0
sysdb memory is 32MB, memory is healthy
sysdb cpu time is 0%, cpu is healthy
sysdb operational space is healthy
sysdb configuration space is healthy
```

# show running performance-mgmt

To display a list of configured templates and the template being applied, use the **show running performance-mgmt** command in XR EXEC mode.

**show running performance-mgmt** [**apply** | **regular-expression** | **resources** | **statistics** | **thresholds**]

## Syntax Description

| | |
|---|---|
| **apply** | (Optional) Displays the list of apply template commands in the current configuration. |
| **regular-expression** | (Optional) Displays the list of regular expression commands in the current configuration. |
| **resources** | (Optional) Displays the existing resource configuration commands applied. |
| **statistics** | (Optional) Displays the list of configured statistics templates. |
| **thresholds** | (Optional) Displays the list of configured threshold templates. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 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

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/RP0/CPU0:router(config)#show running performance-mgmt

performance-mgmt resources tftp-server 192.168.134.254 directory muckier/jagrelo/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

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

**Note**

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

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.


- clear counters, on page 187
- load-interval, on page 189
- show environment, on page 190

# clear counters

To clear the interface counters, use the **clear counters** command in XR EXEC mode.

**clear counters** [**all** | *type interface-path-id*]

**Syntax Description**

| | |
|---|---|
| **all** | (Optional) Clears counters on all interfaces. |
| *type* | (Optional) Interface type. For more information, use the question mark (**?**) online help function. |
| *interface-path-id* | (Optional) Physical interface or virtual interface.<br>**Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br>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**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# clear counters all
```

```
Clear "show interface" counters on all interfaces [confirm]
```

# 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

| | |
|---|---|
| *seconds* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface hundredGigE 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# load-interval 30
```

# show environment

To display environmental parameters of the system, use the **show environment** command in the admin prompt.

**show environment** [ **all** | **fans** | **last** | **current** | **leds** | **power-supply** | **table** | **temperatures** | **voltages** ] *node-id*

**Syntax Description**

| | |
|---|---|
| **all** | (Optional) Displays information for all environmental monitor parameters. |
| **fans** | (Optional) Displays information about the fans. |
| **last** | (Optional) Displays the environmental statistics at the time of the last shutdown. |
| **current** | (Optional) Displays the environmental sensors information. |
| **leds** | (Optional) Displays monitor parameters for LEDs of all cards in the node. |
| **power** | (Optional) Displays power supply voltage and current information. |
| **table** | (Optional) Displays environmental parameter ranges. |
| **temperatures** | (Optional) Displays system temperature information. |
| **voltages** | (Optional) Displays system voltage information. |
| node-id | (Optional) Node whose information you want to display. The node-id argument is expressed in the rack/slot/module notation. |

**Command Default**

All environmental monitor parameters is displayed.

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.3.0 | The **show environment** command was moved from the root-system task ID to the system task ID. |

**Usage Guidelines**

The **show environment** command displays information about the hardware that is installed in the system, including fans, LEDs, power supply voltage, and temperatures.

**Task ID**

| Task ID | Operations |
|---|---|
| system | read |

This example shows sample output from the **show environment** command with the **all** keyword.

```
Router# show environment
Possible completions:
  all        All environment monitor parameters
  altitude   Chassis altitude in Meters
Router# show environment altitude
Thu Nov  21 04:02:01.153 UTC+00:00
================================================================================
   Location      Altitude Value (Meters)     Source
--------------------------------------------------------------------------------
   0             0                           config
Router#
```

This example shows sample output from the **show environment** command with the **current** keyword.

```
Router# show environment current
Thu Nov  21 04:02:07.870 UTC+00:00
================================================================================
Location  CURRENT                     Value
          Sensor                      (mA)
--------------------------------------------------------------------------------
0/0/1
          MPA-P3V3_CFP_IOUT             125
          MPA-Hot_Swap_IIN             1208
0/RP0
          MB-P3V3_SFP_IOUT             2312
          MB-P1V0_CORE_JER0_IOUT      53500
          MB-P1V0_AVDD_JER0_IOUT      17750
          MB-P0V85_SRAM_KBP0_IOUT       750
          MB-P0V85_CORE_KBP0_IOUT      9250
          CPU-CPUVCC-IOUT-P3           7500
          CPU-CPUVCC-IIN-P3            1156
          CPU-VDDQ-1V2-IOUT-P3         3500
          CPU-VDDQ-1V2-IIN-P3           375
          CPU-PVCC-1V05-IOUT-P3        4250
          CPU-PVCC-1V05-IIN-P3          421
Router#
```

This example shows sample output from the **show environment** command with the **fan** keyword to view the chassis fan information.

```
Router# show environment fan
Thu Nov  21 04:02:16.387 UTC+00:00
============================================
Location    Fan        Speed (rpm)
--------------------------------------------
0/FT0
            FAN0            12826
0/FT1
            FAN0            12796
0/FT2
            FAN0            13106
0/FT3
            FAN0            13267
0/FT4
            FAN0            13106
0/FT5
            FAN0            13106
0/FT6
            FAN0            13636
0/FT7
            FAN0            12857
0/PM0
```

```
            FAN0            10016
0/PM1
            FAN0                0
```

This example shows sample output from the **show environment** command with the **power** keyword to view the power information of a router.

```
Router# show environment power
Thu Nov  21 04:02:25.247 UTC+00:00
================================================================================
CHASSIS LEVEL POWER INFO: 0
================================================================================
   Total output power capacity (Group 0 + Group 1) :    1200W +       0W
   Total output power required                     :     670W
   Total power input                               :     253W
   Total power output                              :     226W

Power Group 0:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM0       1.2kW-AC    230.0      1.1     12.0     18.8    OK

Total of Power Group 0:        253W/  1.1A       226W/ 18.8A

Power Group 1:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM1       1.2kW-AC      0.0      0.0      0.0      0.0    FAILED or NO PWR

Total of Power Group 1:          0W/  0.0A         0W/  0.0A

================================================================================
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
================================================================================
   0/0/1        NC55-MPA-1TH2H-S       0          14       ON
   0/0                 -               0           -       -
   0/RP0        NCS-55A2-MOD-SE-S     510          -       ON
   0/FT0        NC55-A2-FAN-FW         20          -       ON
   0/FT1        NC55-A2-FAN-FW         20          -       ON
   0/FT2        NC55-A2-FAN-FW         20          -       ON
   0/FT3        NC55-A2-FAN-FW         20          -       ON
   0/FT4        NC55-A2-FAN-FW         20          -       ON
   0/FT5        NC55-A2-FAN-FW         20          -       ON
   0/FT6        NC55-A2-FAN-FW         20          -       ON
   0/FT7        NC55-A2-FAN-FW         20          -       ON
```

This example shows sample output from the **show environment** command with the power keyword to view the power information of a specified location.

```
Router# show environment power location 0
Possible completions:
  0  0/0  0/0/1  0/FT0  0/FT1  0/FT2  0/FT3  0/FT4  0/FT5  0/FT6  0/FT7  0/PM0  0/PM1  0/RP0
sysadmin-vm:0_RP0# show environment power location 0/RP0
Thu Nov  21 04:02:41.827 UTC+00:00

================================================================================
```

```
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
================================================================================
   0/RP0        NCS-55A2-MOD-SE-S      510           -       ON
sysadmin-vm:0_RP0#
```

This example shows sample output from the **show environment** command with the **temperatures** keyword to view the temperature information of a router.

```
Router# show environment temperatures
Thu Nov  21 04:02:50.992 UTC+00:00
================================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major  Crit
          Sensor                   (deg C)   (Lo) (Lo)  (Lo)  (Hi)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/0/1
          MPA-Port-Side-Temp           26    -10    -5     0   100   105   110
          MPA-DCO-Temp                  -     -3     0     5    70    73    75
          MV88EC808_PHY0_Temp          38    -40   -35   -30   105   108   110
          MV88EC808_PHY1_Temp          34    -40   -35   -30   105   108   110
0/RP0
          Control Sensor               31    -10    -5     0    60    71    82
          FAN-side Sensor              34    -10    -5     0   100   105   110
          MB-P1V0_CORE_JER0_TEMP       57    -10    -5     0   125   127   130
          MB-P1V0_AVDD_JER0_TEMP       56    -10    -5     0   125   127   130
          Slice 0 Die Temp             52    -10    -5     0   115   120   125
          Slice 0 TMP421 Temp          47    -10    -5     0   115   120   125
          MV88EC808_PHY0_Temp          52    -40   -35   -30   100   105   110
          MV88EC808_PHY1_Temp          47    -40   -35   -30   100   105   110
          CPU                          36    -10    -5     0    90    96   102
          PORT-side Sensor             28    -10    -5     0   100   105   110
          MAXIM_RMT_CH1                32    -10    -5     0   125   130   135
          MAXIM_RMT_CH2                42    -10    -5     0   125   130   135
          MAXIM_RMT_CH3                30    -10    -5     0   125   130   135
          MAXIM_RMT_CH4                32    -10    -5     0   125   130   135
          MAXIM_RMT_CH5                56    -10    -5     0   125   130   135
          MAXIM_RMT_CH6                35    -10    -5     0   125   130   135
          MAXIM_LCL_CH7                32    -10    -5     0   125   130   135
0/PM0
          Inlet Temperature            30    -10    -5     0    70    72    75
0/PM1
        ! Inlet Temperature             0    -10
```

This example shows sample output from the **show environment** command with the **temperatures** keyword with a specified location.

```
Router# show environment temperatures location 0/0/1
Thu Nov  21 04:02:59.533 UTC+00:00
================================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major  Crit
          Sensor                   (deg C)   (Lo) (Lo)  (Lo)  (Hi)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/0/1
          MPA-Port-Side-Temp           26    -10    -5     0   100   105   110
          MPA-DCO-Temp                  -     -3     0     5    70    73    75
          MV88EC808_PHY0_Temp          38    -40   -35   -30   105   108   110
          MV88EC808_PHY1_Temp          34    -40   -35   -30   105   108   110
sysadmin-vm:0_RP0#
```

This example shows sample output from the **show environment** command with the **voltages** keyword to view the voltage information of a router.

```
Router# show environment voltages
Thu Nov  21 04:03:11.932 UTC+00:00
================================================================================
Location  VOLTAGE                    Value   Crit Minor Minor  Crit
          Sensor                     (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/0/1
          MPA-P12V_VOUT              11993  10800 11040 12960 13200
          MPA-P3V3_STBY_VOUT          3307   2970  3036  3564  3630
          MPA-P3V3_VA_VOUT            3353   2970  3036  3564  3630
          MPA-P2V5_VA_VOUT            2516   2250  2300  2700  2750
          MPA-P1V2_VA_VOUT            1204   1080  1104  1296  1320
          MPA-P1V8_VOUT               1808   1620  1656  1944  1980
          MPA-P1V0_BV_AVDD_VOUT       1007    900   920  1080  1100
          MPA-P1V0_BV_VDD_VOUT        1001    900   920  1080  1100
          MPA-P2V5_BV_VDDO_VOUT       2517   2250  2300  2700  2750
          MPA-P3V3_CFP_VOUT           3344   2970  3036  3564  3630
          MPA-DCO-VOLTAGE_VOUT           -   2970  3036  3564  3630
          MPA-Hot_Swap_VIN           11979  10560 11040 12960 13440
0/RP0
          MB-P1V0_SEC_S_VOUT          1002    900   920  1080  1100
          MB-P1V0_PHY_S_VOUT           997    900   920  1080  1100
          MB-P1V8_STATS_VOUT          1794   1620  1656  1944  1980
          MB-P5V0_S_VOUT              4992   4500  4600  5400  5500
          MB-P2V5_S_VOUT              2499   2250  2300  2700  2750
          MB-P1V2_S_VOUT              1201   1080  1104  1296  1320
          MB-P3V3_S_VOUT              3311   2970  3036  3564  3630
          MB-P1V2_VA_S_VOUT           1195   1080  1104  1296  1320
          MB-P2V5_VA_S_VOUT           2530   2250  2300  2700  2750
          MB-P3V3_VA_S_VOUT           3305   2970  3036  3564  3630
          MB-P12V_S_VOUT             11982  10800 11040 12960 13200
          MB-P3V3_SFP_VOUT            3311   2970  3036  3564  3630
          MB-P0V72_STATS_VOUT          850    765   782   918   935
          MB-P0V85_STATS_VOUT          843    765   782   918   935
          MB-P0V9_STATS_VOUT           896    810   828   972   990
          MB-P1V2_STATS_VOUT          1200   1080  1104  1296  1320
          MB-P1V0_CORE_JER0_VOUT      1000    900   920  1080  1100
          MB-P1V0_AVDD_JER0_VOUT      1000    900   920  1080  1100
          MB-P3V3_JER0_VOUT           3306   2970  3036  3564  3630
          MB-P1V8_JER0_VOUT           1808   1620  1656  1944  1980
          MB-P1V25_AVDD_JER0_VOUT     1258   1080  1104  1296  1320
          MB-P1V0_DDR_JER0_VOUT       1003    900   920  1080  1100
          MB-P1V35_JER0_VOUT          1353   1215  1242  1458  1485
          MB-P1V2_HVA_KBP0_VOUT       1197   1080  1104  1296  1320
          MB-P0V8_LVA_KBP0_VOUT        880    765   782   918   935
          MB-P0V85_SRAM_KBP0_VOUT      847    765   782   918   935
          MB-P0V85_CORE_KBP0_VOUT      850    765   782   918   935
          CPU-ADM1166_VOUT_CH0        1789   1620  1656  1944  1980
          CPU-ADM1166_VOUT_CH1        2525   2250  2300  2700  2750
          CPU-ADM1166_VOUT_CH2        3312   2970  3036  3564  3630
          CPU-ADM1166_VOUT_CH3        4985   4500  4600  5400  5500
          CPU-ADM1166_VOUT_CH4       11909  10800 11040 12960 13200
          CPU-ADM1166_VOUT_CH5         594    540   552   648   660
          CPU-ADM1166_VOUT_CH6        1304   1170  1196  1404  1430
          CPU-ADM1166_VOUT_CH7        1801   1620  1656  1944  1980
          CPU-ADM1166_VOUT_CH8        1196   1080  1104  1296  1320
          CPU-ADM1166_VOUT_CH9        1050    945   966  1134  1155
          CPU-ADM1166_VOUT_CH10       1702   1530  1564  1836  1870
          CPU-ADM1166_VOUT_CH11       1491   1350  1380  1620  1650
          CPU-CPUVCC-VOUT-P3          1791   1620  1656  1940  1980
```

```
            CPU-CPUVCC-VIN-P3           11937  10800 11400 12600 13200
            CPU-VDDQ-1V2-VOUT-P3         1201   1080  1104  1296  1320
            CPU-VDDQ-1V2-VIN-P3         11968  10800 11400 12600 13200
            CPU-PVCC-1V05-VOUT-P3        1051    945   966  1134  1155
            CPU-PVCC-1V05-VIN-P3        11937  10800 11400 12600 13200
sysadmin-vm:0_RP0#
```



# System Health Check Commands

This module describes the system health check commands available on the router. These commands are used to proactively monitor the health of the router.

For detailed information about system health check concepts, configuration tasks, and examples, see the *System Health Check* chapter in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- healthcheck, on page 198
- healthcheck metric, on page 199
- show healthcheck metric, on page 201
- show healthcheck report, on page 203
- show healthcheck status, on page 204
- use-case, on page 206

# healthcheck

To configure the health check cadence and metrics of a system, use the **healthcheck** command in Configuration mode. To disable health check, use the **no** form of this command.

**Note** Health check service is an optional RPM. You must download and install the package explicitly to use the service.

**healthcheck cadence** <*cadence-configuration*> {**enable**} {**metric** | **cpu** | **fabric-health** | **filesystem** | **fpd** | **free-mem** | **shared-mem**}
**no healthcheck metric** <*metric-name*>

## Syntax Description

| | |
|---|---|
| **cadence** | Collects data about system health for enabled metrics at a configured time interval. The cadence can range from 30 to 1800 seconds. |
| **enable** | Enables health check service on the Route Processor (RP). |
| **metric** {**cpu** \| **fabric-health** \| **filesystem** \| **fpd** \| **free-mem** \| **shared-mem**} | Specifies the configurable metrics based on a threshold that applies only to system resources (CPU, free-mem, shared-mem and filesystem). |

## Command Default

Health check is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | This command was introduced. |

## Usage Guidelines

None

## Task ID

| Task ID | Operations |
|---|---|
| root-system or diag or cisco-support or monitor or root-lr | read, write |

## Examples

This example shows how to enable health check service:

```
Router(config)#healthcheck enable
```

This example shows how to configure cadence (in seconds) at which data about system health is collected:

```
Router(config)#healthcheck cadence 30
```

This example shows how to configure the average utilization threshold of CPU metric:

```
Router(config)#healthcheck metric cpu avg-util 15-minute
```

# healthcheck metric

To disable the health check for the metrics of a system, use the **healthcheck metric** command in Configuration mode.

**healthcheck metric** { **cpu** | **fabric-health** | **filesystem** | **fpd** | **free-mem** | **shared-mem** | **platform** | **redundancy** | **interface-counters** | **asic-errors** | **fabric-stats** } **disable**

## Syntax Description

| | |
|---|---|
| **cpu** | Specifies system health data for cpu configurations |
| **fabric-health** | Specifies system health data for fabric configurations |
| **filesystem** | Specifies system health data for file-system usage configurations |
| **fpd** | Specifies system health data for fpd configurations |
| **free-mem** | Specifies system health data for free memory |
| **shared-mem** | Specifies system health data for shared memory |
| **platform** | Specifies system health data for platform configuration |
| **redundancy** | Specifies system health data for redundancy configuration |
| **interface-counters** | Specifies system health data for interface counters |
| **asic-errors** | Specifies system health data for asic-errors |
| **fabric-stats** | Specifies system health data for fabric statistics |
| **disable** | Disables the collection of health-check information |

## Command Default

Health-check for metrics is enabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | This command was introduced. |

## Usage Guidelines

None

## Task ID

| Task ID | Operations |
|---|---|
| monitor | read, write, execute |

## Examples

This example shows how to disable health check service for plaform:

```
Router(config)#healthcheck metric platform disable
Router(config)#commit
```

This example shows how to disable health check service for interface-counters:

```
Router(config)#healthcheck metric intf-counters disable
Router(config)#commit
```

# show healthcheck metric

To view the detailed information about the utilization and state of each metric used to check the health of the system, use the **show healthcheck metric** command in EXEC mode.

**show healthcheck metric cpu** | **free-mem** | **shared-mem** | **filesystem** | **fpd** | **fabric-health** | **platform** | **redundancy** | **interface-counters** { **summary** | | **detail** } | **asic-errors** { **summary** | | **detail** } | **fabric-stats** { **summary** | | **detail** }

## Syntax Description

| | |
|---|---|
| **cpu** \| **free-mem** \| **shared-mem** \| **filesystem** | Name of the system resource for which the metric is viewed. |
| **fpd** \| **fabric-health** \| **platform** \| **redundancy** | Name of the infrastructure service for which the metric is viewed. |
| **interface-counters** \| **asic-errors** \| **fabric-stats** | Name of the counters for which the metric is viewed. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | 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 healthcheck metric** command to view the CPU usage:

```
Router#show healthcheck metric cpu
CPU Metric State: Normal
Last Update Time: <date-time>
CPU Service State: Enabled
Number of Active Nodes: 2
Configured Thresholds:
   Minor: 20%
   Severe: 50%
   Critical: 75%
Node Name: 0/RP0/CPU0
    CPU 1 Minute Average Usage: 6%
    CPU 5 Minute Average Usage: 5%
    CPU 15 Minute Average Usage: 5% *
Node Name: 0/0/CPU0
    CPU 1 Minute Average Usage: 4%
    CPU 5 Minute Average Usage: 4%
    CPU 15 Minute Average Usage: 3% *
'*' indicates the traceked average CPU utilization
```

## Examples

This is sample output from the **show healthcheck metric platform**:

```
Router#show healthcheck metric platform
Platform Metric State: Normal ==========> Health of the metric
Last Update Time: 25 Jun 05:17:03.508172 =====> Timestamp at which the metric data was
collected
Platform Service State: Enabled =====> Service state of Platform
Number of Racks: 1 ======> Total number of racks in the testbed
Rack Name: 0
Number of Slots: 12
Slot Name: RP0
Number of Instances: 2
Instance Name: CPU0
Node Name 0/RP0/CPU0
Card Type 8800-RP
Card Redundancy State Active
Admin State NSHUT
Oper State IOS XR RUN
```

## Examples

This is sample output from the **show healthcheck metric interface-counters**:

```
Router#show healthcheck interface-counters summary
Interface-counters Health State: Normal ==========> Health of the metric
Last Update Time: 25 Jun 05:59:33.965851 =====> Timestamp at which the metric data was
collected
Interface-counters Service State: Enabled =====> Service state of the metric
Interface MgmtEth0/RP0/CPU0/0 =====> Configured interface for healthcheck monitoring
Counter-Names Count Average Consistently-Increasing
-------------------------------------------------------------------------------------------
output-buffers-failures 0 0 N
Counter-Names =====> Name of the counters
Count =====> Value of the counter collected at "Last Update Time"
Average =====> Average of all values available in buffer
Consistently-Increasing =====> Trend of the counter values, as per data available in buffer
Router#show healthcheck interface-counters detail all
Last Update Time: 25 Jun 06:01:35.217089 =====> Timestamp at which the metric data was
collected
Interface MgmtEth0/RP0/CPU0/0 =====> Configured interface for healthcheck monitoring
Following table displays data for last <x=5> values collected in periodic cadence intervals
-------------------------------------------------------------------------------------------------------
Counter-name Last 5 values
LHS = Earliest RHS = Latest
-------------------------------------------------------------------------------------------------------
output-buffers-failures 0 0 0 0 0
parity-packets-received 0 0 0 0 0
```

# show healthcheck report

To view the health check report for enabled metrics in the system, use the **show healthcheck report** command in XR EXEC mode.

**show healthcheck report**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | 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 healthcheck report** command:

```
Router#show healthcheck report
Healthcheck report for enabled metrics
cpu
  State: Normal
free-memory
  State: Normal
filesystem
  State: Normal
shared-memory
  State: Normal
fpd
  State: Warning
One or more FPDs are in NEED UPGD state
fabric-health
  State: Normal
```

# show healthcheck status

To view the status of health check service and configured parameters for each of the enabled metrics, use the **show healthcheck status** command in XR EXEC mode.

**show healthcheck status**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | 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 healthcheck status** command:

```
Router#show healthcheck status
Healthcheck status: Enabled

Collector Cadence: 60 seconds

System Resource metrics
  cpu
      Thresholds: Minor: 10%
                  Severe: 20%
                  Critical: 30%

       Tracked CPU utilization: 15 min avg utilization

   free-memory
        Thresholds: Minor: 10%
                    Severe: 8%
                    Critical: 5%

   filesystem
        Thresholds: Minor: 80%
                    Severe: 95%
                    Critical: 99%

   shared-memory
        Thresholds: Minor: 80%
                    Severe: 95%
                    Critical: 99%
```

```
Infra Services metrics
   fpd

   fabric-health
```

# use-case

To configure a system healthcheck use-case, use the **use-case** command in the healthcheck configuration mode.

Prior to Cisco IOS XR Release 24.1.1:

**use-case** { **asic-reset** { **disable** | **drop-tolerance** *drop-tolerance-value* } | **packet-drop** { **disable** | **drop-tolerance** *drop-tolerance-value* } }

From Cisco IOS XR Release 24.1.1 onwards:

**use-case** { **asic-reset** { **disable** | **drop-tolerance** *drop-tolerance-value* } | **packet-drop** { **disable** | **window-size** *window-size-value* | **tolerance** { **high** | **medium** | **low** } *drop-tolerance-value* } }

## Syntax Description

| | |
|---|---|
| **asic-reset** | Specify ASIC reset system healthcheck use-case |
| **disable** | Disable ASIC reset or packet-drop use-case. By default the use-case is enabled. |
| **drop-tolerance** *drop-tolerance-value* | Configure packet-drop tolerance value<br>Default value: 10<br>Range for *drop-tolerance-value*: 0 - 100<br>This option is removed from Release 24.1.1 onwards |
| **packet-drop** | Specify packet-drop system healthcheck use-case |
| **window-size** *window-size-value* | Configure the number of cadence intervals to alert you of packet-drops.<br>Default value: 10<br>Range for *window-size-value*: 5-20<br>This option is available from Release 24.1.1 onwards |
| **tolerance** { **high** \| **medium** \| **low** } *drop-tolerance-value* | Specify the NPU trap tolerance level and the drop-tolerance value.<br>Range for *drop-tolerance-value*: 0-1000000<br>This option is available from Release 24.1.1 onwards |

## Command Default

Health check use-case is enabled.

## Command Modes

healthcheck configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 24.2.1 | **window-size** and **tolerance** keywords are introduced<br>**drop-tolerance** keyword is removed |
| Release 7.3.3 / Release 7.5.4 | This command was introduced |

## Usage Guidelines

System Health check and use-cases are not part of the base package and you must explicitly install the '*xr-healthcheck'*optional package to use this service.

## Task ID

| Task ID | Operations |
|---|---|
| root-system or diag or cisco-support or monitor or root-lr | read, write |

### Example

This example shows you how to configure the ASIC reset use-case:

```
Router(config)# healthcheck
Router(config-healthcheck)# use-case asic-reset drop-tolerance 10
Router(config-healthcheck)# enable
```

This example shows you how to configure the packet-drop use-case prior to Cisco IOS XR Release 24.1.1:

```
Router(config)# healthcheck
Router(config-healthcheck)# use-case packet-drop drop-tolerance 10
Router(config-healthcheck)# enable
```

This example shows you how to configure the packet-drop use-case from Cisco IOS XR Release 24.1.1 onwards:

```
Router# conf t
Router(config)# healthcheck
Router(config-healthcheck)# use-case packet-drop window-size 5
Router(config-healthcheck)# use-case packet-drop tolerance high 100
Router(config-healthcheck)# enable
Router(config-healthcheck)# commit
```



# IP Service Level Agreement Commands

This module describes the commands used for implementing IP Service Level Agreements on the router.

**Note** All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about IP Service Level Agreements, configuration tasks, and examples, see the *Implementing IP Service Level Agreements* chapter in the *System Monitoring Configuration Guide for Cisco*

*NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- access-list, on page 213
- action (IP SLA), on page 215
- ageout, on page 217
- buckets (history), on page 218
- buckets (statistics hourly), on page 220
- buckets (statistics interval), on page 221
- control disable, on page 222
- datasize request , on page 224
- destination address (IP SLA), on page 226
- destination port, on page 227
- distribution count, on page 228
- distribution interval, on page 230
- exp, on page 232
- filter, on page 234
- force explicit-null, on page 236
- frequency (IP SLA), on page 238
- history, on page 240
- hw-timestamp disable, on page 242
- interval, on page 243
- ipsla, on page 244
- key-chain, on page 245
- life, on page 246
- lives, on page 247
- local-ip, on page 249
- low-memory, on page 250
- lsp selector ipv4, on page 251
- lsr-path, on page 253
- maximum hops, on page 254
- maximum paths (IP SLA), on page 256
- monitor, on page 258
- mpls discovery vpn, on page 259
- mpls lsp-monitor, on page 260
- operation, on page 261
- output interface, on page 262
- output nexthop, on page 264
- packet count, on page 266
- packet interval, on page 267
- path discover, on page 268
- path discover echo, on page 269
- path discover path, on page 271
- path discover scan, on page 273
- path discover session, on page 275
- react, on page 277

- react lpd, on page 281
- reaction monitor, on page 283
- reaction operation, on page 285
- reaction trigger, on page 286
- recurring, on page 287
- reply dscp, on page 288
- reply mode, on page 290
- responder, on page 292
- responder twamp light, on page 293
- samples, on page 295
- scan delete-factor, on page 297
- scan interval, on page 299
- schedule monitor, on page 301
- schedule operation, on page 302
- schedule period, on page 304
- server twamp, on page 306
- show ipsla application, on page 307
- show ipsla history, on page 309
- show ipsla mpls discovery vpn, on page 311
- show ipsla mpls lsp-monitor lpd, on page 313
- show ipsla mpls lsp-monitor scan-queue, on page 315
- show ipsla mpls lsp-monitor summary, on page 317
- show ipsla responder statistics, on page 320
- show ipsla statistics, on page 322
- show ipsla statistics aggregated, on page 325
- show ipsla statistics enhanced aggregated, on page 334
- show ipsla twamp connection, on page 337
- show ipsla twamp session, on page 338
- show ipsla twamp standards, on page 340
- source address , on page 341
- source port , on page 343
- start-time , on page 344
- statistics, on page 346
- tag (IP SLA), on page 348
- target ipv4, on page 350
- target pseudowire, on page 352
- target traffic-eng , on page 354
- threshold, on page 356
- threshold type average, on page 358
- threshold type consecutive, on page 360
- threshold type immediate, on page 362
- threshold type xofy, on page 364
- timeout (IP SLA), on page 366
- tos, on page 368
- ttl, on page 370
- type icmp echo, on page 372

- type icmp path-echo, on page 373
- type icmp path-jitter, on page 374
- type mpls lsp ping, on page 375
- type mpls lsp trace, on page 377
- type udp echo, on page 379
- type udp jitter, on page 380
- type udp ipv4 address, on page 381
- verify-data, on page 382
- vrf (IP SLA), on page 383
- vrf (IP SLA MPLS LSP monitor), on page 385

# 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

| | |
|---|---|
| *acl-name* | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# access-list ipsla
```

## Related Commands

| Command | Description |
|---|---|
| scan interval, on page 299 | Specifies the frequency at which the MPLS LSP monitor instance checks the scan queue for updates. |

| Command | Description |
| --- | --- |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| **logging** | 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. |
| **trigger** | 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 **ipsla reaction trigger** 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# reaction monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react-cond)# action logging
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| reaction monitor, on page 283 | Configures MPLS LSP monitoring reactions. |
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type immediate, on page 362 | Takes action immediately upon a threshold violation. |
| threshold type xofy, on page 364 | 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

| | |
|---|---|
| *seconds* | 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 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 use the **ageout** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# ageout 3600
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *buckets* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# buckets 30
```

## Related Commands

| Command | Description |
|---|---|
| history, on page 240 | Configures the history parameters for the IP SLA operation. |
| operation, on page 261 | Configures an IP SLA operation. |

| Command | Description |
| --- | --- |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *hours* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# buckets 10
```

## Related Commands

| Command | Description |
|---|---|
| statistics, on page 346 | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# buckets 50
```

## Related Commands

| Command | Description |
|---|---|
| statistics, on page 346 | 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

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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

| 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# control disable
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |

| Command | Description |
| --- | --- |
| schedule operation, on page 302 | 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

*size* Specifies the following ranges and default values that are protocol dependent:

- For a UDP jitter operation, range is 16 to 1500 B.
- For a UDP echo operation, range is 4 to 1500 B.
- For an ICMP echo operation, range is 0 to 16384 B.
- For an ICMP path-echo operation, range is 0 to 16384 B.
- For an ICMP path-jitter operation, range is 0 to 16384 B.
- For an MPLS LSP ping operation, range is 100 to 17986 B.

## 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 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 use the **datasize request** command in IP SLA UDP jitter configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# datasize request 512
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type icmp echo, on page 372 | Configures an IP SLA ICMP echo operation. |
| type icmp path-echo, on page 373 | Configures an IP SLA ICMP path-echo operation. |
| type icmp path-jitter, on page 374 | Configures an IP SLA ICMP path-jitter operation. |
| type udp jitter, on page 380 | 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

| | |
|---|---|
| *ipv4-address* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# destination address 192.0.2.12
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *port* | Port number of the target device. Range is 1 to 65355. |

## Command Default

None

## Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# destination port 11111
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# distribution count 15
```

## Related Commands

| Command | Description |
|---|---|
| buckets (statistics hourly), on page 220 | Sets the number of hours in which statistics are kept. |

| Command | Description |
|---|---|
| distribution interval, on page 230 | Sets the time interval (in milliseconds) for each statistical distribution. |
| maximum hops, on page 254 | Sets the number of hops in which statistics are maintained for each path for the IP SLA operation. |
| maximum paths (IP SLA), on page 256 | Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation. |
| statistics, on page 346 | 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

| | |
|---|---|
| *interval* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# distribution interval 50
```

## Related Commands

| Command | Description |
|---|---|
| buckets (statistics hourly), on page 220 | Sets the number of hours in which statistics are kept. |
| distribution count, on page 228 | Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation. |

| Command | Description |
|---|---|
| maximum hops, on page 254 | Sets the number of hops in which statistics are maintained for each path for the IP SLA operation. |
| maximum paths (IP SLA), on page 256 | Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation. |
| statistics, on page 346 | 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

| | |
|---|---|
| *exp-bits* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
```

```
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-trace)# exp 5
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| **all** | Stores history data for all operations, if set. |
| **failures** | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# filter all
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |

| Command | Description |
| --- | --- |
| schedule operation, on page 302 | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-trace)# force explicit-null
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *seconds* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# schedule monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-sched)# frequency 1200
RP/0/RP0/CPU0:router(config-ipsla-mplslm-sched)# schedule period 600
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| schedule period, on page 304 | 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

| | |
|---|---|
| **buckets** | Sets the number of history buckets that are kept during the lifetime of the IP SLA operation. |
| *buckets* | Number of history buckets that are kept during the lifetime of an IP SLA operation. Range is 1 to 60. |
| **filter** | Defines the type of information that is kept in the history table for the IP SLA operation. |
| **all** | Stores history data for all operations, if set. |
| **failures** | Stores data for operations that failed, if set. |
| **lives** | Sets the number of lives that are maintained in the history table for an IP SLA operation. |
| *lives* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)#
```

## Related Commands

| Command | Description |
|---|---|
| buckets (history), on page 218 | Sets the number of history buckets that are kept during the lifetime of the IP SLA operation. |
| filter, on page 234 | Defines the type of information that are kept in the history table for the IP SLA operation. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| lives, on page 247 | Sets the number of lives that are maintained in the history table for an IP SLA operation. |
| samples, on page 295 | Sets the number of hop entries that are kept in the history table for an IP SLA ICMP path-echo operation. |

# hw-timestamp disable

To disable hardware time stamp configuration, use the **hw-timestamp disable** command in the IP SLA configuration mode.

**hw-timestamp disable**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

IP SLA configuration

**Command History**

| Release | Modification |
|---|---|
| Release 6.0.1 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operation |
|---|---|
| monitor | read, write |

### Example

The following example shows how to disable hardware time stamping:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# hw-timestamp disable
```

# 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

| | |
|---|---|
| *refresh-interval* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls discovery vpn
RP/0/RP0/CPU0:router(config-ipsla-mpls-discovery-vpn)# interval 120
```

## Related Commands

| Command | Description |
|---|---|
| mpls discovery vpn, on page 259 | Configures MPLS label switched path (LSP) provider edge (PE) router discovery. |

# ipsla

To enter IP SLA configuration mode and configure IP Service Level Agreements, use the **ipsla** command in XR Config 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

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)#
```

# 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

| | |
|---|---|
| *key-chain-name* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# key-chain ipsla-keys
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| **forever** | Schedules the operation to run indefinitely. |
| *seconds* | 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 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 use the **life** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# life forever
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *lives* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# lives 2
```

## Related Commands

| Command | Description |
|---|---|
| buckets (history), on page 218 | Sets the number of history buckets that are kept during the lifetime of the IP SLA operation. |

| Command | Description |
|---|---|
| filter, on page 234 | Defines the type of information that are kept in the history table for the IP SLA operation. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| samples, on page 295 | Sets the number of hop entries that are kept in the history table for an IP SLA ICMP path-echo operation. |

# local-ip

To configure the test-session parameters for TWAMP-light responder, use the **local-ip** command in the **ipsla responder twamp-light** mode. To remove the set configuration, use the **no** form of the command.

**local-ip** *local-ip-address* **local-port** *local-port* **remote-ip** *remote-ip-address* **remote-port** *remote-port* **vrf** [**default** | *vrf-name*]

## Syntax Description

| | |
|---|---|
| **local-ip** *local-ip-address* | Configure IPv4/IPv6 address of the interface on the local router |
| **local-port** *local-port* | Configure the UDP port number of the local router. Range is 1 - 65535 |
| **remote-ip** *remote-ip-address* | Configure IPv4/IPv6 address of the interface on the remote router |
| **remote-port** *remote-port* | Configure the UDP port number of the remote router. Range is 1 - 65535 |
| **vrf** [**default** | *vrf-name* ] | Configure the VRF that the interface on the local router is part of |

## Command Default

None

## Command Modes

IPSLA responder TWAMP-light configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 6.6.1 | This command is introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

### Example

This example shows how to run the **responder** command in order to configure TWAMP responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1
Router(config-twamp-light-def)# local-ip 192.0.2.10 local-port 13001 remote-ip 192.0.2.186
 remote-port 13002 vrf default
```

# low-memory

**low-memory** *value*
**no low-memory**

## Syntax Description

| | |
|---|---|
| *value* | Low-water memory mark 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# low-memory 102400
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| show ipsla application, on page 307 | 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

| | |
|---|---|
| *ip-address* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-trace)# lsp selector ipv4 127.10.10.1
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *ip address* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# lsr-path 192.0.2.40
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *hops* | 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, *pathecho*. |

## Command Default

The default value is 16 hops.

## Command Modes

IP SLA operation statistics configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# maximum hops 20
```

## Related Commands

| Command | Description |
|---|---|
| buckets (statistics hourly), on page 220 | Sets the number of hours in which statistics are kept. |
| distribution count, on page 228 | Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation. |
| distribution interval, on page 230 | Sets the time interval (in milliseconds) for each statistical distribution. |

| Command | Description |
| --- | --- |
| maximum paths (IP SLA), on page 256 | Sets the number of paths in which statistics are maintained for each hour for an IP SLA operation. |
| statistics, on page 346 | 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

| | |
|---|---|
| *paths* | 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, *pathecho*. |

## Command Default

The default value is 5 paths.

## Command Modes

IP SLA operation statistics configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# maximum paths 20
```

## Related Commands

| Command | Description |
|---|---|
| buckets (statistics hourly), on page 220 | Sets the number of hours in which statistics are kept. |
| distribution count, on page 228 | Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation. |
| distribution interval, on page 230 | Sets the time interval (in milliseconds) for each statistical distribution. |

| Command | Description |
| --- | --- |
| maximum hops, on page 254 | Sets the number of hops in which statistics are maintained for each path for the IP SLA operation. |
| statistics, on page 346 | 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

| | |
|---|---|
| *monitor-id* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| **interval** | Configures the refresh interval for MPLS label switched path (LSP) monitoring. |

## Command Default

None

## Command Modes

IP SLA configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

Use the **mpls discovery vpn** 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

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

## Examples

The following example shows how to enter IP SLA MPLS discovery VPN mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls discovery vpn
RP/0/RP0/CPU0:router(config-ipsla-mpls-discovery-vpn)#
```

## Related Commands

| Command | Description |
|---|---|
| interval, on page 243 | Configures the refresh interval for 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)#
```

## Related Commands

| Command | Description |
|---|---|
| mpls discovery vpn, on page 259 | Configures MPLS label switched path (LSP) provider edge (PE) router discovery. |

# 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

| | |
|---|---|
| *operation-number* | Operation number. Range is 1 to 2048. |

## Command Default

None

## Command Modes

IP SLA configuration

## Command History

| Release | Modification |
|---|---|
| Release 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 use the IP SLA **operation** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)#
```

## Related Commands

| Command | Description |
|---|---|
| schedule operation, on page 302 | 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

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark (**?**) online help function. |
| *interface-path-id* | Physical interface or virtual interface.<br>**Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.<br>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 6.0 | 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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls ls output interface pos 0/1/0/0
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| output nexthop, on page 264 | Configures the next-hop address to be used for LSP ping or LSP trace operations. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *ip-address* | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-trace)# output nexthop 10.1.1.1
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| output interface, on page 262 | Configures the echo request output interface to be used for LSP ping or LSP trace operations. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *count* | 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 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 use the **packet count** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# packet count 30
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| packet interval, on page 267 | 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

| | |
|---|---|
| *interval* | 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 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 use the **packet interval** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# packet interval 30
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| packet count, on page 266 | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/RP0/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

| | |
|---|---|
| **interval** *time* | Configures the interval (in milliseconds) between MPLS LSP echo requests sent during path discovery. Range is 0 to 3600000. Default is 0. |
| **maximum lsp selector ipv4** *host-address* | 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. |
| **multipath bitmap size** *size* | 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. |
| **retry** *count* | Configures the number of timeout retry attempts for MPLS LSP echo requests sent during path discovery. Range is 0 to 10. Default is 3. |
| **timeout** *value* | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# echo interval 777
```

## Related Commands

| Command | Description |
|---|---|
| path discover path, on page 271 | Configures MPLS LSP path parameters. |
| path discover scan, on page 273 | Configures MPLS LSP scan parameters. |
| path discover session, on page 275 | 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

| | |
|---|---|
| **retry** *range* | 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. |
| **secondary frequency** | Configures a secondary frequency to use after a failure condition (that is, a connection-loss or timeout) occurs. |
| **both** | Enable secondary frequency for a timeout and connection loss. |
| **connection-loss** | Enable secondary frequency for only a connection loss. |
| **timeout** | Enable secondary frequency for only a timeout. |
| *value* | Frequency value range is 1 to 604800. |

## Command Default

None

## Command Modes

MPLSLM LPD configuration

## Command History

| Release | Modification |
|---|---|
| Release 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# path retry 12
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# path secondary frequency both 10
```

## Related Commands

| Command | Description |
|---|---|
| path discover echo, on page 269 | Configures MPLS LSP echo parameters. |
| path discover scan, on page 273 | Configures MPLS LSP scan parameters. |
| path discover session, on page 275 | 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

| | |
|---|---|
| **period** *value* | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# scan period 2
```

## Related Commands

| Command | Description |
|---|---|
| path discover echo, on page 269 | Configures MPLS LSP echo parameters. |

| Command | Description |
| --- | --- |
| path discover path, on page 271 | Configures MPLS LSP path parameters. |
| path discover session, on page 275 | 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

| | |
|---|---|
| **limit** *value* | 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. |
| **timeout** *value* | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# path discover
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-lpd)# session timeout 22
```

## Related Commands

| Command | Description |
|---|---|
| path discover echo, on page 269 | Configures MPLS LSP echo parameters. |
| path discover path, on page 271 | Configures MPLS LSP path parameters. |

| Command | Description |
| --- | --- |
| path discover scan, on page 273 | 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

| | |
|---|---|
| **connection-loss** | Specifies that a reaction occurs if there is a connection-loss for the monitored operation. |
| **jitter-average** [**dest-to-source** \| **source-to-dest**] | 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 **jitter-average** keyword:<br>• **dest-to-source**—(Optional) Specifies the jitter average destination to source (DS).<br>• **source-to-dest**—(Optional) Specifies the jitter average source to destination (SD). |
| **packet-loss** {**dest-to-source** \| **source-to-dest**} | Specifies the reaction on packet loss value violation. The following options are listed for the **packet-loss** keyword:<br>• **dest-to-source**—(Optional) Specifies the packet loss destination to source (DS) violation.<br>• **source-to-dest**—(Optional) Specifies the packet loss source to destination (SD) violation. |
| **rtt** | Specifies that a reaction occurs if the round-trip value violates the upper threshold or lower threshold. |
| **timeout** | Specifies that a reaction occurs if there is a timeout for the monitored operation. |
| **verify-error** | 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 6.0 | This command was introduced. |

## 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.

This table lists the Supported Reaction Configuration, by IP SLA Operation.

***Table 22: Supported Reaction Configuration, by IP SLA Operation***

| Operation | ICMP Echo | Path Echo | UDP Jitter | UDP Echo | ICMP Path Jitter | MPLS LSP Ping | MPLS LSP Trace |
|---|---|---|---|---|---|---|---|
| Failure | -- | -- | -- | -- | -- | -- | -- |
| RTT | Y | Y | Y | Y | Y | Y | Y |
| RTTAvg | -- | -- | -- | -- | -- | -- | -- |
| Timeout | Y | Y | Y | Y | Y | Y | Y |
| connectionLoss | -- | -- | Y | Y | -- | Y | Y |
| verifyError | -- | -- | Y | Y | -- | -- | -- |
| jitterSDAvg | -- | -- | Y | -- | -- | -- | -- |
| jitterDSAvg | -- | -- | Y | -- | -- | -- | -- |
| jitterAvg | -- | -- | Y | -- | -- | -- | -- |
| PacketLossDS | -- | -- | Y | -- | -- | -- | -- |
| PacketLossSD | -- | -- | Y | -- | -- | -- | -- |
| PacketLoss | -- | -- | Y | -- | -- | -- | -- |

## 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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **jitter-average** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **packet-loss** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **rtt** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react rtt
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **timeout** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react timeout
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **verify-error** keyword:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react verify-error
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs when you configure the **react** command or when threshold events occur. |
| operation, on page 261 | Configures an IP SLA operation. |

| Command | Description |
|---|---|
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type immediate, on page 362 | Takes action immediately upon a threshold violation. |
| threshold type xofy, on page 364 | 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

| | |
|---|---|
| **lpd-group** | Specifies that a reaction should occur if there is a status violation for the monitored LPD group. |
| **tree-trace** | Specifies that a reaction should occur if there is a path discovery violation for the monitored LPD group. |
| **action** | Configures the action to be taken on threshold violation. |
| **logging** | 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 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# reaction monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react)# react lpd lpd-group action logging
```

**Related Commands**

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *monitor-id* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# reaction monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react)#
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs when you configure the **react** command or when threshold events occur. |

| Command | Description |
|---|---|
| monitor, on page 258 | Configures an IP SLA MPLS LSP monitor instance. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| schedule monitor, on page 301 | Schedules an IP SLA MPLS LSP monitor instance. |
| threshold type consecutive, on page 360 | Specifies to take action after a number of consecutive violations. |
| threshold type immediate, on page 362 | 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

| | |
|---|---|
| *operation-id* | 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 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 use the **reaction operation** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 1
RP/0/RP0/CPU0:router(config-ipsla-react)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *triggering-operation* | Operation that contains a configured action-type trigger and can generate reaction events. Range is 1 to 2048. |
| *triggered-operation* | Operation that is started when the *triggering-operation* 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction trigger 1 2
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |

# 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 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 use the **recurring** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# recurring
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *dscp-bits* | Differentiated services codepoint (DSCP) value for an echo reply packet. Valid values are from 0 to 63.<br>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 6.0 | This command was introduced. |

## Usage Guidelines

Use the **reply dscp** command to set the DCSP 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 an 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

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-ping)# reply dscp 5
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| **control-channel** | Sets echo requests to reply by way of a control channel.<br>**Note** This option is available only in IP SLA MPLS LSP ping configuration mode. |
| **router-alert** | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-ping)# target pseudowire 192.168.1.4 4211
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-ping)# reply mode control-channel
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | Traces the hop-by-hop route of an LSP path in an MPLS VPN. |

# responder

To configure the responder for IP SLA, use the **responder** command in the **ipsla** mode. To remove the set configuration, use the **no** form of the command.

**responder** [**twamp** | [**twamp-light** **test-session** *test-session-id*] ] [**timeout** *timeout-value*]

## Syntax Description

| | |
|---|---|
| **twamp** | Configure TWAMP responder |
| **twamp-light** | Configure TWAMP-light responder |
| **test-session** *test-session-id* | Configure TWAMP-light test-session id. Range is 1 - 65535 |
| **timeout** *timeout-value* | Configure the inactivity timeout period (in seconds)<br>For TWAMP, the range is 1 - 604800. For TWAMP-light, the range is 60 - 86400 |

## Command Default

Default timeout for TWAMP responder is 900 seconds.

By default, there is no timeout for TWAMP-light responder.

## Command Modes

IPSLA configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 6.3.1 | This command is introduced for TWAMP responder. |
| Release 6.6.1 | This command is introduced for TWAMP-light responder. |

## Usage Guidelines

No specific guidelines impact the use of this command.

### Example

This example shows how to configure the TWAMP responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp timeout 100
```

This example shows how to configure the TWAMP-light responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1 timeout 100
```

# responder twamp light

To configure the TWAMP-light responder, use the **responder twamp-light** command in the **ipsla** configuration mode.

**responder twamp-light test-session** *test-session-id* [ **local-ip** { *local-ip-address* | **any** { **ipv4** | **ipv6** } } **local-port** *local-port-number* **remote-ip** { *remote-ip-address* | **any** { **ipv4** | **ipv6** } } **remote-port** { *remote-port-number* | **any** } **vrf** { *vrf-name* | **any** | **default** } | **timeout** *timeout-value* ]

## Syntax Description

| | |
|---|---|
| **test-session** *test-session-id* | Configure TWAMP-light test-session id.<br>Range: 1 - 65535 |
| **local-ip** { *local-ip-address* \| **any** { **ipv4** \| **ipv6** } } | Configure the local ip-address or allow any local IPv4 or IPv6 address |
| **local-port** *local-port-number* | Configure the local UDP port number.<br>Range: 1 - 65535 |
| **remote-ip** { *remote-ip-address* \| **any** { **ipv4** \| **ipv6** } } | Configure the remote client's ip-address or allow connection from any remote IPv4 or IPv6 address |
| **remote-port** { *remote-port-number* \| **any** } | Configure the UDP port number of the remote client or allow connection from any remote port.<br>Range: 1 - 65535 |
| **vrf** { *vrf-name* \| **any** \| **default** } | Configure vrf for the local ip-address.<br>Possible values for vrf:<br>• *vrf-name* of the vrf of the local ip-address<br>• any: use this only when **local-ip** is configured as any<br>• default: use this when the local ip-address belongs to default vrf |
| **timeout** *timeout-value* | Configure the inactivity timeout period (in seconds)<br>For TWAMP-light, the range is 60 - 86400 |

## Command Default

Default timeout is 900 seconds.

## Command Modes

IPSLA configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 7.4.1 | The **any** option was included for local-ip, remote-ip, remote-port and vrf . |

| Release | Modification |
|---|---|
| Release 6.6.1 | This command was introduced. |

## Usage Guidelines

- Caution must be taken by the administrator when using **any** option as this configuration opens up the specified **local-port** for packets from any IP address.
- Configure **vrf** as **any** only when you configure **local-ip** as **any**.
- Configure **vrf** with a valid vrf value, when you configure **local-ip** with a valid IPv4/IPv6 address.

## Task ID

| Task ID | Operation |
|---|---|
| monitor | read, write |

### Example

This example shows how to configure the twamp-light responder:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1 local-ip 192.0.2.10 local-port
13001 remote-ip 192.0.2.186 remote-port 13002 vrf default
Router(config-ipsla)# responder twamp-light test-session 1 timeout 60
Router(config-ipsla)# commit
```

# samples

To set the number of hop entries that are kept in the history table for an IP SLA ICMP path-echo operation, use the **samples** command in IP SLA operation ICMP path-echo history configuration mode. To use the default value, use the **no** form of this command.

**samples** *sample-count*
**no samples**

## Syntax Description

| | |
|---|---|
| *sample-count* | Number of history samples that are kept in the history table for an IP SLA ICMP path-echo operation. Range is 1 to 30. |

## Command Default

The default value is 16.

## Command Modes

IP SLA operation ICMP path-echo history configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

The **samples** command is supported only when you configure an IP SLA ICMP path-echo operation.

## Task ID

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

## Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# samples 30
```

## Related Commands

| Command | Description |
|---|---|
| buckets (history), on page 218 | Sets the number of history buckets that are kept during the lifetime of the IP SLA operation. |
| filter, on page 234 | Defines the type of information that are kept in the history table for the IP SLA operation. |
| history, on page 240 | Configures the history parameters for the IP SLA operation. |
| operation, on page 261 | Configures an IP SLA operation. |

| Command | Description |
| --- | --- |
| schedule operation, on page 302 | Schedules an IP SLA operation. |

# 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

| | |
|---|---|
| *factor-value* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# scan delete-factor 214
```

## Related Commands

| Command | Description |
|---|---|
| monitor, on page 258 | Configures an IP SLA MPLS LSP monitor instance. |

| Command | Description |
| --- | --- |
| scan interval, on page 299 | Specifies the frequency at which the MPLSLM instance checks the scan queue for updates. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *scan-interval* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# scan interval 120
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| scan delete-factor, on page 297 | Specifies the frequency with which the MPLSLM instance searches for PE routers to delete. |

| Command | Description |
|---|---|
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *monitor-id* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# schedule monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-sched)#
```

## Related Commands

| Command | Description |
|---|---|
| frequency (IP SLA), on page 238 | Configures the frequency interval during which LSP groups and operations are scheduled to start. |
| schedule period, on page 304 | Configures the amount of time during which all LSP operations are scheduled to start or run. |
| start-time , on page 344 | 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 6.0 | 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 **schedule operation** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)#
```

## Related Commands

| Command | Description |
|---|---|
| ageout, on page 217 | Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. |
| operation, on page 261 | Configures an IP SLA operation. |
| life, on page 246 | Specifies the length of time to execute. |
| recurring, on page 287 | Indicates that the operation starts automatically at the specified time and for the specified duration every day. |

| Command | Description |
| --- | --- |
| start-time , on page 344 | 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

| | |
|---|---|
| *seconds* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# schedule monitor 20
RP/0/RP0/CPU0:router(config-ipsla-mplslm-sched)# schedule period 6000
```

## Related Commands

| Command | Description |
|---|---|
| frequency (IP SLA), on page 238 | Configures the frequency interval during which LSP groups and operations are scheduled to start. |
| start-time , on page 344 | 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* ]
**noserver twamp** [ **port** *number* | **timer inactivity** *value* ]

## Syntax Description

| | |
|---|---|
| **port** | Configures the port for the server. |
| *number* | Port number. Range is 1 to 65535. |
| **timer** | Configures the timer for the server. |
| **inactivity** *value* | 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 6.3.1 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| monitor | read, write |

### Example

This example shows how to use the **server twamp** command:

```
RP/0/RP0/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 XR EXEC mode.

**show ipsla application**

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

**Command Default** None

**Command Modes** XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 23: 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 |
|---|---|
| low-memory, on page 250 | Configures a low-water memory mark. |
| operation, on page 261 | 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 XR EXEC mode.

**show ipsla history** [*operation-number*]

**Syntax Description**

| | |
|---|---|
| *operation-number* | (Optional) Number of the IP SLA operation. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | 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 24: 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 |
| 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/RP0/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 25: 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. |
| Sense | Response return code. |
| TargetAddr | IP address of intermediate hop device or destination device. |

## Related Commands

| Command | Description |
|---|---|
| show ipsla statistics aggregated, on page 325 | 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 XR 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 26: 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. |

| Field | Description |
|---|---|
| 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 XR EXEC mode.

**show ipsla mpls lsp-monitor lpd** {**statistics** [*group-ID* | **aggregated** *group-ID*] | **summary** *group*}

| | |
|---|---|
| **statistics** *group-ID* | Displays statistics for the specified LPD group, including the latest LPD start time, return code, completion time, and paths. |
| **aggregated** *group-ID* | Displays the aggregated statistics of the LPD group. |
| **summary** *group- ID* | 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**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 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/RP0/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 27: 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 XR EXEC mode.

**show ipsla mpls lsp-monitor scan-queue** [*monitor-id*]

**Syntax Description**

| | |
|---|---|
| *monitor-id* | (Optional) Number of the IP SLA MPLS LSP monitor instance. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

**Usage Guidelines**

If the *monitor-id* argument is not specified, the scan-queue is displayed for all MPLS LSP monitor instances.

**Task ID**

| Task ID | Operations |
|---|---|
| monitor | read |

**Examples**

The following sample output is from the **show ipsla mpls lsp-monitor scan-queue** command:

```
RP/0/RP0/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 28: 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. |

| Field | Description |
|---|---|
| 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 XR EXEC mode.

**show ipsla mpls lsp-monitor summary** [*monitor-id* [**group** [*group id*]]]

## Syntax Description

| | |
|---|---|
| *monitor-id* | (Optional) Displays a list of LSP group, ping, and trace operations created automatically by the specified MPLSLM instance. |
| **group** *group-id* | (Optional) Displays the ECMP LSPs found through ECMP path discovery within the specified LSP group. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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/RP0/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 29: 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:<br>• up—Indicates that the latest operation cycle was successful.<br>• down—Indicates that the latest operation cycle was not successful.<br>• pending—Indicates that the latest operation cycle is waiting for an LSP ping or trace response. |
| 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/RP0/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 30: show ipsla mpls lsp-monitor summary group Field Descriptions***

| Field | Description |
|---|---|
| GrpID | Group identifer that has been created by this MPLS LSP monitor instance. |
| LSP-Selector | LSP selector address. |

| Field | Description |
|---|---|
| Status | Status of the paths. Values can be as follows:<br>• up—Indicates that all the paths were successful.<br>• down—Indicates that all the paths were not successful.<br>• partial—Indicates that only some paths were successful.<br>• 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. |
| 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 XR EXEC mode.

**show ipsla responder statistics** {**all** | **permanent**} **ports**

## Syntax Description

| | |
|---|---|
| **all** | Port statistics is displayed for all ports. |
| **permanent** | Port statistics is displayed only for permanent ports. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/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 31: 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 XR EXEC mode.

**show ipsla statistics** [*operation-number*]

**Syntax Description**

| | |
|---|---|
| *operation-number* | (Optional) Operation for which the latest statistics are to be displayed. Range is 1 to 2048. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| monitor | read |

**Examples**

The 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/RP0/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
    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 32: 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. |
| 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 Table 24: Response Return Values for the show ipsla history Command, on page 309, in **show ipsla history** command.) |
| LSP Selector | LSP selector address of the path. |

| Field | Description |
|---|---|
| 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 |
|---|---|
| show ipsla statistics aggregated, on page 325 | 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 XR EXEC mode.

**show ipsla statistics aggregated** [**detail**] [*operation-number*]

## Syntax Description

| | |
|---|---|
| **detail** | Displays detailed information. |
| *operation-number* | (Optional) Number of IP SLA operations. Range is 1 to 2048. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## 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/RP0/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/RP0/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 33: 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. |

| Field | Description |
|---|---|
| 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. |
| 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. |

| Field | Description |
|---|---|
| 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. |
| 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. |

| Field | Description |
|---|---|
| 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. |
| 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/RP0/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           6
2     1134423851116 1   1   1   2           129
      0             2419        41          41
2     1134423070733 1   1   2   1           101
      0             1119        16          16
2     0             1   1   3   0           0
      0             0           0           0
```

This table describes the significant fields shown in the display.

***Table 34: show ipsla statistics aggregated detail Field Descriptions***

| Field | Description |
|---|---|
| Entry | Entry number. |
| StartT | Start time of entry, in hundredths of seconds. |
| 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/RP0/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 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
<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 35: 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. |

| Field | Description |
|---|---|
| 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. |
| 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 Table 24: Response Return Values for the show ipsla history Command, on page 309, in **show ipsla history** 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 |
|---|---|
| show ipsla statistics, on page 322 | Displays the operational data for the IP SLA operation. |

| Command | Description |
| --- | --- |
| show ipsla statistics enhanced aggregated, on page 334 | 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 XR EXEC mode.

**show ipsla statistics enhanced aggregated** [*operation-number*] [**interval** *seconds*]

## Syntax Description

| | |
|---|---|
| *operation-number* | (Optional) Operation number for which to display the enhanced history distribution statistics. |
| **interval** *seconds* | (Optional) Specifies the aggregation interval in seconds for which to display the enhanced history distribution statistics. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# show ipsla statistics enhanced aggregated 20

Entry number: 20
Interval : 300 seconds
  Bucket : 1   (0   - 300 seconds)
    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 36: 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 **show ipsla statistics enhanced aggregated** 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. |
| 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. |

| Field | Description |
|---|---|
| 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 |
|---|---|
| show ipsla statistics, on page 322 | Displays the operational data for the IP SLA operation. |
| show ipsla statistics aggregated, on page 325 | 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 conection** command in the XR EXEC mode.

**show ipsla twamp connection** [ **detail***source-ip* | **requests** ]

**Syntax Description**

| | |
|---|---|
| **detail** *source-ip* | Displays details of the connection for a specified source-ip. |
| **requests** | Displays request details. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operation |
|---|---|
| ip-services | read |

### Example

This example shows how to run the **show ipsla twamp conection** command with the **requests** keyword:

```
RP/0/RP0/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 XR EXEC mode.

**show ipsla twamp session** [ **source-ip** *host-name* | **brief** ]

**Syntax Description**

| | |
|---|---|
| **source-ip** *host-name* | Displays session information for the specified source-ip and hostname. |
| **brief** | Displays the session details in brief in tabular format |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.3.1 | This command was introduced. |
| Release 7.4.1 | A new keyword, **brief**, was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operation |
|---|---|
| monitor | read |

### Example

This example shows how to run **show ipsla twamp session** command:

```
Router# show ipsla twamp session
***** TWAMP Sessions *****
No records matching query found
***** TWAMP-LIGHT Sessions *****
Session status: Active
Recvr Addr: any (IPV4)
Recvr Port: 2345
Sender Addr: any (IPV4)
Sender Port: any
Sender VRF Name: any
Session ID: 10
Mode: Unauthenticated
Number of Packets Received: 0
Session timeout: 0
Number of Packets Sent: 0
```

The sample output of **show ipsla twamp session brief** command:

```
Router# show ipsla twamp session brief
* M - Mode of authentication     U - Unauthenticated
  D - DSCP value                 PL - Pad Length
  RX - Packets Received          TX - Packets Sent
  T - TWAMP                      TWL - TWAMP Light
  > - field trimmed

S.No Receiver Address_Port/          VRF Name          M/D   PL     RX/TX    Type   Sender
 Address_Port
-------------------------------------------------------------------------------------------------
1     10.0.88.23_11232 /              default           U/24  80   3150/3150  TWL
10.173.125.230_11332
2     10.0.88.23_11233 /              default           U/40  108  1274/1274  TWL
10.173.125.230_11333
3     10.0.88.23_11234 /              default           U/40  80   3181/3181  TWL
10.173.125.230_11334
4     10.0.88.23_11235 /              default           U/40  298    11/11    TWL
10.173.125.230_11335
5     10.0.88.23_11236 /              default           U/8   298    18/18    TWL
10.173.125.230_11336
6     10.0.88.23_11237 /              default           U/0   298    15/15    TWL
10.173.125.230_11337
```

# show ipsla twamp standards

To display the Two-way Active Management Protocol (TWAMP) standards, use the **show ipsla twamp standards** command in the XR 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

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| ip-services | read |

### Example

This example shows how to use the **show ipsla twamp standards** command:

```
RP/0/RP0/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 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 designate an IP address for the **source address** command in IP SLA UDP jitter configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# source address 192.0.2.9
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| **port** *port* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# source port 11111
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *hh:mm:ss* | Absolute start time in hours, minutes, and seconds. You can use the 24-hour clock notation. For example, the **start-time** *01:02* is defined as 1:02 am, or **start-time** *13:01:30* is defined as start at 1:01 pm. and 30 seconds. The current day is used; unless, you specify a *month* and *day*. |
| *month* | (Optional) Name of the month to start the operation. When you use the *month* 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. |
| *day* | (Optional) Number of the day, in the range of 1 to 31, to start the operation. In addition, you must specify a month. |
| *year* | (Optional) Year in the range of 1993 to 2035. |
| **after** *hh:mm:ss* | Specifies that the operation starts at *hh* hours, *mm* minutes, and *ss* seconds after the **start-time** command is used. |
| **now** | Specifies that the operation should start immediately. |
| pending | Specifies that no information is collected. The default value is the **pending** 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# schedule monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla operation 2
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# destination address 192.0.2.9
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# exit
RP/0/RP0/CPU0:router(config-ipsla-op)# exit

RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 2
RP/0/RP0/CPU0:router(config-ipsla-sched)# start 20:0:0 february 7 2008
RP/0/RP0/CPU0:router(config-ipsla-sched)#
```

## Related Commands

| Command | Description |
|---|---|
| life, on page 246 | Specifies the length of time to execute. |
| operation, on page 261 | Configures an IP SLA operation. |
| recurring, on page 287 | Indicates that the operation starts automatically at the specified time and for the specified duration every day. |
| schedule monitor, on page 301 | Schedules an IP SLA MPLS LSP monitoring instance. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| **hourly** | Sets the distribution for statistics configuration that is aggregated for over an hour. |
| **interval** *seconds* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
```

```
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-mplslm-stats)#
```

## Related Commands

| Command | Description |
|---|---|
| buckets (statistics hourly), on page 220 | Sets the number of hours in which statistics are kept. |
| buckets (statistics interval), on page 221 | Refers to the data buckets in which the enhanced history statistics are kept. |
| distribution count, on page 228 | Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation. |
| distribution interval, on page 230 | Sets the time interval (in milliseconds) for each statistical distribution. |
| monitor, on page 258 | Configures an IP SLA MPLS LSP monitor instance. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| maximum hops, on page 254 | Sets the number of hops in which statistics are maintained for each path for the IP SLA operation. |
| maximum paths (IP SLA), on page 256 | 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

| | |
|---|---|
| *text* | (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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
```

```
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/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/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 1
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# tag mplslm-tag
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *destination-address* | IPv4 address of the target device to be tested. |
| *destination-mask* | Number of bits in the network mask of the target address. The network mask can be specified in either of two ways:<br>• 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.<br>• 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. |

## Command Default

None

## Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-ping)# target ipv4 192.168.1.4 255.255.255.255
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| *destination-address* | IPv4 address of the target device to be tested. |
| *circuit-id* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
```

```
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-trace)# target pseudowire 192.168.1.4 4211
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | 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

| | |
|---|---|
| **tunnel** *tunnel-interface* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-trace)# target traffic-eng tunnel 101
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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

| | |
|---|---|
| **lower-limit** *value* | Specifies the threshold lower-limit value. Range is 1 to 4294967295 ms. Default **lower-limit** value is 3000 ms. |
| **upper-limit** *value* | Specifies the threshold upper-limit value. Range is 5000 to 4294967295 ms. Default **upper-limit** 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
```

```
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type immediate, on page 362 | Takes action immediately upon a threshold violation. |
| threshold type xofy, on page 364 | 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

| | |
|---|---|
| *number-of-probes* | 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 **action** 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type average 8
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type immediate, on page 362 | Takes action immediately upon a threshold violation. |
| threshold type xofy, on page 364 | 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

| | |
|---|---|
| *occurrences* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/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/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# reaction monitor 2
```

```
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react-cond)# threshold type consecutive 2
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| reaction monitor, on page 283 | Configures MPLS LSP monitoring reactions. |
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type immediate, on page 362 | Takes action immediately upon a threshold violation. |
| threshold type xofy, on page 364 | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react  jitter-average
RP/0/RP0/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/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
```

```
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# reaction monitor 2
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-mplslm-react-cond)# threshold type immediate
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| reaction monitor, on page 283 | Configures MPLS LSP monitoring reactions. |
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type xofy, on page 364 | 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 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 use the **threshold type xofy** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type xofy 1 5
```

## Related Commands

| Command | Description |
|---|---|
| action (IP SLA), on page 215 | Specifies what action or combination of actions the operation performs. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |

| Command | Description |
|---|---|
| reaction operation, on page 285 | Configures certain actions that are based on events under the control of the IP SLA agent. |
| react, on page 277 | Specifies an element to be monitored for a reaction. |
| threshold, on page 356 | Sets the lower-limit and upper-limit values. |
| threshold type average, on page 358 | Takes action on average values to violate a threshold. |
| threshold type consecutive, on page 360 | Takes action after a number of consecutive violations. |
| threshold type immediate, on page 362 | 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

| | |
|---|---|
| *milliseconds* | 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 6.0 | This command was introduced. |

## 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.

**Note** If both the **frequency** and **timeout** values of an IPSLA UDP echo operation are the same, say, 1 s and 1000 ms respectively, the current probe iteration will exceed the configured frequency, say, 1002 ms, when the operation times out. As a result, the upcoming operation is skipped to ensure a correct operation interval cycle.

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/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/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)# timeout 10000
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *number* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# tos 60
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *time-to-live* | 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 6.0 | This command was introduced. |

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
```

```
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mpls-lsp-ping)# ttl 200
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | 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 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 use the **type icmp echo** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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 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 use the **type icmp path-echo** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

## Command History

| Release | Modification |
|---|---|
| Release 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 use the **type icmp path-jitter** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-jitter
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-jitter)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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 6.0 | This command was introduced. |

## 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 350 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 354 command)
- Pseudowire (configured with the target pseudowire, on page 352 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp ping
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp ping
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-ping)#
```

## Related Commands

| Command | Description |
|---|---|
| monitor, on page 258 | Configures an IP SLA MPLS LSP monitor instance. |
| operation, on page 261 | Configures an IP SLA operation. |
| schedule monitor, on page 301 | Schedules an IP SLA MPLS LSP monitoring instance. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp trace, on page 377 | 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 6.0 | This command was introduced. |

## 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 350 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 354 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type mpls lsp trace
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-trace)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule monitor, on page 301 | Schedules an IP SLA MPLS LSP monitoring instance. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type mpls lsp ping, on page 375 | 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

## Command History

| Release | Modification |
|---|---|
| Release 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 use the **type udp echo** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

## Command History

| Release | Modification |
|---|---|
| Release 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 use the **type udp jitter** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)#
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *ip-address* | Specifies the IPv4 address at which the operation is received. |
| **port** *port* | 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 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 configure a permanent port for the **type udp ipv4 address** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# responder
RP/0/RP0/CPU0:router(config-ipsla-resp)# type udp ipv4 address 192.0.2.11 port 10001
```

# 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

## Command History

| Release | Modification |
|---|---|
| Release 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 use the **verify-data** command in IP SLA UDP jitter configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# verify-data
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | 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

| | |
|---|---|
| *vrf-name* | 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 6.0 | 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 322 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# vrf vpn2
```

## Related Commands

| Command | Description |
|---|---|
| operation, on page 261 | Configures an IP SLA operation. |
| schedule operation, on page 302 | Schedules an IP SLA operation. |
| type udp jitter, on page 380 | Configures an IP SLA UDP jitter operation. |
| type icmp echo, on page 372 | Configures an IP SLA ICMP echo operation. |
| type icmp path-echo, on page 373 | Configures an IP SLA ICMP path-echo operation. |
| type icmp path-jitter, on page 374 | Configures an IP SLA ICMP path-jitter operation. |
| type udp echo, on page 379 | 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 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

| | |
|---|---|
| *vrf-name* | 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 6.0 | 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# mpls lsp-monitor
RP/0/RP0/CPU0:router(config-ipsla-mplslm)# monitor 2
RP/0/RP0/CPU0:router(config-ipsla-mplslm-def)# type mpls lsp trace
RP/0/RP0/CPU0:router(config-ipsla-mplslm-lsp-trace)# vrf vpn-lsp
```

## Related Commands

| Command | Description |
|---|---|
| monitor, on page 258 | Configures an IP SLA MPLS LSP monitor instance. |
| type mpls lsp ping, on page 375 | Tests connectivity in an LSP path in an MPLS VPN. |
| type mpls lsp trace, on page 377 | Traces the hop-by-hop route of an LSP path in an MPLS VPN. |



# Out Of Resource Handling Commands

This module describes the Cisco IOS XR Software commands to configure graceful handling of out of resource situations for system monitoring on the router.

For detailed information about graceful handling of out of resource concepts, configuration tasks, and examples, see the *Graceful Handling of Out of Resource Situations* chapter in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers*.


- oor hw, on page 388
- hw-module profile qos free-buffer-int-threshold, on page 389
- show controllers npu resources, on page 390
- show controllers npu resources qos, on page 394
- show grid pool, on page 397

# oor hw

To configure threshold values to handle Out of Resource (OOR) situations, use the **oor hw** command in XR Config mode. To remove the **oor hw** configuration file, use the **no** form of this command.

**oor hw threshold** { **red** | **yellow** } *threshold-value*

## Syntax Description

| | |
|---|---|
| **threshold** | Enables the threshold values of OOR states. |
| **red** | Specifies the OOR state, **Red**. |
| **yellow** | Specifies the OOR state, **Yellow**. |
| *threshold-value* | Specifies the threshold value for OOR state. |

## Command Default

The default threshold values for **Red** and **Yellow** OOR states are 95% and 80% respectively.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.1.1 | This command was introduced. |

## Task ID

| Task ID | Operations |
|---|---|
| config-services | read, write |

## Examples

This example shows how to enable threshold values for OOR states:

```
Router(config)#oor hw threshold red 90
Router(config)#oor hw threshold yellow 75
Router(config)#commit
```

# hw-module profile qos free-buffer-int-threshold

To configure threshold limits for Traffic Manager (TM) buffers, use the **hw-module profile qos free-buffer-int-threshold** command in the XR Config mode.

**hw-module profile qos free-buffer-int-threshold** *set-value* *clear-value*

## Syntax Description

| | |
|---|---|
| *set-value* | Configure the value at which the router should set the interrupt for TM free buffers.<br>Range: 0 - 100 |
| *clear-value* | Configure the value at which the router should clear the interrupt for TM free buffers.<br>Range: 0 - 100 |

## Command Default

These thresholds are not enabled by default.

If only *set-value* is configured then *clear-value* defaults to 100.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.7.1 | This command was introduced. |

## Usage Guidelines

You must reload all locations to enable the threshold values for free buffers.

The *set-value* should be configured lower than the *clear-value* .

## Task ID

| Task ID | Operation |
|---|---|
| qos | read, write |

The following example shows how to enable the wred-stats mode.

```
Router#config
Router(config)#hw-module profile qos free-buffer-int-threshold 50 75
Router(config)#commit
Router(config)#exit
Roueter#reload location all
```

# show controllers npu resources

To display the usage of Open Forwarding Abstraction (OFA) resources, use the **show controllers npu resources** command in the XR EXEC mode. OFA is an infrastructure layer which provides an abstraction interface for networking hardware.

**show controllers npu resources** { **fec** | **ecmpfec** | **encap** | **encapAC** | **encapPWE** | **encaptunnels** | **encapARP** | **all** } **location** { **all** *location-id* }

## Syntax Description

| | |
|---|---|
| **all** | Displays the usage of all the OFA hardware resources with respect to a single or all locations. |
| **fec** | Displays the usage of Forward Equivalence Class (FEC) hardware resources for a single location or all locations. |
| **ecmpfec** | Displays the usage of Equal Cost Multi-Path (ECMP) FEC hardware resources for a single location or all locations. |
| **encap** | Displays the usage of Egress Encapsulation Database (EEDB) hardware resources for a single location or all locations. |
| **encapAC** | Displays the usage of Egress Encapsulation Database (EEDB) for attachment circuit (AC) encapsulation for a single location or all locations. |
| **encapPWE** | Displays the usage of Egress Encapsulation Database (EEDB) for pseudowire encapsulation for a single location or all locations. |
| **encaptunnels** | Displays the usage of Egress Encapsulation Database (EEDB) for tunnel encapsulation for a single location or all locations. |
| **encapARP** | Displays the usage of Egress Encapsulation Database (EEDB) for Address Resolution Protocol (ARP) encapsulation for a single location or all locations. |
| **location** *location-id* | Displays the usage of a single or all resource type with respect to a specified location. |
| **location all** | Displays the usage of a single or all resource type for all locations. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.8.1 | The following optional keywords were introduced:<br>• **encapAC**<br>• **encapPWE**<br>• **encaptunnels**<br>• **encapARP** |
| Release 7.6.1 | Keyword **encap** was introduced. |
| Release 7.5.1 | Keywords **fec** and **ecmpfec** were introduced. |
| Release 7.1.1 | This command was introduced. |

## Task ID

| Task ID | Operations |
|---|---|
| interface | read |
| cisco-support | read |

The **show controllers npu resources** command displays Out of Resource (OOR) state.

```
Router# show controllers npu resources encap location 1/0/CPU0
HW Resource Information For Location: 0/1/CPU0
HW Resource Information
Name : encap
Asic Type : Jericho

NPU-0
OOR Summary
Red Threshold : 95 %
Yellow Threshold : 80 %


OFA Table Information
(May not match HW usage)
ipnh : 9
ip6nh : 0
mplsnh : 10984
llnh : 0
srv6nh : 0
ipvrf : 1
mplsmdtbud : 0
iptunnelencap : 0
tep : 0

Current Hardware Usage
Name: encap


Name: bank_0
Estimated Max Entries : 4096
Total In-Use : 2394 (58 %)
```

```
OOR State : Green
OOR State Change Time : 2021.Apr.16 00:22:36 WIB
Bank Info : phase=2 extended=no

--More--
Name: bank_1
Estimated Max Entries : 4096
Total In-Use : 12 (0 %)
OOR State : Green
Bank Info : phase=8 extended=no


Name: bank_2
Estimated Max Entries : 4096
Total In-Use : 9 (0 %)
OOR State : Green
Bank Info : phase=4 extended=no


Name: bank_3
Estimated Max Entries : 4096
Total In-Use : 2 (0 %)
OOR State : Green
OOR State Change Time : 2021.May.02 11:37:03 WIB
Bank Info : phase=2 extended=no


Name: bank_4
Estimated Max Entries : 4096
Total In-Use : 0 (0 %)
OOR State : Green
Bank Info : phase=0 extended=no


Name: bank_5
Estimated Max Entries : 4096
Total In-Use : 0 (0 %)
OOR State : Green
Bank Info : phase=0 extended=no


Name: bank_6
Estimated Max Entries : 4096
Total In-Use : 4096 (100 %)
OOR State : Red
OOR State Change Time : 2021.Apr.24 19:39:09 WIB
Bank Info : phase=1 extended=no


Name: bank_7
Estimated Max Entries : 4096
Total In-Use : 3 (0 %)
OOR State : Green
Bank Info : phase=4 extended=no


Name: bank_8
Estimated Max Entries : 4096
Total In-Use : 4096 (100 %)
OOR State : Red
OOR State Change Time : 2021.Apr.28 02:56:28 WIB
Bank Info : phase=1 extended=no
```

```
Name: bank_9
Estimated Max Entries : 4096
Total In-Use : 2477 (60 %)
OOR State : Green
```

View the encapsulation specific resource details using the respective keyword in the show command. For example, to view the resource details for attachment circuits, use the **show controllers npu resources encapAC** command:

```
Router# show controllers npu resources encapAC location 0/RP0/CPU0
HW Resource Information
    Name                            : encap_AC
    Asic Type                       : Jericho Two

NPU-0
OOR Summary
        Red Threshold               : 95 %
        Yellow Threshold            : 80 %


OFA Table Information
(May not match HW usage)
        ip6nh                       : 0
        ipmctxintf                  : 0
        l2intf                      : 0
        l2port                      : 0

Current J2 Hardware Usage

   Cluster Bank Pair: EEDB_S1_L1
    Max-Entries                     : 98304
    Total In-use                    : 18

    Logical_phase                   : 8 (Encap_Ac)
        Cluster Bank
           Bank Size                : S1
           Estimated Max Entries    : 98304
           OOR State                : Green
           Total In-Use             : 18

           EEDB Bank:
             Estimated Max Entries  : 8192
             OOR State              : Green
             Total In-Use           : 0

    Logical_phase                   : 2 (Encap_NativeArp)
        Cluster Bank
           Bank Size                : L1
           Estimated Max Entries    : 81920
           OOR State                : Green
           Total In-Use             : 0

           EEDB Bank:
             Estimated Max Entries  : 30720
             OOR State              : Green
             Total In-Use           : 0
```

# show controllers npu resources qos

To view the QoS utilization of some packet processing and traffic management resources, use the **show controllers npu resources qos** command in the XR EXEC mode.

**show controllers npu resources qos** [ **all** | **connectors** | **egq-profile** | **egress-qos-map** | **policer** | **rate-class-profile** | **voq** ] **instance** { *num* | **all** } **location** { **all** *location-id* }

## Syntax Description

| | |
|---|---|
| **all** | Displays the usage of the traffic management and packet processing hardware resources with respect to a single or all locations. |
| **connectors** | Displays the usage of the number of NPU connectors or Fabric Access Processors (FAP) for a single location or all locations. |
| **egq-profile** | Displays the usage of egress queue maps for a single location or all locations. They are consumed when you create egress policies with priority marking. |
| **egress-qos-map** | Displays the usage of resources used in creating traffic class and drop precedence (or discard class) maps for egress traffic. |
| **policer** | The number of policers that are allocated and that you can create. The total number of policer banks is inversely proportional to the class map size. |
| **rate-class-profile** | Displays the usage of rate profile pool for a single location or all locations. Interfaces with different line rates and policies with significantly differing shaper and queue lengths use rate profiles. |
| **voq** | Displays the usage of the number of Virtual Output Queues (VOQs) used at a global level from a common pool for a single location or all locations. |
| **instance** *number* | Displays the usage of a single or all resource types with respect to a specific ASIC number or instance to which the interface is mapped. |
| **instance** *all* | Displays the usage of a single or all resource types for all ASIC numbers or instances. |
| **location** *location-id* | Displays the usage of a single or all resource types with respect to a specified location. |
| **location all** | Displays the usage of a single or all resource types for all locations. |

## Command Default

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.11.1 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |
| cisco-support | read |

The **show controllers npu resources qos** command displays usage of packet processing and traffic management resources.

```
Router#show controllers npu resources qos all instance all location 0/0/CPU0

========================================================================
QoS TM Connectors Information For Location: 0/0/CPU0

System information for NPU 0:
Core 0:
                             Used(   %)       Free      Total   Reserved      Per Interface
 Consumption
    Normal Connector Set:        384(  0%)      59008      59392       6144
              16
   Lowrate connector Set:          0(  0%)          0          0

Core 1:
                             Used(   %)       Free      Total   Reserved      Per Interface
 Consumption
    Normal Connector Set:        384(  0%)      59008      59392       6144
              16
   Lowrate connector Set:          0(  0%)          0          0

========================================================================
QoS TM Rate Profile Information:
Note: - This is a global resource and shared across all LCs

                                Used(   %)       Free      Total     Reserved    Highest
Used
                                   3(  5%)         56         59            5
  3

========================================================================
QoS TM EGQ Profile Information For Location: 0/0/CPU0

System information for NPU 0:
Core 0:
                                Used(   %)       Free      Total
                                   8(100%)          0          8

Core 1:
                                Used(   %)       Free      Total
                                   8(100%)          0          8

========================================================================
```

```
QoS PP Policer Banks Information For Location: 0/0/CPU0

System information for NPU 0:
Core 0:
                               Used(   %)       Free      Total       Class-map size
      Policer Banks info:         0(  0%)        218        218                   32

Core 1:
                               Used(   %)       Free      Total       Class-map size
      Policer Banks info:         0(  0%)        218        218                   32

======================================================================
QoS PP Egress QoS Map Information For Location: 0/0/CPU0

System information for NPU 0:      Used(   %)       Free      Total
         L2 Profile Pool:             0(  0%)         14         14
         L3 Profile Pool:             0(  0%)          3          3

======================================================================
QoS VOQ Information For Location: 0/0/CPU0

Note:- This is a global resources shared by all NPUs

                               Used(   %)       Free      Total
               VOQ info:       175(  1%)      11984      12159
```

# show grid pool

To display the utilization of banks in the NPU resources, use the **show grid pool** command in the XR EXEC mode.

**show grid pool** { *pool-id* | **all** } [ **bank** { *bank-id* | **all** } ]

**Syntax Description**

| | |
|---|---|
| *pool-id* | Displays the utilization of pool in the NPU resource.<br>Range: 0 - 16 |
| *bank-id* | Displays the utilization of bank in the specified pool<br>Range: 0 - 255 |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.5.3 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |
| cisco-support | read |

**Examples**

The following example shows how to check the utilization of resources in the bank:

```
Router# show grid pool 1 bank all
Tue Jul 26 11:44:24.960 UTC
Bank Ptr : 0x308ca4bd50
Bank ID : 0
Pool : RIF (id 1)
Bank Start : -1
Bank End : -1
Max Bank Size : 1
Max Resource Pages : 1
Available resource IDs : 1 (100.000% free)
Alarm state : Green
Bank statistics: Success Error (since last clear)
Resource IDs reserved 0 0 0 0
Resource IDs returned 0 0 0 0
Bank Ptr : 0x308ca4bdb8
Bank ID : 1
Pool : RIF (id 1)
Bank Start : 6
Bank End : 8192
Max Bank Size : 8187
```

```
Max Resource Pages : 256
Available resource IDs : 8119 (99.169% free)
Alarm state : Green
HW Resources:
RIF_VSI
Bank statistics: Success Error (since last clear)
Resource IDs reserved 986 0 986 0
Resource IDs returned 918 0 918 0
Client : vlan-fib
Resource IDs reserved 933 0 933 0
Resource IDs returned 865 0 865 0
current usage : 68
Client : ip-tunnel
Resource IDs reserved 32 0 32 0
Resource IDs returned 32 0 32 0
current usage : 0
Client : redirectvrf
Resource IDs reserved 1 0 1 0
Resource IDs returned 1 0 1 0
current usage : 0
Client : l2vpn-mgr
Resource IDs reserved 20 0 20 0
Resource IDs returned 20 0 20 0
current usage : 0
```

***Table 37: Show grid pools field descriptions***

| Field | Description |
|---|---|
| Bank Ptr | Banks memory address |
| Bank ID | Banks unique bank ID |
| Pool ID | Banks resource pool name and ID |
| Bank Start | Banks starting index |
| Bank End | Banks ending index |
| Max Bank Size | Banks total capacity |
| Max Resource Pages | Banks total page capacity |



# Tech-Support Commands

This module describes commands used to collect the **show** command outputs using Cisco IOS XR software.

The **show tech-support** commands collect common data from commands such as **show version** . Each **show tech-support** command also generates and gathers relevant data for a specific area. This data includes trace output to collect debugging information available in the specific area of interest.

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.


- show tech-support custom, on page 400
- show tech-support mgbl, on page 413
- show tech-support mgbl grpc, on page 415
- show tech-support mgbl netconf, on page 417
- show tech-support mgbl telemetry, on page 419
- show tech-support multicast address-family, on page 421
- show tech-support ztp brief, on page 423

# show tech-support custom

To generate and gather tech-support information related to a specific area such as network traffic, control-plane, and the system, use the **show tech-support custom** command in EXEC mode.

**show tech-support custom** { **traffic** | **control-plane** | **system** | **sysadmin** }

## Syntax Description

| | |
|---|---|
| **traffic** | Generates tech-support information related to network traffic. |
| **control-plane** | Generates tech-support information related to the control-plane. |
| **system** | Generates tech-support information related to the system. |
| **sysadmin** | Generates tech-support information related to the system-admin profile. |

## Command Default

None

## Command Modes

EXEC mode

Config mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.6 | The **sysadmin** option was introduced. |
| Release 7.3.5 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

*Table 38: List of Commands collected by each custom option*

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| Control-plane | Release 7.3.6 | |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support aib<br>show tech-support ipv6 nd<br>show tech-support arp<br>show tech-support service-layer<br>show tech-support routing bgp<br>show tech-support routing isis<br>show tech-support routing bfd<br>show tech-support bfdhwoff<br>show tech-support mpls ldp<br>show tech-support bcdlv2<br>show tech-support rib<br>show tech-support mpls lsd<br>show tech-support cef<br>show tech-support cef platform<br>show tech-support gsp<br>show tech-support l2rib<br>show tech-support l2vpn<br>show tech-support lpts<br>show tech-support spp<br>show tech-support clns<br>show tech-support fabric<br>show tech-support l2vpn evpn<br>show tech-support tunnel-ip<br>show tech-support grpc<br>show tech-support appmgr<br>show tech-support netconf<br>show tech-support yserver<br>show tech-support access-lists ipv4<br>show tech-support access-lists ipv6<br>show tech-support bcdl<br>show tech-support bundles<br>show tech-support dhcp ipv4 base<br>show tech-support dhcp ipv4 client |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support dhcp ipv4 proxy<br>show tech-support dhcp ipv4 relay<br>show tech-support dhcp ipv4 server<br>show tech-support dhcp ipv4 snoop<br>show tech-support dhcp ipv6 base<br>show tech-support dhcp ipv6 client<br>show tech-support dhcp ipv6 proxy<br>show tech-support dhcp ipv6 relay<br>show tech-support dhcp ipv6 server<br>show tech-support flowspec<br>show tech-support ipinfra<br>show tech-support pbr<br>show tech-support placed<br>show tech-support raw<br>show tech-support rsi<br>show tech-support spio<br>show tech-support static<br>show tech-support sysdb<br>show tech-support tcp nsr<br>show tech-support udp<br>show tech-support pfi<br>show tech-support cfgmgr<br>show tech-support tty<br>show tech-support rdsfs |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| Traffic | Release 7.3.6 | |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support access-lists ethernet-services<br>show tech-support access-lists ipv4<br>show tech-support access-lists ipv6<br>show tech-support aib<br>show tech-support arp<br>show tech-support bcdl<br>show tech-support bcdlv2<br>show tech-support bfdhwoff<br>show tech-support bundles<br>show tech-support cef<br>show tech-support cef platform<br>show tech-support cfgmgr<br>show tech-support dhcp ipv4 base<br>show tech-support dhcp ipv4 client<br>show tech-support dhcp ipv4 proxy<br>show tech-support dhcp ipv4 relay<br>show tech-support dhcp ipv4 server<br>show tech-support dhcp ipv4 snoop<br>show tech-support dhcp ipv6 base<br>show tech-support dhcp ipv6 client<br>show tech-support dhcp ipv6 proxy<br>show tech-support dhcp ipv6 relay<br>show tech-support dhcp ipv6 server<br>show tech-support ethernet cfm pd<br>show tech-support ethernet interfaces<br>show tech-support ethernet platform<br>show tech-support ethernet protocols oam<br>show tech-support ethernet service-activation-test<br>show tech-support fabric<br>show tech-support flowspec<br>show tech-support grid<br>show tech-support gsp<br>show tech-support ipinfra |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support ipv6 nd<br>show tech-support l2rib<br>show tech-support l2vpn<br>show tech-support l2vpn evpn<br>show tech-support l2vpn platform<br>show tech-support lpts<br>show tech-support mirror<br>show tech-support mpls lsd<br>show tech-support mpls oam<br>show tech-support mpls rsvp<br>show tech-support mpls static<br>show tech-support mpls traffic-eng<br>show tech-support netflow<br>show tech-support ofa<br>show tech-support optics<br>show tech-support pbr<br>show tech-support pfi<br>show tech-support placed<br>show tech-support platform-pfc<br>show tech-support protection-notif<br>show tech-support qos pi<br>show tech-support qos platform<br>show tech-support qos tm<br>show tech-support raw<br>show tech-support resmon<br>show tech-support rib<br>show tech-support routing bfd<br>show tech-support rsi<br>show tech-support secy<br>show tech-support segment-routing traffic-eng<br>show tech-support snmp ifmib<br>show tech-support span<br>show tech-support spio |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support spp<br>show tech-support static<br>show tech-support statsd<br>show tech-support statsd<br>show tech-support sysdb<br>show tech-support tcp nsr<br>show tech-support tunnel-ip<br>show tech-support udp |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| System | Release 7.3.6 | |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support spi<br>show tech-support ofa<br>show tech-support optics<br>show tech-support gsp<br>show tech-support platform timing<br>show tech-support gnss platform<br>show tech-support ptp<br>show tech-support frequency synchronization<br>show tech-support ethernet controllers<br>show tech-support ethernet interfaces<br>show tech-support pfi<br>show tech-support protection-notif<br>show tech-support cfgmgr<br>show tech-support sysdb<br>show tech-support processmgr<br>show tech-support grpc<br>show tech-support telemetry model-driven<br>show tech-support parser<br>show tech-support fabric<br>show tech-support secy<br>show tech-support macsec<br>show tech-support keychain<br>show tech-support kim<br>show tech-support ntp<br>show tech-support placed<br>show tech-support pmengine<br>show tech-support pool<br>show tech-support rdsfs<br>show tech-support resmon<br>show tech-support sdr-invmgr<br>show tech-support sdr-mgbl-proxy<br>show tech-support shmwin<br>show tech-support snmp |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| | | show tech-support ssh<br>show tech-support system-recovery<br>show tech-support tacacs<br>show tech-support tty<br>show tech-support type6<br>show tech-support ztp<br>show tech-support alarm-mgr<br>show tech-support cepki<br>show tech-support statsd<br>show tech-support bundles<br>show tech-support snmp ifmib<br>show tech-support ipinfra<br>show tech-support cef<br>show tech-support cef platform<br>show tech-support rsi |

| Custom Option | Release | List of commands outputs collected |
|---|---|---|
| Sysadmin | Release 7.3.6 | admin show tech-support HBloss<br>admin show tech-support aaa<br>admin show tech-support alarm_mgr<br>admin show tech-support card-mgr<br>admin show tech-support cm<br>admin show tech-support confd<br>admin show tech-support control-ethernet<br>admin show tech-support ctrace<br>admin show tech-support ds<br>admin show tech-support envmon<br>admin show tech-support fabric<br>admin show tech-support fpd<br>admin show tech-support install<br>admin show tech-support obfl<br>admin show tech-support os<br>admin show tech-support pm<br>admin show tech-support sdr_mgr<br>admin show tech-support shelf_mgr<br>admin show tech-support syslog<br>admin show tech-support tacacs-server<br>admin show tech-support tam |

**Note** This command is not required during normal use of the router.

**Task ID**

| Task ID | Operations |
|---|---|
| basic-services or cisco-support | read |

The following example shows the output of the **show tech-support custom traffic** command:

```
Router# show tech-support custom traffic
++ Show tech start time: 2023-Jun-16.195852.UTC ++
Fri Jun 16 19:58:52 UTC 2023 Waiting for gathering to complete
.....................................................................................................
Fri Jun 16 20:05:45 UTC 2023 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
```

```
/harddisk:/showtech/showtech-custom-traffic-2023-Jun-16.195852.UTC.tgz
++ Show tech end time: 2023-Jun-16.200546.UTC ++
```

The following example shows the output of the **show tech-support custom control-plane** command:

```
Router# show tech-support custom control-plane
++ Show tech start time: 2023-Jun-16.194006.UTC ++
Fri Jun 16 19:40:06 UTC 2023 Waiting for gathering to complete
.....................................................................................
Fri Jun 16 19:44:59 UTC 2023 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-custom-control-2023-Jun-16.194006.UTC.tgz
++ Show tech end time: 2023-Jun-16.194459.UTC ++
```

The following example shows the output of the **show tech-support custom system** command:

```
Router# show tech-support custom system
++ Show tech start time: 2023-Jun-16.194549.UTC ++
Fri Jun 16 19:45:50 UTC 2023 Waiting for gathering to complete
.....................................................................................................................
Fri Jun 16 19:54:24 UTC 2023 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-custom-system-2023-Jun-16.194549.UTC.tgz
++ Show tech end time: 2023-Jun-16.195425.UTC ++
```

The following example shows the output of the **show tech-support custom sysadmin** command:

```
Router# show tech-support custom sysadmin
Thu Jan 11 17:45:46.429 PST
++ Show tech start time: 2024-Jan-11.174606.PST ++
Thu Jan 11 17:46:07 PST 2024 Waiting for gathering to complete
.Thu Jan 11 17:46:10 PST 2024 Waiting for Sysadmin show tech-support collection
................................Thu Jan 11 18:17:11 PST 2024 Please collect Admin show
tech-support ctrace in addition to any sysadmin show-tech-support collection

Thu Jan 11 18:17:11 PST 2024 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-F9-custom-sys-admin-2024-Jan-11.174606.PST.tgz
++ Show tech end time: 2024-Jan-11.181723.PST ++
```

# show tech-support mgbl

To collect the logs or traces for gRPC module, Network Configuration Protocol (NETCONF) module, and telemetry, use the **show tech-support mgbl** command in the XR EXEC mode.

**show tech-support mgbl {file | grpc | list-CLIs | location | netconf | rack | telemetry | time-out}**

## Syntax Description

| | |
|---|---|
| **mgbl** | Executes the commands for manageability components. |
| **file** | Specifies a file name with or without a file path where the output is stored.<br>You can either specify the filename or the path of the file.<br>• To specify only the name of the file, use this command:<br>**show tech-support mgbl file** *filename*<br>• To specify the file path, use this command:<br>**show tech-support mgbl file** *filepath*<br>Valid file path options are:<br>• **apphost:** *filename*<br>• **config:** *filename*<br>• **disk0:** *filename*<br>• **ftp:** *filename*<br>• **harddisk:** *filename*<br>• **rootfs:** *filename*<br>• **tftp:** *filename* |
| **grpc** | Collects the logs or traces for gRPC module. |
| **list-CLIs** | Lists the CLIs related to the manageability components. |
| **location** | Specifies the node location. |
| **netconf** | Collects the logs or traces for Network Configuration Protocol (NETCONF) module. |
| **rack** | Specifies the rack (0/1/2). |
| **telemetry** | Collects the logs or traces for telemetry. |
| **time-out** | Specifies the timeout configuration for each show command in seconds. The default value is 900 seconds and its ranges between 120-3600 seconds. |

## Command Default

- The command output is compressed.
- The command does not support location-based collection.

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 24.1.1 | This command was introduced. |

**Usage Guidelines**

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

This example shows the output of the **show tech-support mgbl** command.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl ?
  file       Specify a valid file name (e.g. disk0:tmp.log)
  grpc       Collect showtech for grpc(cisco-support)
  list-CLIs  list the commands that would be run (don't execute)(cisco-support)
  location   Specify a location(cisco-support)
  netconf    Collect showtech for netconf(cisco-support)
  rack       Specify a rack(cisco-support)
  telemetry  Collect showtech for telemetry(cisco-support)
  time-out   per show command timeout configuration(cisco-support)
  <cr>
```

**Note** The **show tech-support mgbl**command does not support location-based collection.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl location 0/RP0/CPU0
Mon Feb 19 02:37:03.652 UTC
++ Show tech start time: 2024-Feb-19.023703.UTC ++
This show tech-support doesn't support location based collection. Exiting.
++ Show tech end time: 2024-Feb-19.023703.UTC ++
```

# show tech-support mgbl grpc

To collect the logs or traces for gRPC module, use the **show tech-support mgbl grpc** command in the XR EXEC mode.

**show tech-support mgbl grpc file** *{filename | filepath}*

## Syntax Description

| | |
|---|---|
| **mgbl** | Executes the commands for manageability components. |
| **grpc** | Collects the logs or traces for gRPC module. |
| **file** | Specifies a file name with or without a file path where the output is stored. |
| *filename* | Specifies the name of the file.<br>**show tech-support mgbl grpc file** *filename* |
| *filepath* | Specifies the file path with the file name.<br>**show tech-support mgbl grpc file** *filepath*<br>Valid file path options are:<br>• **apphost:** *filename*<br>• **config:** *filename*<br>• **disk0:** *filename*<br>• **ftp:** *filename*<br>• **harddisk:** *filename*<br>• **rootfs:** *filename*<br>• **tftp:** *filename* |

## Command Default

- The command output is compressed.
- The command does not support location-based collection.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 24.1.1 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

This example shows the output of the **show tech-support mgbl grpc file** command.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl grpc file disk0:tmp.log
Fri Feb  2 06:12:15.098 UTC
++ Show tech start time: 2024-Feb-02.061215.UTC ++
Fri Feb  2 06:12:16 UTC 2024 Waiting for gathering to complete
............
Fri Feb  2 06:12:53 UTC 2024 Compressing show tech output
Show tech output available at 0/RP0/CPU0 : /disk0:/tmp.log.tgz
++ Show tech end time: 2024-Feb-02.061254.UTC ++
```

**Note** The **show tech-support mgbl grpc** command does not support location-based collection.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl grpc location 0/RP0/CPU0
Fri Feb  2 06:13:34.590 UTC
++ Show tech start time: 2024-Feb-02.061334.UTC ++
This show tech-support doesn't support location based collection. Exiting.
++ Show tech end time: 2024-Feb-02.061335.UTC ++
```

# show tech-support mgbl netconf

To collect the logs or traces for Network Configuration Protocol (NETCONF) module, use the **show tech-support mgbl netconf** command in the XR EXEC mode.

**show tech-support mgbl netconf file** *{filename | filepath}*

## Syntax Description

| | |
|---|---|
| **mgbl** | Executes the commands for manageability components. |
| **netconf** | Collects the logs or traces for Network Configuration Protocol (NETCONF) module. |
| **file** | Specifies a file name with or without a file path where the output is stored. |
| *filename* | Specifies the name of the file.<br>**show tech-support mgbl netconf file** *filename* |
| *filepath* | Specifies the file path with the file name.<br>**show tech-support mgbl netconf file** *filepath*<br>Valid file path options are:<br>• **apphost:** *filename*<br>• **config:** *filename*<br>• **disk0:** *filename*<br>• **ftp:** *filename*<br>• **harddisk:** *filename*<br>• **rootfs:** *filename*<br>• **tftp:** *filename* |

## Command Default

- The command output is compressed.
- The command does not support location-based collection.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 24.1.1 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

This example shows the output of the **show tech-support mgbl netconf file** command.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl netconf file disk0:tmp.log
Fri Feb  2 06:12:15.098 UTC
++ Show tech start time: 2024-Feb-02.061215.UTC ++
Fri Feb  2 06:12:16 UTC 2024 Waiting for gathering to complete
............
Fri Feb  2 06:12:53 UTC 2024 Compressing show tech output
Show tech output available at 0/RP0/CPU0 : /disk0:/tmp.log.tgz
++ Show tech end time: 2024-Feb-02.061254.UTC ++
```



**Note** The **show tech-support mgbl netconf** command does not support location-based collection.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl netconf location 0/RP0/CPU0
Fri Feb  2 06:13:34.590 UTC
++ Show tech start time: 2024-Feb-02.061334.UTC ++
This show tech-support doesn't support location based collection. Exiting.
++ Show tech end time: 2024-Feb-02.061335.UTC ++
```

# show tech-support mgbl telemetry

To collect the logs or traces for telemetry, use the **show tech-support mgbl telemetry** command in the XR EXEC mode.

**show tech-support mgbl telemetry file** *{filename | filepath}*

## Syntax Description

| | |
|---|---|
| **mgbl** | Executes the commands for manageability components. |
| **telemetry** | Collects the logs or traces for telemetry. |
| **file** | Specifies a file name with or without a file path where the output is stored. |
| *filename* | Specifies the name of the file.<br>**show tech-support mgbl telemetry file** *filename* |
| *filepath* | Specifies the file path with the file name.<br>**show tech-support mgbl telemetry file** *filepath*<br>Valid file path options are:<br>• **apphost:** *filename*<br>• **config:** *filename*<br>• **disk0:** *filename*<br>• **ftp:** *filename*<br>• **harddisk:** *filename*<br>• **rootfs:** *filename*<br>• **tftp:** *filename* |

## Command Default

- The command output is compressed.
- The command does not support location-based collection.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 24.1.1 | This command was introduced. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

This example shows the output of the **show tech-support mgbl telemetry file** command.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl telemetry file disk0:tmp.log
Fri Feb  2 06:12:15.098 UTC
++ Show tech start time: 2024-Feb-02.061215.UTC ++
Fri Feb  2 06:12:16 UTC 2024 Waiting for gathering to complete
............
Fri Feb  2 06:12:53 UTC 2024 Compressing show tech output
Show tech output available at 0/RP0/CPU0 : /disk0:/tmp.log.tgz
++ Show tech end time: 2024-Feb-02.061254.UTC ++
```

**Note** The **show tech-support mgbl telemetry** command does not support location-based collection.

```
RP/0/RP0/CPU0:R0#show tech-support mgbl telemetry location 0/RP0/CPU0
Fri Feb  2 06:13:34.590 UTC
++ Show tech start time: 2024-Feb-02.061334.UTC ++
This show tech-support doesn't support location based collection. Exiting.
++ Show tech end time: 2024-Feb-02.061335.UTC ++
```

# show tech-support multicast address-family

To collect the logs related to the multicast configurations specific to the address-family on the device, use the **show tech-support multicast address-family** command in the XR EXEC mode.

**show tech-support multicast address-family** { **ipv4** | **ipv6** } **hardware**

## Syntax Description

| | |
|---|---|
| **multicast** | Shows multicast related information |
| **address-family** | Collects Global Table address family specific information. |
| **ipv4** \| **ipv6** | Collects ipv4 or ipv6 information. |
| **hardware** | Specifies the hardware platform information. |

## Command Default

- The command output is compressed.

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 24.4.1 | The command was modified to include multicast information. |

## Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/***name.tgz* **tftp://***server_path*.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

## Task ID

| Task ID | Operations |
|---|---|
| cisco-support | read |

This example shows the output of the **show tech-support multicast address-family ipv4 hardware** command.

```
RP/0/RP0/CPU0:R0#show tech-support multicast address-family ipv4 hardware
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 Rte, seq #1 route: action commit for
 route (192.0.2.1,198.51.100.1/64) End [Slotmask: 0x1, MGID: 517]
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 Rte, seq #1 route: action commit for
 route (192.0.2.1,198.51.100.1/64) event
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 IDB ctx, seq #1 Platform_idb_opera
DONE action 0x4000 idb ifh 0x2000160 interface type 0x3
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 Intf del, seq #3 RPF signal flag for
 (192.0.2.1,198.51.100.1/64) is set to 0
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 Intf del, seq #2 Successfully turned
 A flag OFF for Bundle-Ether1 (0x2000160) in route (192.0.2.1,198.51.100.1/64)
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629         intf-type=3, mdt-type=0,
#bundle-members=0
```

```
Oct 14 07:15:45.161 mfwd_ipv4_hw/event 0/0/CPU0 t6629 intf: action delete intf Bundle-Ether1
 ifh 0x2000160 non-local (ul ifh 0x0) for route (192.0.2.1,198.51.100.1/64)
```

# show tech-support ztp brief

To collect a brief summary of ZTP show tech information after a reimage, use the **show tech-support ztp brief** command in EXEC mode.

**show tech-support ztp brief**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 26.2.1 | This command was introduced. |

**Usage Guidelines**

During a reimage or reload, any ZTP logs collecte prior to the reimage are removed. Only logs from the new boot time onward are retained. To preserve pre-reimage logs for troubleshooting, we recommend you to create a backup of log files during the reimage process.

The **show tech-support ztp brief** command provides a summarized view of ZTP tech-support data. The command does not collect the pre-reimage logs (`var_log_pre_reimage.tgz`).

The **show tech-support ztp brief**complements the **show tech-support ztp** command, which collects more comprehensive debugging information, including pre-reimage logs (`var_log_pre_reimage.tgz`) for in-depth troubleshooting of ztp issues.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

The following example shows the ztp logs collected using the **show tech-support ztp brief** command:

```
Router# #show tech-support ztp brief
Tue May 26 09:58:24.837 UTC
++ Show tech start time: 2026-May-26.095825.UTC ++
Tue May 26 09:58:32 UTC 2026 Waiting for gathering to complete
...
Tue May 26 09:58:49 UTC 2026 Compressing show tech output
Compressed 22544384 bytes into 22544423 bytes ==> 100.00%
Show tech output available at 0/RP0/CPU0 : /harddisk:/showtech/showtech-SFDR1-ZT

P-2026-May-26.095825.UTC.tar.lz4
++ Show tech end time: 2026-May-26.095850.UTC ++
```



# Traffic Monitoring Commands

This module describes the Cisco IOS XR Software commands to monitor traffic on the router.

For detailed information about monitoring traffic concepts, configuration tasks, and examples, see the *Traffic Monitoring* chapter in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers*.


- show controllers npu exttcamipv4, on page 426
- show controllers npu exttcamipv6, on page 428
- show drops all, on page 430
- show controllers npu stats counters-all, on page 433
- show controllers npu stats traps-all, on page 436
- show controllers npu stats voq, on page 439
- show fwd statistics, on page 443
- show spp client, on page 446
- show spp node-counters, on page 449
- show controllers fia diagshell, on page 453
- show controllers fia statistics, on page 455
- show netio drops, on page 459

# show controllers npu exttcamipv4

To display informations of external TCAM for ipv4, use the **show controllers npu exttcamipv4** command in EXEC mode.

**show controllers npu exttcamipv4 location**

## Syntax Description

| | |
|---|---|
| **exttcamipv4 location** | Displays summary information external TCAM for ipv4 like hardware information and ORR summary of selected location. |

## Command Default

No default behavior or values

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.5 | The command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| npu | read |

This example display informations of external TCAM for ipv4 on the router:

```
Router# sh controllers npu resources exttcamipv4 location 0/RP0/CPU0
HW Resource Information
    Name                            : ext_tcam_ipv4
    Asic Type                       : Jericho Two

NPU-0
OOR Summary
        Estimated Max Entries       : 1838024
        Red Threshold               : 95 %
        Yellow Threshold            : 80 %
        OOR State                   : Green
        High Water Mark             : 1100203
        High Water Mark Time        : 2025.Jun.17 11:37:02 BST
        Bank Info                   : ext_tcam_ipv4

OFA Table Information
(May not match HW usage)
        iproute                     : 1100203

Current Hardware Usage
    Name: ext_tcam_ipv4
        Estimated Max Entries       : 1838024
        Total In-Use                : 1099631  (59 %)
        OOR State                   : Green
        High Water Mark             : 1100203
```

```
High Water Mark Time        : 2025.Jun.17 11:37:02 BST
Bank Info                   : ext_tcam_ipv4
```

# show controllers npu exttcamipv6

To display informations of external TCAM for ipv6, use the **show controllers npu exttcamipv6** command in EXEC mode.

**show controllers npu exttcamipv6 location**

## Syntax Description

| | |
|---|---|
| **exttcamipv6 location** | Displays summary information external TCAM for ipv6 like hardware information and ORR summary of selected location. |

## Command Default

No default behavior or values

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.5 | The command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operation |
|---|---|
| npu | read |

This example display informations of external TCAM for ipv6 on the router:

```
Router# sh controllers npu resources exttcamipv6 location 0/RP0/CPU0
HW Resource Information
    Name                            : ext_tcam_ipv6
    Asic Type                       : Jericho Two

NPU-0
OOR Summary
        Estimated Max Entries       : 1769611
        Red Threshold               : 95 %
        Yellow Threshold            : 80 %
        OOR State                   : Green
        High Water Mark             : 250166
        High Water Mark Time        : 2025.Jun.17 11:28:11 BST
        Bank Info                   : ext_tcam_ipv6

OFA Table Information
(May not match HW usage)
        ip6route                    : 166

Current Hardware Usage
    Name: ext_tcam_ipv6
        Estimated Max Entries       : 1769611
        Total In-Use                : 166      (0 %)
        OOR State                   : Green
        High Water Mark             : 250166
```

```
High Water Mark Time        : 2025.Jun.17 11:28:11 BST
Bank Info                   : ext_tcam_ipv6
```

# show drops all

To display the exact packet drop location in a node, use the **show drops all** command in the XR EXEC mode.

**show drops all** { **commands location** | **location** | **ongoing location** } { *node-id* | **all** }

**Syntax Description**

| | |
|---|---|
| **commands** | Displays commands executed. |
| **location** | Specifies location of line card or route processor. |
| **ongoing** | Shows drops occuring since last executed. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |
| cisco-support | read |

The **show drops all location all** command displays packet drops for all nodes on all locations.

The command outputs given here are truncated.

```
RP/0/RP0/CPU0:ios#show drops all location all
====================================
Checking for drops on 0/4/CPU0
====================================


show controllers npu stats counters-all instance all location:
[np:Slot: 4, instance: 2] ENQ_DISCARDED_PACKET_COUNTER   : 48
[np:Slot: 4, instance: 3] ENQ_DISCARDED_PACKET_COUNTER   : 38


show controllers npu stats counters-all detail instance all location:
.
.
.
[np:Slot: 4, instance: 5] FDR P1FDRDscrdCntA                  : 4536
[np:Slot: 4, instance: 5] FDR P1FDRDscrdCntB                  : 4536



show spp node-counters:
```

```
[spp:fretta/classify] dropped in classify node: 6
[spp:fretta/classify] lnx l2 drop in classify node: 6


show controller fia statistics detail instance all location:
.
.
.
[fia:FIA Statistics Rack: 0, Slot: 4, instance: 2] FDR P1FDRDscrdCntA: 4536
[fia:FIA Statistics Rack: 0, Slot: 4, instance: 2] FDR P1FDRDscrdCntB: 4536
[fia:FIA Statistics Rack: 0, Slot: 4, instance: 2] FDR P2FDRDscrdCntA: 4536
[fia:FIA Statistics Rack: 0, Slot: 4, instance: 2] FDR P2FDRDscrdCntB: 4536


show controller fia diagshell all "diag counter nZ" location:
.
.
.
[fia:R/S/I: 0/4/0] DRCA0 DrcaCntGddr5BistDataErrGlobal: 96
[fia:R/S/I: 0/4/0] DRCA0 DrcaCntGddr5BistDbiErrGlobal: 96
[fia:R/S/I: 0/4/0] DRCB0 DrcbCntGddr5BistDataErrGlobal: 96
[fia:R/S/I: 0/4/0] DRCB0 DrcbCntGddr5BistDbiErrGlobal: 96
[fia:R/S/I: 0/4/0] DRCC0 DrccCntGddr5BistDbiErrGlobal: 96
```

The **show drops all ongoing location all** command displays the packet drops since last executed.

```
Router#show drops all ongoing location all
====================================
Checking for ongoing drops on 0/4/CPU0
====================================
filtering...


====================================
Checking for ongoing drops on 0/4/CPU0
====================================


====================================
Checking for ongoing drops on 0/3/CPU0
====================================


show controllers npu stats counters-all instance all location:
.
.
.
[np:Slot: 3, instance: 3] ENQ_DISCARDED_PACKET_COUNTER   : +1950


show controllers npu stats counters-all detail instance all location:
[np:Slot: 3, instance: 0] IQM1 TotDscrdByteCnt                : +133008


show controller fia statistics detail instance all location:

[fia:FIA Statistics Rack: 0, Slot: 3, instance: 0] IQM0 QueueEnqDscrdPktCnt: +1304

show controller fia diagshell all "diag counter nZ" location:
.
.
.
[fia:R/S/I: 0/3/1] IQM0 IqmQueueEnqDiscardedPacketCounter: +45
```

```
====================================
Checking for ongoing drops on 0/RP0/CPU0
====================================


show interfaces:
[Interface:Bundle-Ether10000] input errors: +65
[Interface:Bundle-Ether10001] input errors: +65
[Interface:Bundle-Ether10002] input errors: +65
[Interface:Bundle-Ether10003] input errors: +64
[Interface:Bundle-Ether10004] input errors: +65
[Interface:Bundle-Ether10005] input errors: +65
[Interface:Bundle-Ether10006] input errors: +65
[Interface:Bundle-Ether10007] input errors: +64
[Interface:Bundle-Ether10008] input errors: +64
[Interface:Bundle-Ether10009] input errors: +65
[Interface:Bundle-Ether20001] input errors: +65

====================================
Checking for ongoing drops on 0/2/CPU0
====================================

show controller fia statistics detail instance all location:
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IqmCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IqmCntCmdErrorsFilterB: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IrppCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IrppCntCmdErrorsFilterB: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM1 IqmCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM1 IqmCntCmdErrorsFilterB: +4590


show controller fia diagshell all "diag counter nZ" location:
[fia:R/S/I: 0/2/0] IPS0 IpsFsmrqDelayCounter: +9
[fia:R/S/I: 0/2/0] IPS1 IpsFsmrqDelayCounter: +7
[fia:R/S/I: 0/2/1] IPS0 IpsFsmrqDelayCounter: +10
[fia:R/S/I: 0/2/1] IPS1 IpsFsmrqDelayCounter: +7


show interfaces:
[Interface:HundredGigE0/2/0/28] input errors: +113
```

# show controllers npu stats counters-all

To display the various statistics for the NPU, use the **show controllers npu stats counters-all** command in the XR EXEC mode.

**show controller npu stats counters-all** { **detail instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **detail instance** *instance-id* | Displays detailed information about a given instance. |
| **detail instance** *all* | Displays detailed information about all instances. |
| **instance** *instance-id* | Displays information about a given instance. |
| **instance** *all* | Displays information about all instances. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |

| Task ID | Operations |
|---|---|
| filesystem | read, write |
| cisco-support | read |

## Examples

The **show controllers npu stats counters-all** command displays the NPU statistics for all instance and all locations.

```
Router# show controller npu stats counters-all instance all location all

FIA Statistics Rack: 0, Slot: 0, Asic instance: 0

Per Block Statistics:

Ingress:

NBI RX:
  RX_TOTAL_BYTE_COUNTER          = 161392268790033002
  RX_TOTAL_PKT_COUNTER           = 164628460653364

IRE:
  CPU_PACKET_COUNTER             = 0
  NIF_PACKET_COUNTER             = 164628460651867
  OAMP_PACKET_COUNTER            = 32771143
  OLP_PACKET_COUNTER             = 4787508
  RCY_PACKET_COUNTER             = 67452938
  IRE_FDT_INTRFACE_CNT           = 192

IDR:
  MMU_IDR_PACKET_COUNTER         = 697231761913
  IDR_OCB_PACKET_COUNTER         = 1

IQM:
  ENQUEUE_PKT_CNT                = 164640311902277
  DEQUEUE_PKT_CNT                = 164640311902198
  DELETED_PKT_CNT                = 0
  ENQ_DISCARDED_PACKET_COUNTER   = 90015441
```

# show controllers npu stats traps-all

To display all the trap events statistics within the NPU, use the **show controllers npu stats traps-all** command in the XR EXEC mode.

**show controller npu stats traps-all** { **detail instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **latest instance** *instance-id* **location** { *node-id* | *path* | *all* } | **nonzero instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **detail instance** *instance-id* | Displays detailed information about a given instance. |
| **detail instance** *all* | Displays detailed information about all instances. |
| **instance** *instance-id* | Displays NPU information about a given instance. |
| **instance** *all* | Displays NPU information about all instances. |
| **latest instance** *instance-id* | Displays the most recent hardware statistics about a given instance. |
| **nonzero instance** *instance-id* | Displays information about a given instance by excluding traps with both zero packets accepted and zero packets dropped. |
| **nonzero instance** *all* | Displays information about all instances by excluding traps with zero packets accepted and zero packets dropped. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |

| | |
|---|---|
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **\| file filename vrf vrfname**.<br>You can save the content in the following locations:<br>• *WORD* - Save the output to a specified filename.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default** None

**Command Modes** XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| interface | read |
| filesystem | read, write |
| cisco-support | read |

## Examples

The **show controllers npu stats traps-all** command displays packets that are locally processed and packets that are dropped by the CPU.

```
Router# show controllers npu stats traps-all instance all location 0/RP0/CPU0

Trap Type                                       NPU  Trap TrapStats   Policer Packet    Packet

                                                ID    ID      ID              Accepted  Dropped
=============================================================================================
RxTrapMimSaMove(CFM_DOWM_MEP_DMM)                0    6    0x6         32037   0         0

RxTrapMimSaUnknown(RCY_CFM_DOWN_MEP_DMM)         0    7    0x7         32037   0         0

RxTrapAuthSaLookupFail (IPMC default)            0    8    0x8         32033   0         0

RxTrapSaMulticast                                0    11   0xb         32018   0         0

RxTrapArpMyIp                                    0    13   0xd         32001   0         0

RxTrapArp                                        0    14   0xe         32001   11        0

RxTrapDhcpv4Server                               0    18   0x12        32022   0         0

RxTrapDhcpv4Client                               0    19   0x13        32022   0         0

RxTrapDhcpv6Server                               0    20   0x14        32022   0         0

RxTrapDhcpv6Client                               0    21   0x15        32022   0         0

RxTrapL2Cache_LACP                               0    23   0x17        32003   0         0

RxTrapL2Cache_LLDP1                              0    24   0x18        32004   0         0

RxTrapL2Cache_LLDP2                              0    25   0x19        32004   1205548   0

RxTrapL2Cache_LLDP3                              0    26   0x1a        32004   0         0
```

The above sample displays only a part of the actual output; the actual output displays more details.

# show controllers npu stats voq

To display statistics related to the Virtual Output Queues (VOQs) on the NPU, use the **show controllers npu stats voq** command in the XR EXEC mode.

**show controller npu stats voq** { **base** *voq-base number* { **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **src-slice** *slice-id* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } } | **ingress interface** { *voq-Interface-handle-number* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **CEM** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **EH** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Fi** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Fo** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **FH** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Gi** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Hu** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Mg** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **PTP** *R/S/I/P* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **Te** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **TF** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **TH** *R/S/I/P/B* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | *all* **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } } } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **base** *voq-base number* | Specifies the voq-base number. |
| **src-slice** *slice-id* **instance** | Specifies the slice id. |
| **ingress interface** <*voq-Interface handle number*> | Specifies voq-Interface handle number. |
| **ingress interface** *CEM* | Specifies circuit emulation interface. |
| **ingress interface** *EH* | Specifies 800 Gigabit ethernet interface type. |
| **ingress interface** *Fi* | Specifies 50 Gigabit ethernet interface type. |
| **ingress interface** *Fo* | Specifies 40 Gigabit ethernet interface type. |
| **ingress interface** *FH* | Specifies 400 Gigabit ethernet interface type. |
| **ingress interface** *Gi* | Specifies Gigabit ethernet interface type. |
| **ingress interface** *Hu* | Specifies 100 Gigabit ethernet interface type. |
| **ingress interface** *Mg* | Specifies ethernet interface type. |
| **ingress interface** *PTP* | Specifies ethernet interface type. |
| **ingress interface** *Te* | Specifies 10 Gigabit ethernet interface type. |

| | |
|---|---|
| **ingress interface** *TF* | Specifies 25 Gigabit ethernet interface type. |
| **ingress interface** *TH* | Specifies 200 Gigabit ethernet interface type. |
| **ingress interface** *all* | Specifies all interface type. |
| *R/S/I/P/B* | Specifies the Rack/Slot/Instance/Port/Breakout of the voq. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |

| Task ID | Operations |
|---|---|
| filesystem | read, write |
| cisco-support | read |

## Examples

The **show controllers npu stats voq** command displays packets that are processed on the NPU and dropped in the interface VoQs.

```
Router# show controllers npu stats voq ingress interface hundredGigE 0/0/0/16 instance all
 location 0/RP0/CPU0

Interface Name    =   Hu0/0/0/16
Interface Handle  =      f0001b0
Location          =   0/RP0/CPU0
Asic Instance     =            0
VOQ Base          =        10288
Port Speed(kbps)  =    100000000
Local Port        =        local
VOQ Mode          =            8
Shared Counter Mode =          2
       ReceivedPkts    ReceivedBytes   DroppedPkts     DroppedBytes
-------------------------------------------------------------------
TC_{0,1} = 114023724       39908275541     113945980       39881093000
TC_{2,3} = 194969733       68239406550     196612981       68814543350
TC_{4,5} = 139949276       69388697075     139811376       67907466750
TC_{6,7} = 194988538       68242491778     196612926       68814524100
```

# show fwd statistics

To display the forwarder driver statistics information, use the **show fwd statistics** command in the XR EXEC mode.

**show fwd statistics** { **all** { **detail location** { *node-id* | *path* } | **location** { *node-id* | *path* } | [ *output-modifiers* ] } | **egress** { **detail location** { *node-id* | *path* } | **location** { *node-id* | *path* } | [ *output-modifiers* ] } | **ingress** { **detail location** { *node-id* | *path* } | **location** { *node-id* | *path* } | [ *output-modifiers* ] } } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **all** | Displays all packet statistics. |
| **egress** | Displays egress packet statistics. |
| **ingress** | Displays ingress packet statistics. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| cisco-support | read |

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

## Examples

The **show fwd statistics** command displays the forwarder driver statistics information on a particular node or location.

```
Router# Show fwd statistics all location 0/RP1/CPU0
RECEIVE STATISTICS SUMMARY:
rx_pkts: 485060
punt_pkts: 416647
ingress_total_drops: 6117
TRANSMIT STATISTICS SUMMARY:
inject_pkts: 103632
tx_pkts: 101434
tx_null_ifh_pkts: 6006
mcast_all_lccpu_pkts: 1206
lpts_all_lccpu_pkts: 0
mgmt_loopback_pkts: 0
lpts_loopback_pkts: 5788
dlrsc_rp_loopback_pkts: 0
local_node_loopback_pkts: 2198
hw_ts_offset_exceeded: 0
egress_total_drops: 0
```

# show spp client

To display the client information within the Software Packet Path (SPP), use the **show spp client** command in the XR EXEC mode.

**show spp client** { **detail location** { *node-id* | *path* | *all* } | **location** { *node-id* | *path* | *all* } | **punt** { **queues location** { *node-id* | *path* | *all* } | **status location** { *node-id* | *path* | *all* } } | [ *output-modifiers* ] } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| **punt queues** | Specifies client punt queues. |
| **punt status** | Specifies client punt status. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 6.0.1 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| transport | read |

| Task ID | Operations |
|---|---|
| optical | read |

## Examples

The **show spp client** command displays the client information within the SPP on a particular node or location.

```
Router# show spp client detail location 0/0/CPU0
Fri Sep  6 11:58:45.157 UTC
Client connections allowed: 1
Ctx allocator: 65536 items 65531 free 0 shortages

SPP Queues
==========
    Main input queue at 0x0x3087516040
      Persistent: F, Mutex: T, Pulse: T, Blocking: T Invalid: F
      Head 1184, Tail 1184, Coalesced 0
      Cur 0, Max 2048, Enqueues 5280, High WM: 4 (14:02:40.278 Sep 05 24 UTC) Drops: 0
      elsize 8 coid 1 pid 4980 pulse_code 124 pulse_value 0 prio 10
Clients
=======
netio, JID 212 (pid 6184)
-----------------------------------------------------------
  Reconnect Pending: F, Exited: F, Keep Queues: F, Pakman Client: T
  Quota:
    Current: 0, Limit: 32768, Available: 0, Enqueued: 0, Drops 0
  Queues:
    Control Queue at 0x0x3087e62400
      Punt SF: nused 0, is not scheduled
      Persistent: F, Mutex: T, Pulse: T, Blocking: F Invalid: F
      Head 0, Tail 0, Coalesced 0
      Cur 0, Max 10, Enqueues 0, High WM: 0 (13:55:40.406 Sep 05 24 UTC) Drops: 0
      elsize 8 coid 0 pid 6184 pulse_code 0 pulse_value 0 prio 10
    Punt Queue key 0x03000041 at 0x0x3087e5d940
```

The above sample displays only a part of the actual output; the actual output displays more details.

# show spp node-counters

To display the node counters for the Software Packet Path (SPP), use the **show spp node-counters** command in the XR EXEC mode.

**show spp node-counters** { **location** { *node-id* | *path* | *all* } | [ *output-modifiers* ] } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default** None

**Command Modes** XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 25.4.1 | New counters are added. These counters will appear in the output when such condition occurs and the counters become non-zero.<br>• **Inject (Stage2)**—The packets are temporarily queued within the client/inject node of the SPP process when congestion occurs. These packets will be dequeued and transmitted once the congestion subsides.<br>• **mgmt tx pkt drops**—If a packet is dropped while being transmitted to the management interface.<br>• **ptp tx pkt drops**—If a packet is dropped while being transmitted to the PTP interface.<br>• **ce tx pkt drops**—If a packet is dropped while being transmitted to the NPU using control ethernet interface. |
| Release 6.0.1 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| transport | read |
| optical | read |

## Examples

The **show spp node-counters** command displays the node counters for the SPP on a particular node or location.

```
Router# show spp node-counters location 0/0/CPU0
fretta/classify
 forwarded NPU packet to NetIO:              21
                     PUNT ARP:               1
                   PUNT IFIB:               20
               IFIB RAWIP4_FM:              20
------------------------------
client/inject
        pkts injected into spp:              22
  NetIO->NPU injected into spp:              22
 NetIO->NPU & NetIO->MGMT pkts:              22
```

```
               Inject (Stage2):               1
          NetIO->NPU PROTO ARP:               2
         NetIO->NPU PROTO IPV4:              20
------------------------------
socket/rx
                ether raw pkts:              21
------------------------------
socket/tx
                      ce pkts:              22
------------------------------
pkt_classrx
            LPTS: ICMPv4 to XR:              20
              Total Pkts to XR:              21
             Total Pkts to Lnx:               1
               LPTS: ARP reply:               1
      Total Pkts to both dests:               1
------------------------------
client/punt
              punted to client:              21
------------------------------
```

The above sample displays only a part of the actual output; the actual output displays more details.

# show controllers fia diagshell

To debug asics, use the **show controllers fia diagshell** command in the XR EXEC mode.

**show controllers fia diagshell slot** *diagnostic command* **location** { *location node-id* | *all* }

## Syntax Description

| | |
|---|---|
| **slot** | Specifies the slot in the chassis where the FIA component is located. |
| *diagnostic command* | Enter specific commands available within the diagnostic shell to perform various checks and gather information. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| interface | read |
| cisco-support | read |

## Examples

The **show controllers fia diagshell** command to display port module information from NPU slot 0 for location 0/0/CPU0.

```
Router# show controllers fia diagshell 0 "PortMod info pm" location 0/0/CPU0
Node ID: 0/0/CPU0

R/S/I: 0/0/0
 PM id |    type     |    phys    | logic ports
-------------------------------------------------
   00  | Pm4x25      | 001 - 004  |001
   01  | Pm4x25      | 005 - 008  |005
   02  | Pm4x25      | 009 - 012  |009
   03  | Pm4x25      | 013 - 016  |013
   04  | Pm4x25      | 017 - 020  |017
   05  | Pm4x25      | 021 - 024  |021
   06  | Pm4x25      | 049 - 052  |no port attached
```

```
07  | Pm4x25      | 053 - 056  |no port attached
08  | Pm4x25      | 057 - 060  |no port attached
09  | Pm4x25      | 061 - 064  |061
10  | Pm4x25      | 065 - 068  |065
11  | Pm4x25      | 069 - 072  |069
12  | Pm4x10      | 025 - 028  |no port attached
13  | Pm4x10      | 029 - 032  |no port attached
14  | Pm4x10      | 033 - 036  |no port attached
15  | Pm4x10      | 037 - 040  |no port attached
16  | Pm4x10      | 041 - 044  |253
17  | Pm4x10Q     | 041 - 044  |no port attached
18  | Pm4x10      | 045 - 048  |no port attached
19  | Pm4x10Q     | 045 - 048  |no port attached
20  | Dnx_fabric  | 192 - 195  |256 - 259
21  | Dnx_fabric  | 196 - 199  |260 - 263
22  | Dnx_fabric  | 200 - 203  |264 - 267
```

The above sample displays only a part of the actual output; the actual output displays more details.

# show controllers fia statistics

To display the fabric ASIC's statistical information about drop counters, packet counters, and error counters for a specific fabric plane or for all planes, use the **show controllers fia statistics** command in the XR EXEC mode.

**show controller fia statistics** { **detail instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } | **instance** { *instance-id* **location** { *node-id* | *path* | *all* } | *all* **location** { *node-id* | *path* | *all* } } } [ *output-modifiers* { **begin** *line* | **exclude** *line* | **file** | **include** *line* | **utility** *line* } ]

## Syntax Description

| | |
|---|---|
| **detail instance** *instance-id* | Displays detailed information about a given instance. |
| **detail instance** *all* | Displays detailed information about all instances. |
| **instance** *instance-id* | Displays information about a given instance. |
| **instance** *all* | Displays information about all instances. |
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays the information about a specific node. |
| **location** *all* | Displays information about all nodes. |
| *output-modifiers* **begin** *line* | Displays information from the line that matches to the given content.<br>For example, if you want to display the running configuration starting from the interface configurations, you can enter as **\| begin interface**. |
| *output-modifiers* **exclude** *line* | Displays information by filtering out lines that contain the given content.<br>For example, if you want to view a configuration but skip all lines that mention "interface", you can enter as **\| exclude interface**. |
| *output-modifiers* **include** *line* | Displays information that includes the content that you have given.<br>For example, if you want to view lines that contain the word "interface" within a configuration, you can enter as **\| include interface**. |
| *output-modifiers* **utility** *line* | Specifies various Unix command-line tools to manipulate or analyze the command's output.<br>For example, if you want to sort the output of a command alphabetically, you can enter as **\| utility sort**. |

| | |
|---|---|
| *output-modifiers* **file** | Saves the information to a specific file.<br>For example, if you want to save information to a specific file, you can enter as **`\| file filename vrf vrfname`**.<br>You can save the content in the following locations:<br>• *filename* - Save the output to a specified filename in VRF.<br>• *append* - Add the output to the end of an existing file.<br>• *config* - Save the output to the device's configuration.<br>• *disk0* - Store the output on the device's disk0 storage.<br>• *ftp* - Transfer and save the output to an FTP server.<br>• *harddisk* - Save the output to the device's internal hard disk.<br>• *http* - Send the output to an HTTP server.<br>• *https* - Send the output to an HTTPS server.<br>• *rootfs* - Save the output to the root file system of the device.<br>• *scp* - Securely copy the output to a remote server using SCP.<br>• *sftp* - Securely transfer the output to a remote server using SFTP.<br>• *tftp* - Transfer the output to a TFTP server. |

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

| Release | Modification |
|---|---|
| Release 7.3.5 | This command was introduced. |

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

| Task ID | Operations |
|---|---|
| interface | read |

| Task ID | Operations |
|---|---|
| filesystem | read, write |
| cisco-support | read |

## Examples

The **show controllers fia statistics** command displays the statistical information about drop counters, packet counter and error counter for instance 0 and location 0/1/CPU0.

```
Router# show controllers fia statistics instance 0 location 0/1/CPU0

FIA Statistics Rack: 0, Slot: 1, Asic instance: 0

FIA Rx (To Fabric) Statistics.

 ------------------------------------------------{*}*--------------------

 Input Pkt counters                                    Pkts             Bytes

    Rx pkts from pse                 :        665777182      288589641737

    Rx pkts from switch              :          5562700        2452202671

        bcast pkts from switch       :                0

        mcast pkts from switch       :          5444333

        ucast pkts from switch       :           118367

    Rx pkts enqueued(IQM)            :        665895523      293281221178

    Rx pkts dequeued(IQM)            :        665895523      293281221178

    Rx pkts sent to fabric           :        665895523


Cell counters:

    Data cells sent to fabric        :       1544969295      293281221178

    Control cells sent to fabric     :     420450857496

 Drop counters:

     Rx burst error drops(NBI)        :               0

     Rx error drops(Switch)           :               0

     Rx error drops(pse)              :               0

    Rx pkt discard drops(IQM)        :          5443758        2337309048

     Pkt crc error drops(FDT)         :               0

     Unreachable dest cell drops      :               0

    Internal Error Count             :              0

    Internal Drop Count              :              0
```

The above sample displays only a part of the actual output; the actual output displays more details.

# show netio drops

To display Network Input and Output (Netio) packet drops information, use the **show netio drops** command in XR EXEC mode.

**show netio drops location** *node-id*

## Syntax Description

| | |
|---|---|
| **location** *node-id* | Specifies the node. The *node-id* argument is entered in the *rack/slot/module* notation. Displays Netio drop counters for the designated node. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 6.0 | This command was introduced. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| netio | show output |

## Examples

The **show netio drops** command displays the netio drops for location 0/RSP0/CPU0.

```
Router# show netio drops loc 0/rsp0/cpu0
Drops for interfaces on node 0/RSP0/CPU0
------------------------------------------------------------------------------
Interface: FINT0/RSP0/CPU0 (0x080000c0)
------------------------------------------------------------------------------
Interface input drops:         1008181180 pkts
Interface input errors:        47494 pkts
Interface input unknown proto: 0 pkts
Interface output drops:        255 pkts
Interface output errors:       0 pkts
```

The above sample displays only a part of the actual output; the actual output displays more details.



# Audit Monitoring Commands

This module describes the audit monitoring commands available on the router. These commands are used to proactively monitor the security and compliance of the router by enabling audit monitoring.

For detailed information about system health check concepts, configuration tasks, and examples, see the *Implementing Audit Monitoring* chapter in the *System Monitoring Configuration Guide for Cisco NCS 5500 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 540 Series RoutersSystem Monitoring Configuration Guide for Cisco NCS 560 Series Routers*.


- linux security audit, on page 462
- show linux security audit, on page 467

# linux security audit

To enable the Linux audit monitoring and logging capabilities, use the **linux security audit** command in XR Config mode.

**linux security audit** { **monitor** { **all** | **authlog-files** | **cron-files** | **dns-client-files** | **docker** | **file-deletion** | **file-perm-changes** | **kernel-module-mgmt** | **process-audits** | **system-login-reboot** | **system-software** | **system-time-change** | **user-group-config-files** | **user-privilege-mgmt** | **xr-software** | **logging** | **syslog** | **keepalive interval** *interval* } }

## Syntax Description

| | |
|---|---|
| **monitor** | Enable audit monitoring. |
| **all** | Enable audit monitoring for all rule groups. |
| **authlog-files** | Enable audit monitoring for changes in authlog files. |
| **cron-files** | Enable audit monitoring for changes in cron files. |
| **dns-client-files** | Enable audit monitoring for changes in DNS client files. |
| **docker** | Enable audit monitoring for changes in docker. |
| **file-deletion** | Enable audit monitoring for file deletion. |
| **file-perm-changes** | Enable audit monitoring for changes in file permissions. |
| **kernel-module-mgmt** | Enable audit monitoring for kernel module management. |
| **process-audits** | Enable audit monitoring for process audits. |
| **system-login-reboot** | Enable audit monitoring for system login and reboot. |
| **system-software** | Enable audit monitoring for changes in system software. |
| **system-time-change** | Enable audit monitoring for changes in system time. |
| **user-group-config-files** | Enable audit monitoring for changes in user group configuration files. |
| **user-privilege-mgmt** | Enable audit monitoring for changes in user privileges. |
| **xr-software** | Enable audit monitoring for changes in IOS XR software. |
| **logging syslog** | Enable forwarding of audit logs to a remote syslog server. |
| **keepalive interval** *interval* | Enables AuditD process keepalive and sets the keepalive interval in minutes. |

## Command Default

Audit monitoring is disabled.

## Command Modes

XR Config mode

## Command History

| Release | Modification |
|---|---|
| Release 26.3.1 | Two new options, **keepalive** and **interval**, were added to the command. |
| Release 25.3.1 | This command was introduced. |

## Usage Guidelines

The router stores audit logs locally at **/var/log/audit/audit.log**, unless you enable log forwarding.

The table lists the rules within each of the rule-groups.

| Rule-group | Rules |
|---|---|
| xr-software | -a always,exit -F arch=b64 -F dir=/pkg/bin -F perm=wa -k xr_bin_changes<br>-a always,exit -F arch=b64 -F dir=/pkg/sbin -F perm=wa -k xr_sbin_changes<br>-a always,exit -F arch=b64 -F dir=/pkg/lib -F perm=wa -k xr_lib_changes |
| user-group-config-files | -a always,exit -F arch=b64 -F path=/etc/passwd -F perm=wa -k passwd_changes<br>-a always,exit -F arch=b64 -F path=/etc/shadow -F perm=wa -k shadow_changes<br>-a always,exit -F arch=b64 -F path=/etc/group -F perm=wa -k group_changes<br>-a always,exit -F arch=b64 -F path=/etc/sudoers -F perm=wa -k sudoers_changes |
| dns-client-files | -a always,exit -F arch=b64 -F path=/etc/hosts -F perm=wa -k hosts_changes<br>-a always,exit -F arch=b64 -F path=/etc/resolv.conf -F perm=wa -k dns_changes<br>-a always,exit -F arch=b64 -F path=/var/run/resolv.conf -F perm=wa -k dns_changes |
| authlog-files | -a always,exit -F arch=b64 -F path=/var/log/auth.log -F perm=wa -k authlog_changes |
| system-time-change | -a always,exit -F arch=b64 -F path=/etc/localtime -F perm=wa -k time_changes |
| system-login-reboot | -a always,exit -F arch=b64 -F path=/var/log/wtmp -F perm=wa -k shutdown_reboot |

| Rule-group | Rules |
|---|---|
| cron-files | -a always,exit -F arch=b64 -F path=/etc/crontab -F perm=wa -k cron_changes<br>-a always,exit -F arch=b64 -F dir=/etc/cron.d -F perm=wa -k cron_changes<br>-a always,exit -F arch=b64 -F dir=/etc/cron.daily -F perm=wa -k cron_changes<br>-a always,exit -F arch=b64 -F dir=/etc/cron.hourly -F perm=wa -k cron_changes<br>-a always,exit -F arch=b64 -F dir=/etc/cron.weekly -F perm=wa -k cron_changes<br>-a always,exit -F arch=b64 -F dir=/etc/cron.monthly -F perm=wa -k cron_changes |
| kernel-module-mgmt | -a always,exit -F arch=b64 -F path=/sbin/insmod -F perm=x -k modules<br>-a always,exit -F arch=b64 -F path=/sbin/rmmod -F perm=x -k modules<br>-a always,exit -F arch=b64 -F path=/sbin/modprobe -F perm=x -k modules<br>-a always,exit -F arch=b64 -F path=/usr/bin/kmod -F perm=x -k modules |
| system-software | -a always,exit -F arch=b64 -F dir=/bin -F perm=wa -k bin_changes<br>-a always,exit -F arch=b64 -F dir=/sbin -F perm=wa -k sbin_changes<br>-a always,exit -F arch=b64 -F dir=/usr/bin -F perm=wa -k usr_bin_changes<br>-a always,exit -F arch=b64 -F dir=/usr/sbin -F perm=wa -k usr_sbin_changes |
| docker | -a always,exit -F arch=b64 -F path=/lib/systemd/system/docker.service -F perm=wa -k docker_service<br>-a always,exit -F arch=b64 -F path=/lib/systemd/system/docker.socket -F perm=wa -k docker_socket<br>-a always,exit -F arch=b64 -F path=/usr/bin/dockerd -F perm=xa -k docker_daemon<br>-a always,exit -F arch=b64 -F path=/etc/docker/daemon.json -F perm=wa -k docker_config<br>-a always,exit -F arch=b64 -F dir=/var/lib/docker -F perm=wa -k docker_storage<br>-a always,exit -F arch=b64 -S execve -F path=/usr/bin/docker -k docker_commands |
| process-audits | -a always,exit -F arch=b64 -S execve -F auid>=1000 -F auid!=-1 -k process_audit |

| Rule-group | Rules |
|---|---|
| file-perm-changes | -a always,exit -F arch=b64 -S fchmodat -k file_perm_changes |
| user-privilege-mgmt | -a always,exit -F arch=b64 -S setuid,setresuid,setreuid,setfsuid,setgid,setresgid,setregid,setfsgid -k user_group_management |
| file-deletion | -a always,exit -F arch=b64 -S unlink,unlinkat -k file_deletion |

This table provides the description of the various components of the rules:

| Component | Description |
|---|---|
| -a | Action, e.g., `always,exit` means always log on exit of syscall |
| -F | Field match, e.g., `arch=b64` (architecture), `dir=`, `path=`, `perm=`, etc. |
| arch=b64 | Architecture: 64-bit |
| dir= | Directory to monitor (e.g., `/pkg/bin`, `/etc/cron.d`) |
| path= | File to monitor (e.g., `/etc/passwd`, `/usr/bin/docker`) |
| perm= | Permissions watched: `r` (read), `w` (write), `x`(execute), `a` (attribute change) |
| -k | Key: Custom tag for easier filtering/searching in audit logs (e.g., `xr_bin_changes`, `cron_changes`) |
| -S | Syscall(s) to monitor (e.g., `execve`, `fchmodat`, `unlink`) |
| auid | Audit user ID; `auid>=1000` means all regular (non-system) users |
| always,exit | Log every time the rule is matched on syscall exit |

## Task ID

| Task ID | Operation |
|---|---|
| network | read, write |
| interface | read, write |
| system | read, write |

### Example

This example shows how you can enable audit monitoring with the **linux security audit monitor** command.

```
Router# conf t
Router(config)# linux security audit monitor xr-software
Router(config)# linux security audit monitor user-group-config-files
Router(config)# commit
```

This example shows how you can enable audit log forwarding with the **linux security audit logging syslog** command.

```
Router# conf t
Router(config)# linux security audit logging syslog
Router(config)# logging 10.0.1.2 vrf default port 514
Router(config)# commit
```

This example shows how you can configure the AuditD process keepalive command.

```
Router# conf t
Router(config)# linux security audit keepalive interval 1010
Router(config)# linux security audit logging syslog
Router(config)# logging 10.0.1.2 vrf default port 514
Router(config)# commit
```

# show linux security audit

To view the details of the Linux security audit information, use the **show linux security audit** command in XR EXEC mode.

**show linux security audit** { **monitor status** { *rule-group* | **detail** *rule-group* } | **logging syslog** }

## Syntax Description

| | |
|---|---|
| **monitor** | Displays the audit monitor information. |
| **status** | Displays the current active audit rules. |
| *rule-group* | Displays the status of the specified rule group.<br>This field takes these values: **all, authlog-files, cron-files, dns-client-files, docker, file-deletion, file-perm-changes, kernel-module-mgmt, process-audits, system-login-reboot, system-software, system-time-change, user-group-config-files, user-privilege-mgmt, xr-software** |
| **detail** | Displays the detailed status of the specified rule group. |
| **logging** | Displays the audit logging information. |
| **syslog** | Displays the remote syslog server information. |

## Command Default

None

## Command Modes

XR EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 25.3.1 | This command was introduced. |

## Usage Guidelines

This table specifies the command usage:

| Command | Description |
|---|---|
| `show linux security audit monitor status` | Shows all currently enabled rules. |
| `show linux security audit monitor status detail` | Shows all currently enabled rules with per-location status. |
| `show linux security audit monitor status` | Shows status and rules for any key (enabled or disabled). |
| `show linux security audit monitor status detail` | Shows per-location status for any key (enabled or disabled). |
| `show linux security audit logging syslog` | Shows syslog forwarding status and configured servers. |

## Task ID

| Task ID | Operation |
|---|---|
| system | read |

### Example

The example displays the status of the audit rule-groups.

```
Router# show linux security audit monitor status
key name: xr-software                status: enabled
rules:
-a always,exit -F arch=b64 -F dir=/pkg/bin -F perm=wa -k xr_bin_changes
-a always,exit -F arch=b64 -F dir=/pkg/sbin -F perm=wa -k xr_sbin_changes
-a always,exit -F arch=b64 -F dir=/pkg/lib -F perm=wa -k xr_lib_changes
------------------------------------------------------------
key name: user-group-config-files    status: enabled
rules:
-a always,exit -F arch=b64 -F path=/etc/passwd -F perm=wa -k passwd_changes
-a always,exit -F arch=b64 -F path=/etc/shadow -F perm=wa -k shadow_changes
-a always,exit -F arch=b64 -F path=/etc/group -F perm=wa -k group_changes
-a always,exit -F arch=b64 -F path=/etc/sudoers -F perm=wa -k sudoers_changes
------------------------------------------------------------
```

This example displays the audit log forwarding details.

```
Router# show linux security audit logging syslog
status: enabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: default port: 514
ipaddr: 2001:db8::1 vrf: default port: 514
```



# INDEX


## A

access-list command 213
action (IP SLA) command 215
ageout command 217

## B

buckets (history) command 218
buckets (statistics hourly) command 220
buckets (statistics interval) command 221

## C

control disable command 222

## D

datasize request command 224
destination address (IP SLA) command 226
destination port command 227
distribution count command 228
distribution interval command 230

## E

exp command 232

## F

filter command 234
force explicit-null command 236
frequency (IP SLA) command 238

## H

history command 240
hw-timestamp disable command 242

## I

interval command 243

## K

key-chain command 245

## L

life command 246
lives command 247
low-memory command 250
lsp selector ipv4 command 251
lsr-path command 253

## M

maximum hops command 254
maximum paths (IP SLA) command 256
monitor command 258
monitor interface command 139
mpls discovery vpn command 259
mpls lsp-monitor command 260

## O

operation command 261
output interface command 262
output nexthop command 264

## P

packet count command 266
packet interval command 267
path discover command 268
path discover echo command 269
path discover path command 271
path discover scan command 273
path discover session command 275

## R

react command 277
react lpd command 281
reaction monitor command 283
reaction operation command 285
reaction trigger command 286

recurring command 287
reply dscp command 288
reply mode command 290

## S

samples command 295
scan delete-factor command 297
scan interval command 299
schedule monitor command 301
schedule operation command 302
schedule period command 304
show alarms 36
show event manager environment command 80
show ipsla application command 307
show ipsla history command 309
show ipsla mpls discovery vpn command 311
show ipsla mpls lsp-monitor lpd command 313
show ipsla mpls lsp-monitor scan-queue command 315
show ipsla mpls lsp-monitor summary command 317
show ipsla responder statistics ports command 320
show ipsla statistics aggregated command 325
show ipsla statistics command 322
show ipsla statistics enhanced aggregated command 334
source address command 341
source port command 343
start-time command 344
statistics command 346

## T

tag (IP SLA) command 348
target ipv4 command 350
target pseudowire command 352
target traffic-eng command 354
threshold command 356
threshold type average command 358
threshold type consecutive command 360
threshold type immediate command 362
threshold type xofy command 364
timeout command 366
tos command 368
ttl command 370
type icmp echo command 372
type icmp path-echo command 373
type icmp path-jitter command 374
type mpls lsp ping command 375
type mpls lsp trace command 377
type udp echo command 379
type udp ipv4 address command 381
type udp jitter command 380

## V

verify-data command 382
vrf (IP SLA MPLS LSP monitor) command 385
vrf (IP SLA) command 383