System Monitoring Command Reference for Cisco 8000 Series Routers

First Published: 2020-03-01

Last Modified: 2024-03-31

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

CONTENTS

Preface

This preface contains these sections:

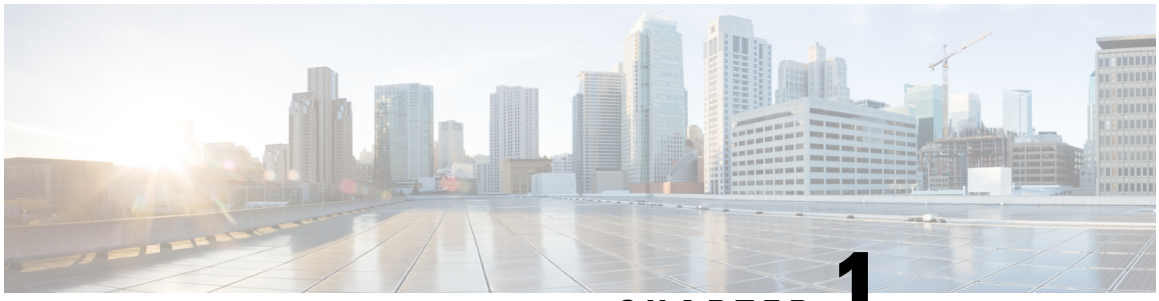
Changes to This Document

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

Table 1: Changes to This Document

Date	Summary
June 2024	Republished for Release 24.2.1.
January 2024	Republished for Release 7.3.6.
August 2023	Republished for Release 7.3.5.
May 2021	Republished for Release 7.3.15.
February 2021	Republished for Release 7.3.1.
August 2020	Republished for Release 7.0.14.
March 2020	Initial release of this document.

Obtaining Documentation and Submitting a Service Request



CHAPTER 1

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.

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 8000 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 8000 Series Routers*.

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 7.0.12	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 7.0.12	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 7.0.12	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 7.0.12	This command was introduced.

Usage Guidelines Use the show logging correlator buffer, on page 35 command to confirm that records have been cleared.

Use the logging correlator buffer-size, on page 13 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: • **alerts** • **critical** • **emergencies** • **errors** • **informational** • **notifications** • **warnings** **Note** 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.
	
	Ranges for the *hh* **:** *mm* **:** *ss month day year* arguments are as follows:
	
	• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
	• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
	• *ss*—Seconds. Range is 00 to 59.
	• *month*—(Optional) The month of the year. The values for the *month* argument are:
	  • january
	  • february
	  • march
	  • april
	  • may
	  • june
	  • july
	  • august
	  • september
	  • october
	  • november
	  • december
	• *day*—(Optional) Day of the month. Range is 01 to 31.
	  • *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

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 7.0.12	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 40 command to verify that events have been cleared from the logging events buffer.

Use the logging events buffer-size, on page 16 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 7.0.12	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 40 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 7.0.12	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 37 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 7.0.12	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 37 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)#
```

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 38 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 7.0.12	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 36 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 40 **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 35 to display messages stored in the logging correlator buffer.

Use the logging correlator buffer-size, on page 13 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 7.0.12	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 11 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 7.0.12	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 43 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 7.0.12	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
HundredGigE0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : Interface
HundredGigE0/2/0/0, 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 HundredGigE0/2/0/0, 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
HundredGigE0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : interface
```

```
HundredGigE0/2/0/0: Interface HundredGigE0/2/0/0, changed state to Down
LC/0/2/CPU0:Aug 12 01:20:59.451 : ifmgr[159]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
HundredGigE0/2/0/0: Line protocol on Interface HundredGigE0/2/0/0, 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). See the "Usage Guidelines" for 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 7.0.12	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 7.0.12	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 43 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 7.0.12	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 7.0.12	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 7.0.12	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 43 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 7.0.12	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 7.0.12	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 7.0.12	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 43 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 31 to view the router alarms in brief.

Use the show alarms detail, on page 32 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 31	Displays router alarms in brief.
show alarms detail, on page 32	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 27	Displays router alarms in brief and detail.
show alarms detail, on page 32	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 27	Displays router alarms in brief and detail.
show alarms brief, on page 31	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 7.0.12	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 7.0.12	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 13 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 7.0.12	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 7.0.12	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: • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notifications** • **informational** **Note** 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.
	
	Ranges for the *hh* **:** *mm* **:** *ss month day year* arguments are as follows:
	• *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
	• *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
	• *ss*—Seconds. Range is 00 to 59.
	• *month*—(Optional) The month of the year. The values for the *month* argument are:
	  • january
	  • february
	  • march
	  • april
	  • may
	  • june
	  • july
	  • august
	  • september
	  • october
	  • november
	  • december
	• *day*—(Optional) Day of the month. Range is 01 to 31.
	• *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

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 7.0.12	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 7.0.12	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 16 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 20 command.
Filter	The lowest severity level for events that will be displayed. This field is controlled by the logging events level, on page 19 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 7.0.12	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
```

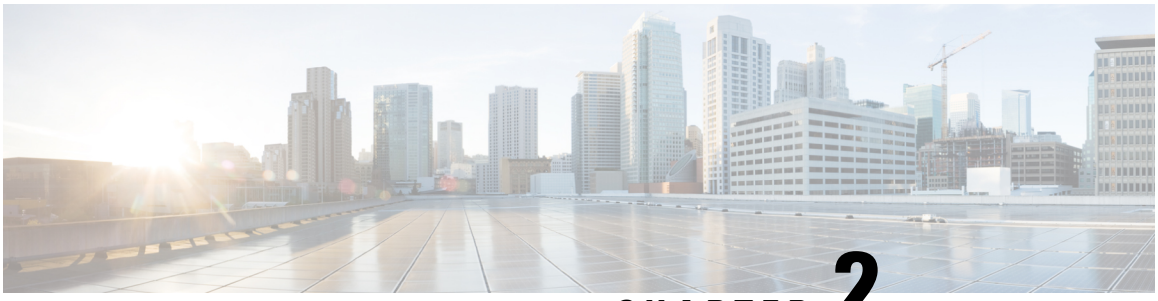
This example displays information about all logging suppression rules applied to a specific source location on the router:

```
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
```



CHAPTER 2

Embedded Event Manager Commands

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

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

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

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 8000 Series Routers*.

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 7.0.12	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 7.0.12	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 49 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. 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 [*system* | **user**]	(Optional) Specifies the type of policy to register. Use the *system* keyword to register a system policy defined by Cisco and the *user* keyword to register 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 7.0.12	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 8000 Series Routers* 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 52 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 7.0.12	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 7.0.12	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.

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. However the policies of **none** type have to be run manually using **event manager run** command. A **none** type event is a dummy event. An EEM script can register for **none** type event using **event_register_none** tcl command in the script.

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 53 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 7.0.12	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 7.0.12	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 7.0.12	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 7.0.12	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:

- **application**—Application event type
- **cli**—CLI event type
- **config**—Conf event type
- **counter**—Counter event type
- **hardware**—Hardware event type
- **none**—None event type
- **oir**—Online insertion and removal (OIR) event type
- **process-abort**—Event type for abnormal termination of process
- **process-start**—Process start event type
- **process-term**—Process termination event type
- **process-user-restart**—Process user restart event type
- **process-user-shutdown**—Process user shutdown event type
- **snmp**—SNMP event type
- **snmp-proxy**—SNMP PROXY event type
- **statistics**—Statistics event type
- **syslog**—Syslog event type
- **timer-absolute**—Absolute timer event type
- **timer-countdown**—Countdown timer event type
- **timer-cron**—Clock daemon (cron) timer event type
- **timer-watchdog**—Watchdog timer event type
- **track**—Track event type
- **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 7.0.12	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.
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 7.0.12	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
```

show event manager statistics-table

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

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

Syntax Description

stats-name	Specific statistics type to be displayed. There are three statistics types: • generic (ifstats-generic) • interface table (ifstats-iftable) • data rate (ifstats-datarate)
all	Displays the possible values for the *stats-name* argument. Displays the output for all the statistics types.

Command Default

None

Command Modes

XR EXEC mode

Usage Guidelines

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager statistics-table all

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

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

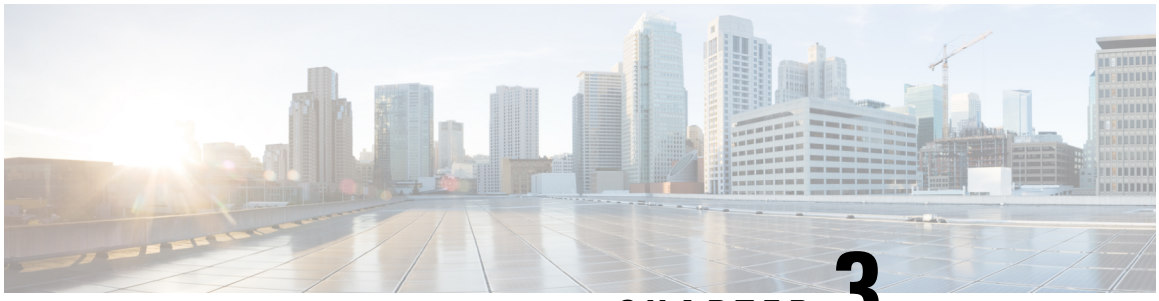
```
RP/0/RP0/CPU0:router# show event manager statistics-table ifstats-iftable

Name                    Type      Description
PacketsReceived         uint64    Packets rcvd
```

```
BytesReceived            uint64    Bytes rcvd
PacketsSent              uint64    Packets sent
BytesSent                uint64    Bytes sent
MulticastPacketsReceived uint64    Multicast pkts rcvd
BroadcastPacketsReceived uint64    Broadcast pkts rcvd
MulticastPacketsSent     uint64    Multicast pkts sent
BroadcastPacketsSent     uint64    Broadcast pkts sent
OutputDropsCount         uint32    Total output drops
InputDropsCount          uint32    Total input drops
InputQueueDrops          uint32    Input queue drops
RuntPacketsReceived      uint32    Received runt packets
GiantPacketsReceived     uint32    Received giant packets
ThrottledPacketsReceived uint32    Received throttled packets
ParityPacketsReceived    uint32    Received parity packets
UnknownProtocolPacketsReceiveduint32    Unknown protocol pkts rcvd
InputErrorsCount         uint32    Total input errors
CRCErrorCount            uint32    Input crc errors
InputOverruns            uint32    Input overruns
FramingErrorsReceived    uint32    Framing-errors rcvd
InputIgnoredPackets      uint32    Input ignored packets
InputAborts              uint32    Input aborts
OutputErrorsCount        uint32    Total output errors
OutputUnderruns          uint32    Output underruns
OutputBufferFailures     uint32    Output buffer failures
OutputBuffersSwappedOut  uint32    Output buffers swapped out
Applique                 uint32    Applique
ResetCount               uint32    Number of board resets
CarrierTransitions       uint32    Carrier transitions
AvailabilityFlag         uint32    Availability bit mask
NumberOfSecondsSinceLastClearCountersuint32    Seconds since last clear counters
LastClearTime            uint32    SysUpTime when counters were last cleared (in seconds)
```

This table describes the significant fields displayed in the example.

Table 10: show event manager statistics-table Field Descriptions

Field	Description
Name	Name of the statistic. When the **all** keyword is specified, there are three types of statistics displayed: • ifstats-generic • ifstats-iftable • ifstats-datarate When a statistics type is specified, the statistics for the statistic type are displayed.
Type	Type of statistic.
Description	Description of the statistic.



CHAPTER 3

Logging Services Commands

This module describes the Cisco IOS XR7 Software commands to configure system logging (syslog) for system monitoring on the router.

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

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** *type* | **format** **rfc5424** | **history** | **hostnameprefix** | **localfilesize** | **monitor** | **operator** | **port** | **severity** | **source-address** | **source-interface** *ipv4 address* | **suppress** | **trap** }

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 *type*	Modifies message logging facilities.
format	Configures the syslog message format to send to the server.
rfc5424	Sets the syslog message format according to RFC 5424.
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
operator	Sets severity operator of messages for anparticular remote host/vrf.
port	Sets UDP port for this remote host/vrf.
severity	Sets severity of messages for particular remote host/vrf

source-address *ipv4 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.

Command Default

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

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.2.1	The **facility** and **source-address** options per remote syslog server were introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging** command to identify a syslog server host to receive messages. By issuing this command more than once, you build a list of syslog servers that receive messages.

When syslog messages are sent to a syslog server, the Cisco IOS XR software includes a numerical message identifier in syslog messages. The message identifier is cumulative and sequential. The numerical identifier included in syslog messages sent to syslog servers provides a means to determine if any messages have been lost.

Use the logging trap, on page 89 command to limit the messages sent to snmp server.

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

Task ID

Task ID	Operations
logging	read, write

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

```
Router(config)#logging host1
```

```
Router(config)#logging A.B.C.D
facility        Modify message logging facilities
operator        Set severity operator of  messages for particular remote host/vrf
port            Set UDP port for this remote host/vrf
severity        Set severity of  messages for particular remote host/vrf
source-address  Specify source address of the logging host
vrf             Set VRF option
```

```
Router(config)#logging A.B.C.D
Router(config)#commit
Wed Nov 14 03:47:58.976 PST
```

```
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 7.0.12	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 11: 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

Command	Range	Description	Recommended Setting
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* }

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

Command Default

None

Command Modes

XR Config mode

XR Config Mode

Command History

Release	Modification
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
```

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 7.0.12	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 12: Severity Levels for Messages

Level Keywords	Level	Description	Syslog Definition
emergencies	0	Unusable system	LOG_EMERG
alerts	1	Need for immediate action	LOG_ALERT
critical	2	Critical condition	LOG_CRIT
errors	3	Error condition	LOG_ERR
warnings	4	Warning condition	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational message only	LOG_INFO

Level Keywords	Level	Description	Syslog Definition
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 console disable
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 7.0.12	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

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 7.3.15	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 container named DOCKER:

```
Router# configure
Router(config)# logging container all
Router(config)# commit

Router# 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:Mar  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:Mar  5 06:58:13.053 UTC: config[66985]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Mar  5 06:59:04.775 UTC: ubuntu-1[67232]: %OS-SYSLOG-6-DOCKER_APP :
^[]0;root@c382b2e7bed6: /^Groot@c382b2e7bed6:/# testlog
RP/0/RP0/CPU0:Mar  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:Mar  5 06:59:45.028 UTC: config[67139]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Mar  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:Mar  5 06:59:56.073 UTC: ubuntu-1[67976]: %OS-SYSLOG-6-DOCKER_APP : testlog-123

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

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

RP/0/RP0/CPU0:Mar  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 7.0.12	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.

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 events link-status (interface)

To enable the logging of link-status system logging (syslog) messages on a specific interface for virtual interfaces and subinterfaces, use the **logging events link-status** command in the appropriate interface or subinterface mode. To disable the logging of link status messages, use the **no** form of this command.

logging events link-status
no logging events link-status

Syntax Description

This command has no keywords or arguments.

Command Default

The logging of link-status messages is disabled for virtual interfaces and subinterfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages. The **logging events link-status** command enables messages for virtual interfaces and subinterfaces only.

The **logging events link-status** command allows you to enable and disable logging on a specific interface for bundles, tunnels, and VLANs.

Use the **no logging events link-status** command to disable the logging of link-status messages.

Note Enabling the **logging events link-status** command on a specific interface overrides the global configuration set using the **logging events link-status** command described in this section.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows the results of turning on logging for a bundle interface:

```
RP/0/RP0/CPU0:router(config)# int bundle-ether1
RP/0/RP0/CPU0:router(config-if)# logging events link-status
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit

LC/0/4/CPU0:Jun 29 12:51:26.887 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0, changed state to Up

LC/0/4/CPU0:Jun 29 12:51:26.897 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0, changed state
 to Up

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

LC/0/4/CPU0:Jun 29 12:51:32.375 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0, changed state to Down

LC/0/4/CPU0:Jun 29 12:51:32.376 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0, changed state
 to Down
```

This example shows a sequence of commands for a tunnel interface with and without logging turned on:

```
RP/0/RP0/CPU0:router(config)# int tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# logging events link-status
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:Jun 29 14:05:57.732 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Administratively Down

RP/0/RP0/CPU0:Jun 29 14:05:57.733 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Administratively Down

RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:Jun 29 14:06:02.104 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Down

RP/0/RP0/CPU0:Jun 29 14:06:02.109 : ifmgr[176]:
```

```
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Down
```

This example shows the same process for a subinterface:

```
RP/0/RP0/CPU0:router(config)# int HundredGigE 0/0/0/0.1
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# no shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# logging events link-status
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:46.710 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0.1, changed
state to Administratively Down

LC/0/5/CPU0:Jun 29 14:06:46.726 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0.1, changed state to Administratively
 Down

RP/0/RP0/CPU0:router(config-subif)# no shutdown
RP/0/RP0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:52.229 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0.1, changed state to Up


LC/0/5/CPU0:Jun 29 14:06:52.244 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0.1, changed
state to Down
```

logging facility

To configure the type of syslog facility in which system logging (syslog) messages are sent to syslog servers, use the **logging facility** command in 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 7.0.12	This command was introduced.

Usage Guidelines

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

Table 13: 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
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

Facility Type	Description
uucp	UNIX-to-UNIX copy system

Use the logging, on page 64command 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 logging destination, use the **logging file** command in XR Config mode. To remove the file logging destination, use the **no** form of this command.

logging file *filename* [**discriminator** {**match** | **nomatch**}] [**path** *pathname* {**maxfilesize** | **severity**}]
no logging file

Syntax Description

filename	Specifies the filename of the file to display.
discriminator	Specifies the match or nomatch syslog discriminator.
path *pathname*	Specifies the location to save the logging file.
maxfilesize	(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	(optional) Specifies the severity level for the logging file. Default is informational. • alerts Immediate action needed (severity=1) • critical Critical conditions (severity=2) • debugging Debugging messages (severity=7) • emergencies System is unusable (severity=0) • errors Error conditions (severity=3) • informational Informational messages (severity=6) • notifications Normal but significant conditions (severity=5) • warnings Warning conditions (severity=4)

Command Default None

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines Use the **logging file** command to set the logging file destination. To set the logging file discriminator you have to specify the file name. If it exceeds the maximum file size, then a wrap occurs.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to set the maximum file size for the defined file destination:

```
RP/0/RP0/CPU0:router(config)# logging file file1 path /harddisk:/logfiles/ maxfilesize 2048
```

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 format rfc5424

To configure the format of the system logging (syslog) messages according to the one outlined in RFC 5424, use the **logging format rfc5424** command in XR Config mode. To return console logging to the default setting, use the **no** form of this command.

logging format rfc5424

Syntax Description

format	Specifies the format of the syslog messages sent to the server.
rfc5424	Configures the format of the syslog messages according to the one outlined in RFC 5424.

Command Default

By default, this feature is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	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 format specified in RFC 5424:

```
Router(config)#logging 209.165.200.225 vrf default severity info
Router(config)#logging format rfc5424
Router(config)#commit

Router(config)#do show run logging
logging format rfc5424
logging 209.165.200.225 vrf default severity info
```

logging history

To change the severity level of system logging (syslog) messages sent to the history table on the router and a Simple Network Management Protocol (SNMP) network management station (NMS), use the **logging history** command in XR Config mode. To remove the **logging history** command from the configuration and return the logging of messages to the default level, use the **no** form of this command.

logging history *severity*
no logging history

Syntax Description

severity	Severity level of messages sent to the history table on the router and an SNMP NMS, including events of a higher severity level (numerically lower). Settings for the severity levels and their respective system conditions are listed under the Usage Guidelines section for the **logging console** command.

Command Default

severity: **warnings**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Logging of messages to an SNMP NMS is enabled by the **snmp-server enable traps** command. Because SNMP traps are inherently unreliable and much too important to lose, at least one syslog message, the most recent message, is stored in a history table on the router.

Use the **logging history** command to reflect the history of last 500 syslog messages. For example, when this command is issued, the last 500 syslog messages with severity less than warning message are displayed in the output of **show logging history** command.

Use the show logging history command to display the history table, which contains table size, message status, and message text data.

Use the logging history size command to change the number of messages stored in the history table.

The value specified for the *severity* argument causes messages at that severity level and at numerically lower levels to be stored in the history table of the router and sent to the SNMP NMS. Severity levels are numbered 0 to 7, with 1 being the most important message and 7 being the least important message (that is, the lower the number, the more critical the message). For example, specifying the level critical with the **critical** keyword causes messages at the severity level of **critical** (2), **alerts** (1), and **emergencies** (0) to be stored in the history table and sent to the SNMP NMS.

The **no logging history** command resets the history level to the default.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to change the level of messages sent to the history table and to the SNMP server to **alerts** (1), which means that messages at the severity level of **alerts** (1) and **emergencies** (0) are sent:

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

logging history size

To change the number of system logging (syslog) messages that can be stored in the history table, use the **logging history size** command in XR Config mode. To remove the **logging history size** command from the configuration and return the number of messages to the default value, use the **no** form of this command.

logging history size *number*
no logging history *number*

Syntax Description

number	Number from 1 to 500 indicating the maximum number of messages that can be stored in the history table. The default is 1 message.

Command Default

number: 1 message

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging history size** command to change the number of messages that can be stored in this history table. When the history table is full (that is, when it contains the maximum number of messages specified with the command), the oldest message is deleted from the table to allow the new message to be stored.

Use the logging history command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the number of messages stored in the history table to 20:

```
RP/0/RP0/CPU0:router(config)# logging history size 20
```

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 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging hostnameprefix** command to append a hostname prefix to messages sent to syslog servers from the router. You can use these prefixes to sort the messages being sent to a given syslog server from different networking devices.

Use the **logging** 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 ipv4/ipv6

To configure the differentiated services code point (DSCP) or the precedence value for the IPv4 or IPv6 header of the syslog packet in the egress direction, use the **logging** {**ipv4** | **ipv6**} command in XR EXEC mode. To remove the configured DSCP or precedence value, use the **no** form of this command.

logging {**ipv4** | **ipv6**} {**dscp** *dscp-value* | **precedence** {*numbername*}}
no logging {**ipv4** | **ipv6**} {**dscp** *dscp-value* | **precedence** {*numbername*}}

Syntax Description

ipv4 / **ipv6**	Sets the DSCP or precedence bit for IPv4 or IPv6 packets.
dscp *dscp-value*	Specifies differentiated services code point value or per hop behavior values (PHB). For more information on PHB values, see Usage Guideline section below. The range is from 0 to 63. The default value is 0.
precedence {*number* | *name*}	Sets Type of Service (TOS) precedence value. You can specify either a precedence number or name. The range of argument *number* is between 0 to 7. The *name* argument has following keywords: • routine—Match packets with routine precedence (0) • priority—Match packets with priority precedence (1) • immediate—Match packets with immediate precedence (2) • flash—Match packets with flash precedence (3) • flash-override—Match packets with flash override precedence (4) • critical—Match packets with critical precedence (5) • internet—Match packets with internetwork control precedence (6) • network—Match packets with network control precedence (7)

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

By specifying PHB values you can further control the format of locally generated syslog traffic on the network.

You may provide these PHB values:

- af11—Match packets with AF11 DSCP (001010)
- af12—Match packets with AF12 dscp (001100)

- af13—Match packets with AF13 dscp (001110)
- af21— Match packets with AF21 dscp (010010)
- af22—Match packets with AF22 dscp (010100)
- af23—Match packets with AF23 dscp (010110)
- af31—Match packets with AF31 dscp (011010)
- af32—Match packets with AF32 dscp (011100)
- af33—Match packets with AF33 dscp (011110)
- af41—Match packets with AF41 dscp (100010)
- af42—Match packets with AF42 dscp (100100)
- af43— Match packets with AF43 dscp (100110)
- cs1—Match packets with CS1(precedence 1) dscp (001000)
- cs2—Match packets with CS2(precedence 2) dscp (010000)
- cs3—Match packets with CS3(precedence 3) dscp (011000)
- cs4—Match packets with CS4(precedence 4) dscp (100000)
- cs5—Match packets with CS5(precedence 5) dscp (101000)
- cs6—Match packets with CS6(precedence 6) dscp (110000)
- cs7—Match packets with CS7(precedence 7) dscp (111000)
- default—Match packets with default dscp (000000)
- ef—Match packets with EF dscp (10111)

Assured Forwarding (AF) PHB group is a means for a provider DS domain to offer different levels of forwarding assurances for IP packets. The Assured Forwarding PHB guarantees an assured amount of bandwidth to an AF class and allows access to additional bandwidth, if obtainable.

For example AF PHB value af11 - Match packets with AF11 DSCP (001010), displays the DSCP values as 10 and 11. The DSCP bits are shown as 001010 and 001011 .

AF11 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (1)
- Dropped last in AF1 class

Similarly AF PHB value af12 - Match packets with AF12 dscp (001100), displays the DSCP values as 12 and 13. The DSCP bits are shown as 001100 and 001101.

AF12 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (2)

- Dropped second in AF1 class

Class Selector (CS) provides backward compatibility bits,

CS PHB value cs1 - Match packets with CS1(precedence 1) dscp (001000)

CS1 stands for:

- CS1 DSCP bits are displayed as 001000 and 001001
- priority stated as 1

Expedited Forwarding (EF) PHB is defined as a forwarding treatment to build a low loss, low latency, assured bandwidth, end-to-end service. These characteristics are suitable for voice, video and other realtime services.

EF PHB Value ef - Match packets with EF dscp (101110) - this example states the recommended EF value (used for voice traffic).

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to configure DSCP value as 1 for IPv4 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv4 dscp 1
```

This example shows how to configure DSCP value as 21 for IPv6 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv6 dscp 21
```

This example shows how to configure precedence value as 5 for IPv6 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv6 precedence 5
```

logging localfilesize

To specify the size of the local logging file, use the **logging localfilesize** command in XR Config mode. To remove the **logging localfilesize** command from the configuration file and restore the system to the default condition, use the **no** form of this command.

logging localfilesize *bytes*
no logging localfilesize *bytes*

Syntax Description

bytes	Size of the local logging file in bytes. Range is 0 to 4294967295. Default is 32000 bytes.

Command Default *bytes*: 32000 bytes

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines Use the **logging localfilesize** command to set the size of the local logging file.

Task ID

Task ID	Operations
logging	read, write

Examples This example shows how to set the local logging file to 90000 bytes:

```
RP/0/RP0/CPU0:router(config)# logging localfilesize 90000
```

logging monitor

To specify terminal lines other than the console terminal as destinations for system logging (syslog) messages and limit the number of messages sent to terminal lines based on severity, use the **logging monitor** command in XR Config mode. To remove the **logging monitor** command from the configuration file and disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor [*severity*]
no logging monitor

Syntax Description

severity	(Optional) Severity level of messages logged to the terminal lines, including events of a higher severity level (numerically lower). The default is **debugging**.

Command Default *severity*: **debugging**

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines The **logging monitor** is for the terminal monitoring. Use the **logging monitor** command to restrict the messages displayed on terminal lines other than the console line (such as virtual terminals). The value set for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the monitor.

Use the **terminal monitor** command to enable the display of syslog messages for the current terminal session.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the severity level of messages logged to terminal lines to errors:

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

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

Command Default

No source IP address is specified.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Normally, a syslog message contains the IP address of the interface it uses to leave the networking device. Use the **logging source-interface** command to specify that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the networking device.

Use the logging, on page 64 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 deprecated

To prevent the logging of messages to the console to indicate that commands are deprecated, use the **logging suppress deprecated** command in XR Config mode. To remove the **logging suppress deprecated** command from the configuration file, use the **no** form of this command.

logging suppress deprecated
no logging suppress deprecated

Syntax Description

This command has no keywords or arguments.

Command Default

Console messages are displayed when deprecated commands are used.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **logging suppress deprecated** command affects messages to the console only.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to suppress the consecutive logging of deprecated messages:

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

logging suppress duplicates

To prevent the consecutive logging of more than one copy of the same system logging (syslog) message, use the **logging suppress duplicates** command in 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 7.0.12	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 console** command.

Command Default

severity: **informational**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	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.

The "Usage Guidelines" section for the logging console command lists the syslog definitions that correspond to the debugging message levels.

Use the logging, on page 64 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 enable** 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)# 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
```

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 7.0.12	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
```

severity (logging)

To specify the filter level for logs, use the **severity** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

severity {*severity*}
no severity

Syntax Description

severity	Severity level for determining which messages are logged to the archive. Possible severity levels and their respective system conditions are listed in the "Usage Guidelines" section for the **logging console** command. The default is **informational**.

Command Default

Informational

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **severity** command to specify the filter level for syslog messages. All syslog messages higher in severity or the same as the configured value are logged to the archive.

The "Usage Guidelines" section for the logging console command describes the acceptable severity levels for the *severity* argument.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to specify that warning conditions and higher-severity messages are logged to the archive:

```
Router(config)# logging archive
Router(config-logging-arch)# severity warnings
```

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 alarm-location information. The **trace** option shows trace data for the alarm location components.
correlator*options*	(Optional) Displays content and information about correlation buffer. Options available are: • buffer: Displays content of the correlation buffer. • info: Displays information about event correlation. • 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. The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are: • *month*—The month of the year. The values for the *month* argument are the names of the twelve months. • *day*—Day of the month. Range is from 01 to 31. • *hh* **:**—Hours. Range is from 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is from 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is from 00 to 59.
events *options*	Displays content and information about the event buffer.The various options available are: • buffer: Displays content of the event buffer. • info: Displays information about events buffer. • rule: Displays specified rules. • ruleset: Displays rulesets. • trace: Displays trace data for the correlation component.
history	Displays 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. The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are as follows: • *month*—The month of the year. The values for the *month* argument are the names of the twelve months. • *day*—Day of the month. Range is from 01 to 31. • *hh* **:**—Hours. Range is from 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is from 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is from 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 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 7.0.12	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.”

To find out OOR state of a router's hardware and Software Development Kit (SDK) resources, you can view the sample output from the **show logging** command with the output modifier as OOR. You can configure the threshold value at which a router reaches the **OOR State Red** or **Yellow** by using the `oor hw threshold` command. For more information, see `oor hw threshold` command in the chapter *Logging Services Commands* of *System Monitoring Command Reference for Cisco 8000 Series Routers*.

```
Router# show logging | inc OOR
Wed Jan 6 23:36:34.138 EST
LC/0/0/CPU0:Jan 6 23:01:09.609 EST: npu_drvr[278]: %PLATFORM-OFA-4-OOR_YELLOW : NPU 1, Table
 nhgroup, Resource stage2_lb_group
LC/0/0/CPU0:Jan 6 23:01:29.655 EST: npu_drvr[278]: %PLATFORM-OFA-4-OOR_YELLOW : NPU 1, Table
 nhgroup, Resource stage2_lb_member
LC/0/0/CPU0:Jan 6 23:01:38.938 EST: npu_drvr[278]: %PLATFORM-OFA-1-OOR_RED : NPU 3, Table
nhgroup, Resource stage2_lb_group
```

show logging history

To display information about the state of the system logging (syslog) history table, use the **show logging history** command in XR EXEC mode mode.

show logging history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show logging history** command to display information about the syslog history table, such as the table size, the status of messages, and the text of messages stored in the table. Simple Network Management Protocol (SNMP) configuration parameters and protocol activity also are displayed.

Use the logging history command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Use the logging history size to change the number of syslog messages that can be stored in the history table.

Task ID

Task ID	Operations
logging	read

Examples

This is the sample output from the **show logging history** command:

```
RP/0/RP0/CPU0:router# show logging history
```

```
Syslog History Table: '1' maximum table entries
saving level 'warnings' or higher
137 messages ignored, 0 dropped, 29 table entries flushed
SNMP notifications disabled
```

This table describes the significant fields shown in the display.

Table 15: show logging history Field Descriptions

Field	Description
maximum table entries	Number of messages that can be stored in the history table. Set with the **logging history size** command.
saving level	Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notifications are enabled). Set with the **logging history** command.
messages ignored	Number of messages not stored in the history table because the severity level is greater than that specified with the **logging history** command.
SNMP notifications	Status of whether syslog traps of the appropriate level are sent to the SNMP server. Syslog traps are either enabled or disabled through the **snmp-server enable** command.

terminal monitor

To enable the display of debug command output and system logging (syslog) messages for the current terminal session, use the **terminal monitor** command in XR EXEC mode.

terminal monitor [**disable**]

Syntax Description

disable	(Optional) Disables the display of syslog messages for the current terminal session.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **terminal monitor** command to enable the display of syslog messages for the current terminal session.

Note Syslog messages are not sent to terminal lines unless the **logging monitor** is enabled.

Use the **terminal monitor disable** command to disable the display of logging messages for the current terminal session. If the display of logging messages has been disabled, use the **terminal monitor** command to re-enable the display of logging messages for the current terminal session.

The **terminal monitor** command is set locally, and does not remain in effect after a terminal session has ended; therefore, you must explicitly enable or disable the **terminal monitor** command each time that you would like to monitor a terminal session.

Task ID

Task ID	Operations
logging	execute

Examples

This example shows how to enable the display syslog messages for the current terminal session:

```
RP/0/RP0/CPU0:router# terminal monitor
```

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.

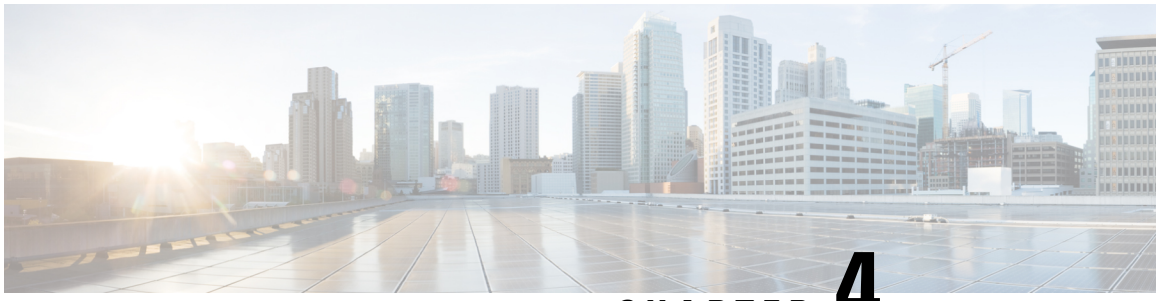
For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

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
```



CHAPTER 4

Onboard Failure Logging Commands

This module describes the Cisco IOS XR7 Software commands used for viewing the onboard failure logging (OBFL) outputs on the router. OBFL gathers boot, environmental, and critical hardware 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, providing improved accuracy in hardware troubleshooting and root cause isolation analysis. Stored OBFL data can be retrieved in the event of a failure and is accessible even if the card does not boot.

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 OBFL is activated by default in all cards and cannot be disabled.

Related Documents

For detailed information about OBFL concepts, configuration tasks, and examples, see the *Onboard Failure Logging* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

clear logging onboard

To clear OBFL logging messages from a node or from all nodes, use the **clear logging onboard** command in XR EXEC mode.

clear logging onboard [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Clears OBFL messages from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default All OBFL logging messages are cleared from all nodes.

Command Modes XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **clear logging onboard** command to clear OBFL messages from all nodes. Use the **clear logging onboard** command with the **location** *node-id* keyword and argument to clear OBFL messages for a specific node. If the specified node is not present, an error message is displayed.

Caution The **clear logging onboard** command permanently deletes all OBFL data for a node or for all nodes. Do not clear the OBFL logs without specific reasons, because the OBFL data is used to diagnose and resolve problems in FRUs.

Caution If OBFL is actively running on a card, issuing the **clear logging onboard** command can result in a corrupt or incomplete log at a later point in time. OBFL should always be disabled before this command is issued.

Task ID

Task ID	Operations
logging	read

Examples

In the following example, the OBFL data is cleared for all nodes in the system:

```
Router# clear logging onboard
Remove all onboard failure log files for 0/RP0/CPU0? [confirm] y
Router#
```

show logging onboard

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

show logging onboard { **alarm** | **current** | **fpd** | **inventory** | **npu** | **temperature** | **uptime** | **voltage** } [**location** *node-id*] [**verbose**]

Syntax Description

alarm	Displays the OBFL alarm information.
current	Displays the OBFL electric current sensor data..
fpd	Displays the OBFL FPD data information.
inventory	Displays the OBFL inventory data information.
npu	Displays the OBFL NPU lifetime data.

temperature	Displays temperature information.
uptime	Displays the OBFL uptime.
voltage	Displays voltage information.
location *node-id*	(Optional) Displays OBFL messages from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	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.

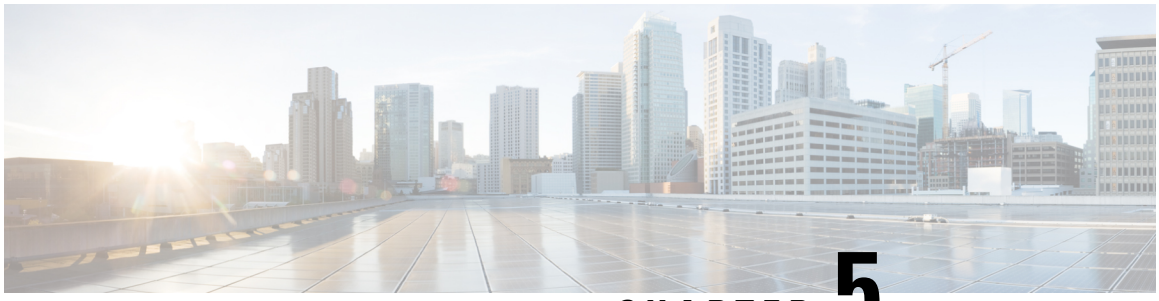
Task ID

Task ID	Operations
logging	read

Examples

This example displays uptime information from the OBFL feature:

```
Router# show logging onboard uptime
OBFL uptime information for: 0/RP0/CPU0
    * indicates incomplete time-sync while record was written
    ! indicates time reset backwards while system was running
--------------------------------------------------------------------------------
    Entity Name                    : Value
--------------------------------------------------------------------------------
    UPTIME CARD INFORMATION
--------------------------------------------------------------------------------
    Previous Chassis SN            : FOC2325NREU
    Current Chassis SN             : FOC2325NREU
    Previous R/S/I                 : -/-/-
    Current R/S/I                  : 0/0/0
    Write Interval                 : 15 (min)
    First Power On TS              : 07/02/2019 02:49:13
    Last Erase TS                  : 03/03/2020 02:46:46
    Rack Change Count              : 0
    Slot Change Count              : 0
    Last Reset Reason              : 0
--------------------------------------------------------------------------------
    UPTIME INFORMATION
--------------------------------------------------------------------------------
    Start Time (UTC)     | End Time (UTC)       | Card Uptime info
    mm/dd/yyyy hh:mm:ss | mm/dd/yyyy hh:mm:ss | Weeks.Days.Hrs.Min.Sec
--------------------------------------------------------------------------------
    02/29/2020 02:08:18 | 03/03/2020 16:39:00 | 0.3.14.30.42
```



CHAPTER 5

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.

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 8000 Series Routers*.

monitor

To monitor counters with full screen auto-updating statistics in real time, use the **monitor** command in XR EXEC mode.

monitor { **interface** [*interface-type* *forward-interface*] | **processes** | **threads** **iteration** *number-of-iteration* }

Syntax Description

interface	Displays interface statistics in real-time.

interface-type	Specifies the Interface type. For more information, use the question mark (**?**) online help function.
forward-interface	Specifies the interface in Rack/Slot/Instance/Port format. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
processes	Displays process statistics in real-time.
threads	Displays thread statistics in real-time.
iteration *number-of-iteration*	Specifies the iteration of the thread.

Command Default

The display refreshes every 2 seconds for the monitor command.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Table 16: Interactive Commands Available for the Monitor 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** or **y** keys to display statistics in packets ("**k**") or bytes ("**y**").

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 or packets.**	
k	Displays statistics in packets ("**k**").
y	(Default) Displays statistics in bytes ("**y**").
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

This is the sample output for the **monitor processes** command. This command displays statistics for all processes in the system.

```
Router# monitor processes

top - 06:55:00 up 1 day, 53 min,  0 users,  load average: 0.16, 0.16, 0.17
Tasks: 476 total,   1 running, 474 sleeping,   0 stopped,   1 zombie
%Cpu(s):  1.4 us,  2.8 sy,  0.0 ni, 95.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 32620396 total, 26953916 free,  3459252 used,  2207228 buff/cache
KiB Swap:        0 total,        0 free,        0 used. 27780560 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND

 4360 root      20   0 8522304  50912  39736 S   5.0  0.2  71:14.11 gsp

 4266 root      20   0 8682364 250472 219884 S   4.0  0.8  55:12.60 spp

 4437 root      20   0 11.489g 847708 190376 S   3.0  2.6 106:27.92 NPU Main Thread

 2818 root      20   0  400632  25636  16372 S   1.0  0.1   8:51.17 docker-containe
```

```
4004 root      20   0 8815260 128036  22980 S   0.7  0.4  10:36.15 SPI Envmon Main

4273 root      20   0 9014704  24536  14760 S   0.7  0.1  13:51.04 wd main

9020 root      20   0   30876   3432   2516 R   0.7  0.0   0:00.10 top

   7 root      20   0       0      0      0 S   0.3  0.0   0:29.94 rcu_sched

 532 root      20   0   42396   6316   4384 S   0.3  0.0   0:00.95 systemd-udevd

4382 root      20   0 7899076  11596   9340 S   0.3  0.0   5:26.69 npu_cfg

4974 root      20   0 8945128  39460  31576 S   0.3  0.1   0:25.38 eth_mgmt

5138 root      20   0 8950280  54216  46884 S   0.3  0.2   0:31.70 ipv6_mfwd_partn

5210 root      20   0 8860556  40356  33444 S   0.3  0.1   1:16.63 xlncd

6088 root      20   0 8911892  40720  35212 S   0.3  0.1   0:00.51 sshd_child_hand

6356 root      20   0 9756120  71712  45168 S   0.3  0.2   5:59.85 pim6

6379 root      20   0 9360656  56624  40020 S   0.3  0.2   2:13.26 igmp

6390 root      20   0 9345208  68944  48724 S   0.3  0.2   3:31.12 mrib6

6539 root      20   0 9785.9m  47284  41672 S   0.3  0.1   0:14.70 udp_main

6580 root      20   0 8717900  29348  24156 S   0.3  0.1   1:23.88 bundlemgr_local

6716 root      20   0 8784028  25228  15628 S   0.3  0.1   0:27.79 Plat SL Client

   1 root      20   0   41700   8032   5364 S   0.0  0.0   0:09.24 systemd
```

monitor interface

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

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

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
wide	Display detailed statistics of the interfaces.
full-name	Display full name of the interfaces. For more information, use the question mark (**?**) online help function.

Command Default

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

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.5.4	The argument *full-name* was introduced.

Usage Guidelines

The argument *full-name* is supported only in 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 interface** *FourHundredGigE0/0/0/0*

To display more than one selected interface, enter the **monitor interface** command with multiple *type interface-path-id* arguments. For example: **monitor interface** *HundredGigE0/0/0/0 HundredGigE0/0/0/1 HundredGigE0/0/0/2*

To display a range of interfaces, enter the **monitor interface** command with a wildcard. For example: **monitor** *interface HundredGigE0/0/**

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 the below 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*

Table 17: 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** or **y** keys to display statistics in packets ("**k**") or bytes ("**y**").
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 or packets.**	
k	Displays statistics in packets ("**k**").
y	(Default) Displays statistics in bytes ("**y**").
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.

```
Router# monitor interface
 Mon Jan 16 11:14:01.107 UTC

 R1                   Monitor Time: 00:00:30          SysUptime: 00:48:19

 Protocol:General
 Interface             In(bps)       Out(bps)     InBytes/Delta  OutBytes/Delta
 FH0/0/0/0                 0/  0%         0/  0%         0/0             0/0
 FH0/0/0/1                 0/  0%         0/  0%         0/0             0/0
 FH0/0/0/10                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/11                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/12                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/13                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/14                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/15                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/16                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/17                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/18                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/19                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/2                 0/  0%         0/  0%         0/0             0/0
 FH0/0/0/20                0/  0%         0/  0%         0/0             0/0
 FH0/0/0/21                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 fourHundredGigE 0/0/0/0
 Mon Jan 16 11:08:07.126 UTC

 R1                   Monitor Time: 00:00:18          SysUptime: 00:42:13


 FourHundredGigE0/0/0/0 is administratively down, line protocol is administratively down
 Encapsulation ARPA

 Traffic Stats:(2 second rates)                                  Delta
   Input  Packets:                          0                        0
```

```
  Input  pps:                             0
  Input  Bytes:                           0                           0
  Input  Kbps (rate):                     0                      (  0%)
  Output Packets:                         0                           0
  Output pps:                             0
  Output Bytes:                           0                           0
  Output Kbps (rate):                     0                      (  0%)

Errors Stats:
  Input  Total:                           0                           0
  Input  CRC:                             0                           0
  Input  Frame:                           0                           0
  Input  Overrun:                         0                           0
  Output Total:                           0                           0
  Output Underrun:                        0                           0

Quit='q', Freeze='f', Thaw='t', Clear='c', Interface='i',
Next='n', Prev='p'

Brief='b', Detail='d', Protocol(IPv4/IPv6)='r'
```

This is the sample output 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
 FH0/0/0/0                0/  0%        0/  0%        0/0             0/0
 FH0/0/0/1                0/  0%        0/  0%        0/0             0/0
 FROM-BGL-AA-             0/ --%        0/ --%        0/0             0/0
 FROM-BGL-AA-             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
 Mon Jan 16 11:15:36.431 UTC

 R1                   Monitor Time: 00:00:04          SysUptime: 00:49:28

 Protocol:General
 In(bps)       Out(bps)      InBytes/Delta  OutBytes/Delta       Interface
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/0
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/1
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/10
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/11
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/12
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/13
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/14
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/15
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/16
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/17
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/18
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/19
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/2
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/20
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/21

 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       Interface
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/0
   0/  0%        0/  0%         0/0             0/0         FourHundredGigE0/0/0/1
   0/ --%        0/ --%         0/0             0/0         FROM-BGL-AA-BB-TO-SJC-CC-DD-1
   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 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 full-name
 Mon Jan 16 11:17:39.694 UTC

 R1                   Monitor Time: 00:00:14          SysUptime: 00:51:41

 Protocol:General
 In(bps)       Out(bps)      InBytes/Delta  OutBytes/Delta  ErrIn/Delta  ErrCRC/Delta
ErrFr/Delta   ErrOvr/Delta   ErrOut/Delta   ErrUnd/Delta
 Interface : FourHundredGigE0/0/0/0
```

```
   0/  0%        0/  0%        0/0             0/0           0/0           0/0
0/0           0/0           0/0           0/0
 Interface : FourHundredGigE0/0/0/1
   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
 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

 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: • **bgp**—Applies a template for monitoring a Border Gateway Protocol (BGP) neighbor. • **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. • **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. • **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. • **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor. • **node cpu**—Applies a template for monitoring the central processing unit (CPU) on a node. Use the *node-id* argument with this entity. • **node memory** —Applies a template for monitoring memory utilization on a node. Use the **location** keyword and *node-id* argument with this entity. • **node process**—Applies a template for monitoring a process on a node. Use the *node-id* and *process-id* arguments with this entity. • **ospf v2protocol**—Applies a template for monitoring an Open Shortest Path First v2 (OSPFv2) process instance. • **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. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
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 7.0.12	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* 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:

```
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:

```
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:

```
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:

```
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: • **bgp**—Applies a statistics collection template for Border Gateway Protocol (BGP). • **interface basic-counters**—Applies a statistics collection template for basic counters. • **interface data-rates**—Applies a statistics collection template for data rates. • **interface generic-counters**—Applies a statistics collection template for generic counters. • **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor. • **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. • **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. • **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. • **ospf v2protocol**—Applies a statistics collection template for Open Shortest Path First v2 (OSPFv2) process instances. • **ospf v3protocol**—Applies a statistics collection template for OSPFv3 process instances.
location {**all** | *node-id*}	Specifies all nodes or a particular node. 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* 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 7.0.12	This command was introduced.

Usage Guidelines

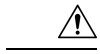
Use the **performance-mgmt apply statistics** command to apply a statistics template and enable statistics collection. Only one template for each entity can be enabled at a time. After samples are taken, the data is sent to a directory on an external TFTP server, and a new collection cycle starts. The directory where data is copied to is configured using the *performance-mgmt resources tftp-server* 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* 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* command.

For more information on the steps to create and apply statistics collection template, refer the topic *Configuring PM Statistics Collection Templates* in the *Implementing Performance Management* chapter of *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.



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:

```
Router(config)#performance-mgmt apply statistics bgp template bgp1
```

This example shows how to enable statistics collection for generic counters using the default template:

```
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:

```
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:

```
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: • **bgp**—Applies a threshold monitoring template for Border Gateway Protocol (BGP). • **interface basic-counters**—Applies a threshold monitoring template for basic counters. • **interface data-rates**—Applies a threshold monitoring template for data rates. • **interface generic-counters**—Applies a threshold monitoring template for generic counters. • **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor. • **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. • **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. • **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. • **ospf v2protocol**—Applies a threshold monitoring template for OSPFv2. • **ospf v3protocol**—Applies a threshold monitoring template for OSPFv3.
location {**all** | *node-id*}	Specifies all nodes or a particular node. 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 146 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 7.0.12	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 128 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 7.0.12	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. **Note** 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 7.0.12	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 7.0.12	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 7.0.12	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: • **bgp**—Creates a statistics collection template for Border Gateway Protocol (BGP). • **interface basic-counters**—Creates a statistics collection template for basic counters. • **interface data-rates**—Creates a statistics collection template for data rates. • **interface generic-counters**—Creates a statistics collection template for generic counters. • **mpls ldp**—Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor. • **node cpu**—Creates a statistics collection template for the central processing unit (CPU). • **node memory**—Creates a statistics collection template for memory utilization. • **node process**—Creates a statistics collection template for processes. • **ospf v2protocol**—Creates a statistics template for Open Shortest Path First v2 (OSPFv2) protocol instances. • **ospf v3protocol**—Creates a statistics template for OSPFv3 protocol instances.
template	Specifies that a template will be used for collection.
template-name	A template name can be any combination of alphanumeric characters, and may include the underscore character (_). Use the show running performance-mgmt, on page 146 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. 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 7.0.12	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 125 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 118 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:

```
Router(config)#performance-mgmt statistics interface data-rates int_data_rates
Router(config_stats-if-rate)# sample-size 25
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: • **bgp** —Creates a template for threshold collection for Border Gateway Protocol (BGP). • **interface basic-counters** —Creates a threshold monitoring template for basic counters. • **interface data-rates** —Creates a threshold monitoring template for data rates. • **interface generic-counters** —Creates a threshold monitoring template for generic counters. • **mpls ldp** —Applies a template for monitoring an MPLS Label Distribution Protocol (LDP) neighbor. • **node cpu** —Creates a threshold monitoring template for the central processing unit (CPU). • **node memory** —Creates a threshold monitoring template for memory utilization. • **node process** —Creates a threshold monitoring template for processes. • **ospf v2protocol** —Creates a threshold monitoring template for Open Shortest Path First v2 (OSPFv2) process instances. • **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 146 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 19: Attribute Values, on page 131 for a list of attributes.
operation	A limiting operation for thresholding that includes: • **EQ** —Equal to. • **GE** —Greater than or equal to. • **GT** —Greater than. • **LE** —Less than or equal to. • **LT** —Less than. • **NE** —Not equal to. • **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. 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.
delta	It compares current and previous data metric values for threshold evaluation.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.7.1	The argument *delta* was introduced.
Release 7.0.12	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 18: 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 19: Attribute Values

Entity	Attributes	Description
bgp	ConnDropped	Number of times the connection was dropped.
	ConnEstablished	Number of times the connection was established.
	ErrorsReceived	Number of error notifications received on the connection.
	ErrorsSent	Number of error notifications sent on the connection.
	InputMessages	Number of messages received.
	InputUpdateMessages	Number of update messages received.
	OutputMessages	Number of messages sent.
	OutputUpdateMessages	Number of update messages sent.
interface basic-counters	InOctets	Bytes received (64-bit).
	InPackets	Packets received (64-bit).
	InputQueueDrops	Input queue drops (64-bit).
	InputTotalDrops	Inbound correct packets discarded (64-bit).
	InputTotalErrors	Inbound incorrect packets discarded (64-bit).
	OutOctets	Bytes sent (64-bit).
	OutPackets	Packets sent (64-bit).
	OutputQueueDrops	Output queue drops (64-bit).
	OutputTotalDrops	Outbound correct packets discarded (64-bit).
	OutputTotalErrors	Outbound incorrect packets discarded (64-bit).

Entity	Attributes	Description
interface data-rates	Bandwidth	Bandwidth, in kbps.
	InputDataRate	Input data rate in kbps.
	InputPacketRate	Input packets per second.
	InputPeakRate	Peak input data rate.
	InputPeakPkts	Peak input packet rate.
	OutputDataRate	Output data rate in kbps.
	OutputPacketRate	Output packets per second.
	OutputPeakPkts	Peak output packet rate.
	OutputPeakRate	Peak output data rate.

Entity	Attributes	Description
interface generic-counters	InBroadcastPkts	Broadcast packets received.
	InMulticastPkts	Multicast packets received.
	InOctets	Bytes received.
	InPackets	Packets received.
	InputCRC	Inbound packets discarded with incorrect CRC.
	InputFrame	Inbound framing errors.
	InputOverrun	Input overruns.
	InputQueueDrops	Input queue drops.
	InputTotalDrops	Inbound correct packets discarded.
	InputTotalErrors	Inbound incorrect packets discarded.
	InUcastPkts	Unicast packets received.
	InputUnknownProto	Inbound packets discarded with unknown proto.
	OutBroadcastPkts	Broadcast packets sent.
	OutMulticastPkts	Multicast packets sent.
	OutOctets	Bytes sent.
	OutPackets	Packets sent.
	OutputTotalDrops	Outbound correct packets discarded.
	OutputTotalErrors	Outbound incorrect packets discarded.
	OutUcastPkts	Unicast packets sent.
	OutputUnderrun	Output underruns.

Entity	Attributes	Description
mpls ldp	AddressMsgsRcvd	Address messages received.
	AddressMsgsSent	Address messages sent.
	AddressWithdrawMsgsRcvd	Address withdraw messages received.
	AddressWithdrawMsgsSent	Address withdraw messages sent.
	InitMsgsSent	Initial messages sent.
	InitMsgsRcvd	Initial messages received.
	KeepaliveMsgsRcvd	Keepalive messages received.
	KeepaliveMsgsSent	Keepalive messages sent.
	LabelMappingMsgsRcvd	Label mapping messages received.
	LabelMappingMsgsSent	Label mapping messages sent.
	LabelReleaseMsgsRcvd	Label release messages received.
	LabelReleaseMsgsSent	Label release messages sent.
	LabelWithdrawMsgsRcvd	Label withdraw messages received.
	LabelWithdrawMsgsSent	Label withdraw messages sent.
	NotificationMsgsRcvd	Notification messages received.
	NotificationMsgsSent	Notification messages sent.
	TotalMsgsRcvd	Total messages received.
	TotalMsgsSent	Total messages sent.
node cpu	AverageCPUUsed	Average system percent CPU utilization.
	NoProcesses	Number of processes.
node memory	CurrMemory	Current application memory (in bytes) in use.
	PeakMemory	Maximum system memory (in MB) used since bootup.
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. **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 7.0.12	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 20: show performance-mgmt bgp Field Descriptions

Field	Description
ConnDropped	Number of times the connection was dropped.
ConnEstablished	Number of times the connection was established.

Field	Description
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. **Note** The data is available to be display only as the monitor data is collected.
statistics	Displays the data collected from statistics collection samples.
data-rates	Displays data from interface data rates entity collections.
generic-counters	Displays data from interface generic counters entity collections.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Displays all interface instances. **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 7.0.12	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 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 21: 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. **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. **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 7.0.12	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 22: 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. **Note** 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. **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 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 7.0.12	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 23: 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. **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 7.0.12	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 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 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

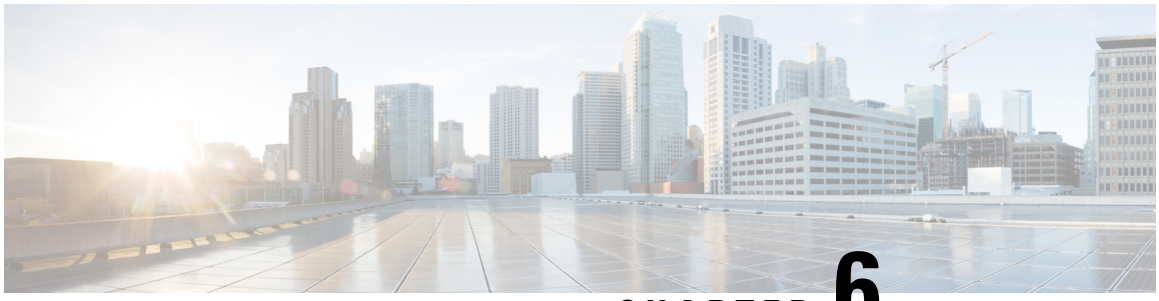
Task ID	Operations
monitor	read, write

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
```



CHAPTER 6

Diagnostic Commands

This module describes the Cisco IOS XR Software commands to configure diagnostics for system monitoring on the router.

For detailed information about the online diagnostics, refer *Online Diagnostics* module in *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

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

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

show diag

To display details about the hardware and software on each node in a router, use the **show diag** command in XR EXEC mode.

show diag [**location** *node-id*] [**chassis** | **details** | **eeprom** | **fans** | **power-supply** | **summary**]

Syntax Description

location *node-id*	(Optional) Displays diagnostic information from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
chassis	(Optional) Displays detailed diagnostics information for the chassis.
details	(Optional) Displays detailed diagnostics information for the current node.

eeprom	(Optional) Displays field diagnostics results from the EEPROM.
fans	(Optional) Displays information about the fans tray.
power-supply	(Optional) Displays information about the power supply.
summary	(Optional) Displays summarized diagnostics results for all nodes in the system.

Command Default

Diagnostics for all nodes installed in the router are displayed.

Hardware and software information for all nodes installed in the router is displayed

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show diag** command displays detailed information on the hardware components for each node, and on the status of the software running on each node.

Task ID

Task ID	Operations
sysmgr	read

Examples

The following example shows excerpts of output from the **show diag details** command:

```
Router# show diag details
Rack 0-Chassis IDPROM - Cisco 8201 1RU System with 24x400GE QSFP56-DD & 12x100GE QSFP28
 Info
    Controller Family          : 0045
    Controller Type            : 0613
    PID                        : 8201-SYS
    Version Identifier         : V00
    UDI Description            : Cisco 8201 1RU System with 24x400GE QSFP56-DD & 12x100GE
QSFP28
    Chassis Serial Number      : FOC2325NREU
    Top Assy. Part Number      : 68-6825-06
    Top Assy. Revision         : 09
    PCB Serial Number          : FOC2324NP35
    PCA Number                 : 73-19428-08
    PCA Revision               : 04
    CLEI Code                  : UNASSIGNED
    ECI Number                 : ECI123
    Deviation Number # 1       : 0
    Deviation Number # 2       : 0
    Deviation Number # 3       : 0
    Deviation Number # 4       : 0
    Deviation Number # 5       : 1126
    Manufacturing Test Data    : 00 00 00 00 00 00 00 00
    Calibration Data           : 00000000
    Chassis MAC Address        : 6c8b.d31f.d400
    MAC Addr. Block Size       : 512
    Hardware Revision          : 0.9
```

```
    Unknown Field (type 0x00d7): 0
    Device values # 1          : 21 80 84 0c 00 00 00 00

0/RP0/CPU0-Base Board IDPROM - Cisco 8201 1RU System with 24x400GE QSFP56-DD & 12x100GE
QSFP28
 Info
    Controller Family          : 0045
    Controller Type            : 0613
    PID                        : 8201-SYS
    Version Identifier         : V00
    UDI Description            : Cisco 8201 1RU System with 24x400GE QSFP56-DD & 12x100GE
QSFP28
    Chassis Serial Number      : FOC2325NREU
    Top Assy. Part Number      : 68-6825-06
    Top Assy. Revision         : 09
    PCB Serial Number          : FOC2324NP35
    PCA Number                 : 73-19428-08
    PCA Revision               : 04
    CLEI Code                  : UNASSIGNED
    ECI Number                 : ECI123
    Deviation Number # 1       : 0
    Deviation Number # 2       : 0
    Deviation Number # 3       : 0
    Deviation Number # 4       : 0
    Deviation Number # 5       : 1126
    Manufacturing Test Data    : 00 00 00 00 00 00 00 00
    Calibration Data           : 00000000
    Chassis MAC Address        : 6c8b.d31f.d400
    MAC Addr. Block Size       : 512
    Hardware Revision          : 0.9
    Unknown Field (type 0x00d7): 0
    Device values # 1          : 21 80 84 0c 00 00 00 00

HundredGigE0/0/0/0-IDPROM - Cisco QSFP28 100G SR4 Pluggable Optics Module
 Info
    IDPROM Format Revision   : 05
    Hardware Revision        : 1
    PID                      : QSFP-100G-SR4-S
    Version Identifier       : V02
    UDI Description          :
    CLEI Code                : CMUIAL8CAB
    ECI Number               : 0
    Top Assy. Part Number    : AFBR-89CDDZ-CS3
    Top Assy. Revision       : 05
    PCB Serial Number        : AVF2131S02J
    PCA Number               : N/A
    PCA Revision             : N/A
    Deviation Number # 1     : 0
    Asset ID                 :
    Asset Alias              :
..........
```

The output displayed for the **show diag details** command is the most comprehensive output displayed for **show diag** command variations. All other variations show a subset of the fields displayed except for the **show diag chassis**, **show diag fans**, and **show diag power-supply** commands, which also enable you to display EEPROM information.

```
RP/0/RP0/CPU0:P1#show diag eeprom
Thu Mar 12 18:16:32.436 UTC
Rack 0-Chassis IDPROM - Cisco 8201 1RU Chassis

 00:  1B 5C 04 FF 48 00 45 40 06 13 CB 92 38 32 30 31   .\..H.E@....8201
 10:  2D 53 59 53 00 00 00 00 00 00
```

```
20:  30 30 00 DA 3C 43 69 73 63 6F 20 38 32 30 31 20   00..<Cisco 8201
30:  31 52 55 20 43 68 61 73 73 69 73 00 00 00 00 00   1RU Chassis.....
40:  00 00 00 00 00 00 00 00 00 00 00 00 2D 44 44      ............-DD
50:  20 26 20 31 32 78 31 30 30 47 20 51 53 46 50 32    & 12x100G QSFP2
60:  38 C2 8B 46 4F 43 32 32 31 37 45 4C 5A 4C 87 44   8..FOC2217ELZL.D
70:  18 86 04 8D 30 37 20 20 C1 8B 46 4F 43 32 32 31   ....07  ..FOC221
80:  39 5A 4F 55 47 E2 46 00 49 00 48 7E 05 8A 30 35   9ZOUG.F.I.H~..05
90:  20 20 C6 8A 55 4E 41 53 53 49 47 4E 45 44 EB 86     ..UNASSIGNED..
A0:  45 43 49 31 32 33 88 00 00 00 00 88 00 00 00 00   ECI123..........
B0:  88 00 00 00 00 88 00 00 00 00 88 00 00 02 35 C4   ..............5.
C0:  08 00 00 00 00 00 00 00 00 00 86 00 00 00 00 C3 06   ................
D0:  78 99 52 4C D8 00 43 02 00 41 00 01 D7 44 00 00   x.RL..C..A...D..
E0:  00 00 C9 08 2F 20 22 08 00 00 00 00 FF FF FF FF   ..../ ".........
F0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
100:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
110:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
120:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
130:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
140:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
150:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
160:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
170:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
180:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
190:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1A0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1B0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1C0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1D0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1E0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
1F0:  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
```

This table describes the significant fields shown in the display.

Table 24: show diag Field Descriptions

Field	Description
MAIN	Provides the following general information about the hardware: • Board type • Revision • Device identifier • Serial number
PCA	Cisco printed circuit assembly (PCA) hardware and revision number.
PID	Displays the product identifier (PID) revision for the specified node.
VID	Displays the version identifier (VID) for the specified node.
CLEI	Displays the common language equipment identifier (CLEI) for the specified node.
ECI	Displays the equipment catalog item (ECI) for the specified node.
Board State	Displays the current software on the board and whether or not the board is running.

Field	Description
PLD	Displays the information about the following programmable logic device (PLD) components on the current module: • Processor • Power • MONLIB
SPEED	Displays speed information for the various components of the specified node, in megahertz.
MEM Size	Displays the memory size of the specified node, in megabytes.
RMA	Displays returned material adjustment (RMA) information for the specified node.
DIAGNOSTICS RESULTS	Provides the following information about the last diagnostics test that was run on the specified node: • ENTRY 1 • TIMESTAMP—Time stamp for the last diagnostic test that was run on the node. • VERSION • PARAM1 • PARAM2 • TESTNUM—Identifies the test that was run on the node. • RESULT—Displays whether the last diagnostic test passed or failed. • ERRCODE

diagnostic monitor interval

To change the interval at which the online diagnostic tests send packets to the Network Processing Units (NPU) for a specific interval at a specified location, use the **diagnostic monitor interval** command in Config mode. To disable the configuration and restore the system to its original state, use the **no** form of this command.

diagnostic monitor interval location *node-id* **test** *test-name* *number-of-days hours:minutes:seconds.milliseconds*

Syntax Description

node-id	Specifies a location where diagnostic monitoring was configured. The *node-id* argument is entered in the *rack/slot/module* notation.
test-name	Name of the diagnostic test.
number-of-days	Interval between each test run. The *number-of-days* variable specifies the number of days between each test run.

hours:minutes:seconds.milliseconds	The *hours:minutes:seconds.milliseconds* variable specifies the test interval. Hours is a number in the range from 0 through 23, minutes is a number in the range from 0 through 59, seconds is a number in the range from 0 through 59, and milliseconds is a number in the range of 0 through 999.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

Examples

This example shows how to set the diagnostic testing at an interval of 1 hour, 2 minutes, 3 seconds, and 4 milliseconds at location 0/1/CPU0:

```
Router# config
Router(config)# diagnostic monitor interval location 0/1/cpu0 test 1 0 1:2:3.4
```

diagnostic monitor location disable

To disable automatic diagnostic testing for a specified location, use the **diagnostic monitor location disable** command in Config mode. To enable the diagnostic testing, use the **no** form of this command.

diagnostic monitor location *node-id* **test** *test-name* **disable**

Syntax Description

node-id	Specifies a location where diagnostic monitoring was configured. The *node-id* argument is entered in the *rack/slot/module* notation.
test-name	Name of the diagnostic test.
disable	Disables diagnostic monitoring for a specified location.

Command Default

By default, the automatic diagnostic tests are enabled in the system.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

Examples

This example shows how to disable the online diagnostic execution at location 0/1/CPU0:

```
Router# config
Router(config)# diagnostic monitor location 0/1/cpu0 test 1 disable
```

diagnostic monitor syslog

To enable the generation of a system log message when any online diagnosis fails, use the **diagnostic monitor syslog** command in Config mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor syslog

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

The following example shows how to generate a system log message when any online diagnostic test fails:

```
Router(config)# diagnostic monitor syslog
```

diagnostic monitor threshold

To set the number of successive failures that triggers the generation of an NP data log, use the **diagnostic monitor threshold** command in Config mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

diagnostic monitor threshold location *node-id* **test** *test-name* **failure-count** *failures*

Syntax Description

node-id	Specifies a location where diagnostic monitoring was configured. The *node-id* argument is entered in the *rack/slot/module* notation.
test-name	Specifies the name of the diagnostic test.
failures	Number of test failures that are allowed. The given range is 1 to 99.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

The following example shows how to set the failure threshold to 35 test failures for test 1 at location 0/1/CPU0:

```
Router# config
Router(config)# diagnostic monitor threshold location 0/1/cpu0 test 1 failure count 35
```

show dataplane-health status

To check the status of a data plane health test and information on whether the test is still running or if it's completed, along with a summary of the results, use the **show dataplane-health status** command in XR EXEC mode.

show dataplane-health status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.5	This command was introduced.

Usage Guidelines

Use the **show dataplane-health status** command to check the status of a data plane health test and information on whether the test is still running or if it's completed, along with a summary of the results.

Task ID

Task ID	Operations
system	read

Examples

This example displays the status of a data plane health test that is in progress:

```
Router# show dataplane-health status
Dataplane health monitoring in progress..
```

This example displays the status of a data plane health test that is completed and has errors:

```
Router# show dataplane-health status
Dataplane health monitoring completed
Summary of results (Module: fabric):
##############################################################################
Output summary legend:
ERROR: Tests were not run for this slice due to some errors
GOOD: Tests were successful for this slice
LOSS: Packet loss was observed for this slice
CORRUPT: Packet corruption was observed for this slice
##############################################################################
  LC    NP     Slice        GOOD        LOSS     CORRUPT       ERROR
------------------------------------------------------------------------------
------------------------------------------------------------------------------
   1     0         0     2526253           0           0           0
                   1     2527136           0           0           0
                   2     2526235           0           0           0
         1         0     2527166           0           0           0
                   1     2527217           0           0           0
                   2     2526424           0           0           0
------------------------------------------------------------------------------
   2     0         0     2526733           0           0           0
                   1     2526948           0           0           0
                   2     2526554           0           0           0
         1         0     2526294           0           0           0
                   1     2526220           0           0           0
                   2     2526085           0           0           0
------------------------------------------------------------------------------
   3     0         0     2525876           0           0           0
                   1     2526642           0           0           0
                   2     2525957           0           0           0
```

```
          1         0     2526491          0          0          0
                    1     2526263          0          0          0
                    2     2526200          0          0          0
          2         0     2526804          0          0          0
                    1     2526135          0          0          0
                    2     2526328          0          0          0
-------------------------------------------------------------------------------
   4      0         0      493934          0      11501          0
                    1           0          0          0          0
                    2           0          0          0          0
          1         0      493605          0      11591          0
                    1           0          0          0          0
                    2           0          0          0          0
-------------------------------------------------------------------------------
   5      0         0      505389          0         30          0
                    1           0          0          0          0
                    2           0          0          0          0
          1         0      505358          0         23          0
                    1           0          0          0          0
                    2           0          0          0          0
-------------------------------------------------------------------------------
   6      0         0     2526307          0          0          0
                    1     2525905          0          0          0
                    2     2526142          0          0          0
          1         0     2526755          0          0          0
                    1     2526603          0          0          0
                    2     2526607          0          0          0
*********************************************************************************
Corruption detected:(LC4/0 <-> FC2/0) (LC4/1 <-> FC2/0) (LC5/0 <-> FC3/0) (LC5/1 <-> FC3/0)


*********************************************************************************
FAILURES DETECTED IN DATAPATH for fabric mode.
Please run "monitor dataplane-health module no-fabric"
Please check /harddisk:/dph_mon/dataplane_health_fabric_mode_report.txt
*********************************************************************************
```

show diagnostic trace location

To display the logging information of the online diagnostic tests for a specific location, use the **show diagnostic trace location** command in Config mode.

show diagnostic trace location *node-id*

Syntax Description

node-id	Specifies a location where diagnostic monitoring was configured. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

The following example shows the online diagnostic logging information at 0/1/CPU0 location:

```
Router# config
Router(config)# show diagnostic trace location 0/1/CPU0
Apr  1 18:09:38.180 diags/online/packet 0/1/CPU0 t5879 Sending a packet to SPP
Apr  1 18:09:38.180 diags/online/packet 0/1/CPU0 t5879 Sending a packet to SPP
Apr  1 18:09:38.180 diags/online/engineer 0/1/CPU0 t5879 Now sending a pak(seq 1276),
destination slot 1 (card type 0x2), NP 0
Apr  1 18:09:38.180 diags/online/engineer 0/1/CPU0 t5879 Now sending a pak(seq 1276),
destination slot 1 (card type 0x2), NP 1
Apr  1 18:09:38.180 diags/online/engineer 0/1/CPU0 6904# t5879 Slot 1 has 2 NPs for NPU
loopback test, Inactive NP mask: 0x0
Apr  1 18:09:38.180 diags/online/engineer 0/1/CPU0 7456# t5879 Packets sent, time
tick=77148425000000
Apr  1 18:09:38.190 diags/online/gold_message 0/1/CPU0 9188# t5879 0/1/CPU0:
SFNPULoopback{ID=1} Completed Successfully.
Apr  1 18:09:38.190 diags/online/gold_message 0/1/CPU0 9740# t5879 0/1/CPU0: running parallel
 test...
Apr  1 18:09:38.190 diags/online/engineer 0/1/CPU0 8008# t5879 Time took to receive 2 pkts:
 10000000 nsec, timeout val: 500000000 nsec
Apr  1 18:09:38.190 diags/online/engineer 0/1/CPU0 8560# t5879 Successfully verified a
packet, seq. no.: 1276
Apr  1 18:09:38.190 diags/online/engineer 0/1/CPU0 9112# t5879 Successfully verified a
packet, seq. no.: 1276
Apr  1 18:09:38.190 diags/online/engineer 0/1/CPU0 9664# t5879 exp_mask: 0x00000003 mask:
0x00000003, err_mask: 0x00000000
```

show diagnostic result

To display diagnostic test results, use the **show diagnostic result** command in EXEC mode.

show diagnostic result location *node-id* **[detail]**

Syntax Description

location *node-id*	Displays the diagnostic test results for a specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Specifies detailed results.

Command Default None

Command Modes Exec mode

Command History

Release	Modification
Release 7.5.2/Release 7.3.5	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
diag	read, write
cisco-support	read

The following example shows the online diagnostic test results at 0/5/CPU0 location:

```
Router#show diagnostic result location 0/5/CPU0

0/5/CPU0:

Overall diagnostic result: PASS
Diagnostic level at card bootup: bypass

Test results: (. = Pass, F = Fail, U = Untested)

1 ) SFNPULoopback --------------------> .


Router#show diagnostic result location 0/5/CPU0 detail

0/5/CPU0:

Overall diagnostic result: PASS
Diagnostic level at card bootup: bypass

Test results: (. = Pass, F = Fail, U = Untested)

_____________________________________________________________________________

1 ) SFNPULoopback --------------------> .

Error code ------------------> 0 (DIAG_SUCCESS)
Total run count -------------> 31
Last test execution time ----> Fri Jun 9 08:28:39 2023
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> Fri Jun 9 08:28:39 2023
Total failure count ---------> 0
Consecutive failure count ---> 0
```

monitor dataplane-health

To monitor the health of data plane components including fabric and NPUs, use the **monitor dataplane-health** command in EXEC mode.

monitor dataplane-health [module { **fabric** | **no-fabric** } **pattern** { *byte-pattern* | **default-patterns** } **duration** *test-duration* **gap** *time-gap* **report** { **detail** | **summary** } **location** { **all** | *node-id* } **stop-on-failure-for-lc** { **false** | **true** } **prompt]**

Syntax Description

fabric	(Optional) Checks the fabric path for issues.
no-fabric	(Optional) Checks the NPU path for issues.
pattern { *byte-pattern* | **default-patterns** }	(Optional) Specifies the data pattern that must be used by the utility to detect datapath memory corruption. You can either specify a byte pattern from a range of 0-255, or specify **default-patterns**. The available default patterns are **0x00, 0xf0, 0x0f, 0xff, 0x55**.
duration *test-duration*	(Optional) Specifies the duration for which the traffic tests are run for each pattern. The default duration is 10 seconds per pattern. For example, if the default pattern is used, and duration is specified as 10 seconds, the test traffic runs for 50 seconds. Range is 1–60 seconds.
gap *time-gap*	(Optional) Specifies the time interval between traffic test runs on consecutive NPU slices. Default gap is 5 seconds. Range is 1–30 seconds.
report { **detail** | **summary** }	(Optional) Displays the summary or detailed report. By default, the summary report is displayed. Detail option displays more detailed information. In both cases, a detailed report (regardless of the selected option) is saved at the location: `harddisk:/dataplane_health_detail_report.txt` **Note** You must archive the report file before subsequent runs, as this file is overwritten on re-execution of the command.
location { **all** | *node-id* }	(Optional) Specifies the line card on which the utility is run. By default, the utility is executed on all LCs in the system. You can also choose a specific LC if necessary.
stop-on-failure-for-lc { **true** | **false** }	(Optional) Specifies if the testing must stop or continue when the utility detects an issue. If **true** (default) option is selected, the testing stops when an issue is detected. If **false** is selected, the testing continues to completion even after an issue is detected on the LC.
prompt	(Optional) Displays a warning message on the impact of this utility, and prompts for your confirmation to run this utility. If you choose NO to the prompt, tests will not be executed. By default, the utility does not prompt for your confirmation.

Command Default

Monitoring is disabled.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.3.5	This command was introduced.

Usage Guidelines

Use the **monitor dataplane-health** command to run the Data plane Health Check utility. Do not use this command on a router that carries live traffic, as this utility affects the system performance. Use this command only on an isolated router.

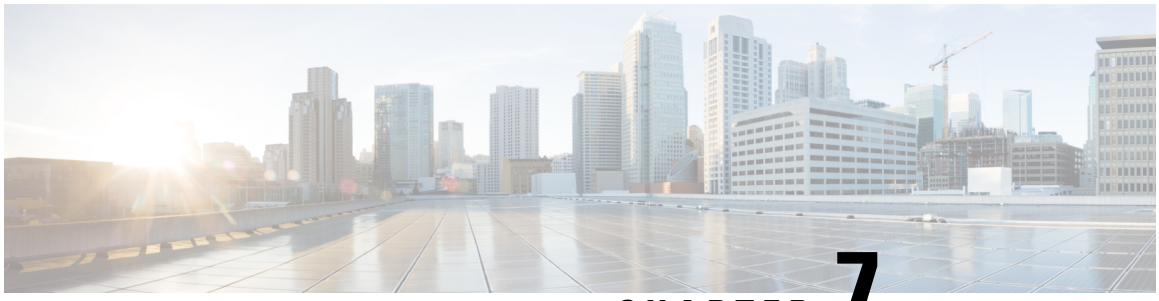
Task ID

Task ID	Operations
system	execute
basic-services	

This example shows how to run the Data plane Health Check utility:

```
Router# monitor dataplane-health

Wed Aug  9 20:28:18.263 UTC
THIS COMMAND IMPACTS SYSTEM PERFORMANCE AND SHOULD IDEALLY BE RUN ON A ROUTER THAT IS
ISOLATED.
DO YOU REALLY WANT TO CONTINUE? (yes/no):
yes
Details of the test results are logged in harddisk:/dataplane_health_detail_report.txt
Estimated time for completion: 804 seconds
Ensure that the terminal/vty session timeout is greater than 804 seconds
Testing in progress (suggest not to break the tests)
.....................................................................................................................
Datapath test on all requested LC/NPU/slice completed
Summary of results:
###############################################################################
Output summary legend:
ERROR: Tests were not run for this slice due to some errors
GOOD: Tests were successful for this slice
LOSS: Packet loss was observed for this slice
CORRUPT: Packet corruption was observed for this slice
###############################################################################
-------------------------------------------------------------------------------
  LC    NP     Slice    GOOD    LOSS   CORRUPT     ERROR
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
   1     0         0     500       0         0         0
                   1     500       0         0         0
                   2     500       0         0         0
         1         0     500       0         0         0
                   1     500       0         0         0
                   2     500       0         0         0
         2         0     500       0         0         0
                   1     500       0         0         0
                   2     500       0         0         0
-------------------------------------------------------------------------------
   2     0         0     501       0         0         0
                   1     500       0         0         0
                   2     500       0         0         0
         1         0     501       0         0         0
                   1     501       0         0         0
                   2     500       0         0         0
         2         0     500       0         0         0
                   1     501       0         0         0
                   2     500       0         0         0
-------------------------------------------------------------------------------
   3     0         0       0       0         0         5
                   1     500       0         0         0
                   2       0       0         0         5
```

```
          1         0       0       0         0         5
                    1     500       0         0         0
                    2       0       0         0         5
          2         0       0       0         0         5
                    1     500       0         0         0
                    2       0       0         0         5
          3         0       0       0         0         5
                    1     500       0         0         0
                    2       0       0         0         5
********************************************************************************
SOME ERRORS PREVENTED DATAPATH CHECKS FROM BEING RUN FOR SOME LC/NP/SLICE
Please check harddisk:/dataplane_health_detail_report.txt
********************************************************************************
```



CHAPTER 7

Graceful Handling of Out of Resource Situations 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 8000 Series Routers*.

oor hw

To configure hardwares for Out of Resource (OOR) situations and to configure OOR threshold values, 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 { **dampening** *timeout-value* | **threshold** | { **red** *red-threshold-value* | **yellow** *yellow-threshold-value* } }

oor hw { **dampening** *timeout-value* | **threshold** { **red yellow** } *threshold-value* }

Syntax Description

dampening *timeout-value*	Configures the timeout value of dampening the OOR state.
threshold	Configures the threshold values of OOR states.
red *red-threshold-value*	Specifies the threshold value for OOR state, **Red**. This value indicates that the hardware and SDK resources are utilized over the permissible limits.You can configure this value as a percentage.

yellow *yellow-threshold-value*	Specifies the threshold value for OOR state, **Yellow**. This value indicates that the hardware and SDK resources are close to being utilized over the permissible limits.You can configure this value as a percentage.

Command Default

By default, the threshold value for **Red** and **Yellow** OOR states are 95% and 80% respectively.

Command Modes

XR Config mode

Task ID

Task ID	Operations
config-services	read, write

Examples

This example shows how to configure threshold values for OOR states:

```
Router(config)#oor hw threshold red 96
Router(config)#oor hw threshold yellow 85
Router(config)#commit
```

show ofa transport async stats client fib

To display the async response error stats that are sent through the out-of-band async channel from OFA npu_drvr to FIM Mgr, you can use the **show ofa transport async stats client fib** command in XR EXEC mode.

show ofa transport async stats client fib

Command Default

None

Command Modes

XR Exec Mode

Command History

Release	Modification
Release 7.5.4	This command was updated to include support for Protection Groups.
Release 7.3.1	This command was introduced.

The following example displays entries that are queued in the FIB OOR retry queue based on the object queue ID, using the **show ofatransport async stats client fib** command:

```
RP/0/RP0/CPU0:PE1# show ofa transport async stats client fib <>
Client name: OfaAsyncFeedbackClientFib

Channel Type:
```

```
Async P2P Notification:

Message Type:
NoMemory rx:0 tx:0

HwFailure rx:0 tx:0

OutOfResource rx:0 tx:0

IssuV2Primary rx:0 tx:0

ReplayDone rx:0 tx:0

Dump rx:0 tx:0

DelayedDelete rx:8 tx:8

NpuUp rx:0 tx:0

NpuDown rx:0 tx:0

WbStart rx:0 tx:0

WbEnd rx:0 tx:0

DebugInfo rx:0 tx:0

AsyncProgramError rx:44 tx:44 → Default Async errors sent to PI-FIB

AsyncResolveError rx:0 tx:0

AsyncEnoent rx:0 tx:0

AsyncSWIDOutOfResource rx:0 tx:0

NpdEvent rx:0 tx:0

FabricUp rx:0 tx:0

FabricDown rx:0 tx:0

OorMsg rx:0 tx:0

CustomMsg rx:224 tx:224 → Custom Async errors sent to PI-FIB
```

show cef object-queue

To display entries that are queued in the FIB OOR retry queue based on the object queue ID, you can use the **show cef object-queue location** command in XR EXEC mode.

show cef object-queue

Syntax Description

location	Displays the queued entries in the FIB OOR for all locations.

Command Default

None

Command Modes XR Exec Mode

Command History

Release	Modification
Release 7.5.4	This command was updated to include support for Protection Groups.
Release 7.3.1	This command was introduced.

The following example displays entries that are queued in the FIB OOR retry queue based on the object queue ID, using the **show cef object-queue location** <> command:

```
RP/0/RP0/CPU0:PE1# show cef object-queue location 0/0/cpu0
Queue                          QID   No. of Markers   No. of Objects
-------------------------------------------------------------------------
OOR FEC                        23    0                17

OOR LEAF                       24    1                0
OOR NHINFO                     25    1                0
OOR GENERIC                    26    1                0
```

The following is an example usage of the **show cef object-queue queue** <*queue-id*> **location** <> command:

```
RP/0/RP0/CPU0:PE1#sh cef object-queue queue 23 location 0/0/cpu0
Wed Nov 18 21:39:04.432 EST
PATHLIST pl:0x309a912db0 paths:2 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.1.10.16/32 leaf:0x309713a890
PATHLIST pl:0x309a912cc8 paths:2 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.1.14.218/32 leaf:0x309e46c8b8
PATHLIST pl:0x309a912be0 paths:2 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.1.17.63/32 leaf:0x309e469738
PATHLIST pl:0x309a912a10 paths:2 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.1.22.9/32 leaf:0x309e503b00
PATHLIST pl:0x309a912928 paths:2 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.1.24.110/32 leaf:0x309e4f1a40
PATHLIST pl:0x309a912758 paths:3 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.0.0.182/32 leaf:0x30ad885fa0
PATHLIST pl:0x309a9124a0 paths:3 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.0.19.208/32 leaf:0x30ad889228
PATHLIST pl:0x309a9123b8 paths:3 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.0.26.46/32 leaf:0x30ad889c78
PATHLIST pl:0x309a905430 paths:3 pl-type:Shared
1st prefix dependent: default 0xe0000000 202.0.51.166/32 leaf:0x3096582798
```

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 { *resource-type* | **all** } **location** { **all** *location-id* }

Syntax Description

all	Use the **all** keyword to display the usage of all the OFA resources for a single location or all locations.
resource-type	Specify the **resource-type** to display the usage of the particular OFA resource for a single location or all locations.
location all	Use the **location all** keywords to display the usage of a single resource type or all resource types for all locations.
location *location-id*	Specify the *location-id* to display the usage of a single resource type or all resource types for the particular location.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	The following resource types are added to the command: • egresslargeencaptb • sipidxtbl • myipv4tbl • tunneltermination
Release 7.3.1	This command was introduced.

Task ID

Task ID	Operations
interface	read
cisco-support	read

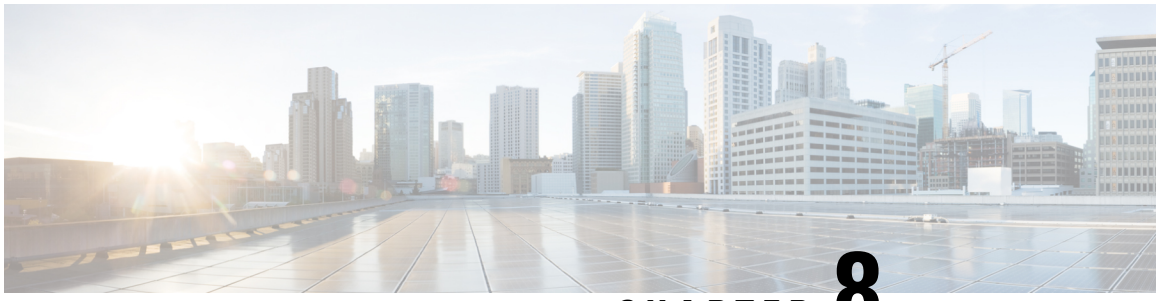
The **show controllers npu resources lpmtcam location** *0/0/CPU0* command displays that the lptcam resource has reached Out of Resource (OOR) state as it has exceeded the usage thresholds.

```
RP/0/RP0/CPU0:ios# show controllers npu resources lpmtcam location 0/0/CPU0
HW Resource Information
    Name                            : lpm_tcam
    Asic Type                       : Pacific

NPU-0
OOR Summary
        Estimated Max Entries       : 100
        Red Threshold              : 95 %
        Yellow Threshold            : 80 %
```

```
        OOR State                    : Red
        OOR State Change Time        : 2020.Dec.17 09:53:02 EST
```

This example displays the IPv6 shortening entry as highlighted below. With both the IPv6 LPM normal entries and IPv6 LPM shortening entries in the output, you can determine the total number of IPv6 routes.

```
RP/0/RP0/CPU0:ios# show controllers npu resources lpmtcam location 0/0/CPU0
Thu Jan 18 00:59:50.488 UTC
HW Resource Information
    Name : lpm_tcam
    Asic Type : Q200

NPU-0
OOR Summary
  Estimated Max Entries : 100
  Red Threshold : 95 %
  Yellow Threshold : 80 %
  OOR State : Green

OFA Table Information
(May not match HW usage)
 iprte : 3
 ip6rte : 2
 ip6mcrte : 0
 ipmcrte : 0

Current Hardware Usage
 Name: lpm_tcam
 Estimated Max Entries : 100
 Total In-Use : 0 (0 %)
 OOR State : Green

 Name: v4_lpm
 Total In-Use : 6

 Name: v6_lpm
 Total In-Use : 4

 Name: v6_shortening_lpm
 Total In-Use : <>
```



CHAPTER 8

IP Service Level Agreements Commands

This module describes the Cisco IOS XR Software commands to implement IP service level agreements for system monitoring on the router.

For detailed information about IP service level agreements concepts, configuration tasks, and examples, see the *Implementing IP Service Level Agreements* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# access-list ipsla
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react connection-loss
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# action logging
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

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

```
Rouuter# configure
Rouuter(config)# ipsla
Rouuter(config-ipsla)# schedule operation 1
Rouuter(config-ipsla-sched)# ageout 3600
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# buckets 30
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# buckets 10
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics interval 60
Router(config-ipsla-op-stats)# buckets 50
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# control disable
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# datasize request 512
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# destination address 192.0.2.12
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# destination port 11111
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# distribution count 15
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# distribution interval 50
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# exp 5
```

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)# exp 5
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# filter all
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# force explicit-null
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
Router(config-ipsla-mplslm-sched)# frequency 1200
Router(config-ipsla-mplslm-sched)# schedule period 600
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls discovery vpn
Router(config-ipsla-mpls-discovery-vpn)# interval 120
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# key-chain ipsla-keys
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
Router(config-ipsla-sched)# life forever
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# lives 2
```

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 7.3.2	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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# low-memory 102400
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# lsp selector ipv4 127.10.10.1
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# lsr-path 192.0.2.40
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# statistics hourly
Router(config-ipsla-op-stats)# maximum hops 20
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# statistics hourly
Router(config-ipsla-op-stats)# maximum paths 20
```

monitor (IP SLA)

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls discovery vpn
Router(config-ipsla-mpls-discovery-vpn)#
```

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

None

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)#
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the IP SLA **operation** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)#
```

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

Command Default

No default behavior or values.

Command Modes

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls ls output interface pos 0/1/0/0
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# output nexthop 10.1.1.1
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **packet count** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# packet count 30
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# packet interval 30
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enter path discover submode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
```

```
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# echo interval 777
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# path retry 12
Router(config-ipsla-mplslm-lsp-lpd)# path secondary frequency both 10
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# scan period 2
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# session timeout 22
```

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: • **dest-to-source**—(Optional) Specifies the jitter average destination to source (DS). • **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: • **dest-to-source**—(Optional) Specifies the packet loss destination to source (DS) violation. • **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 7.3.2	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 25: 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

Operation	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	ICMP Path Jitter	MPLS LSP Ping	MPLS LSP Trace
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react connection-loss
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **jitter-average** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **packet-loss** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **rtt** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react rtt
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **timeout** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react timeout
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **verify-error** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react verify-error
Router(config-ipsla-react-cond)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)# react lpd lpd-group action logging
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)#
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **reaction operation** command:

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# reaction operation 1
Router(config-ipsla-react)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction trigger 1 2
```

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. 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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# reply dscp 5
```

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. **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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# target pseudowire 192.168.1.4 4211
Router(config-ipsla-mpls-lsp-ping)# reply mode control-channel
```

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*]

responder twamp [**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) Range is 1 - 604800 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 7.3.2	This command is introduced.

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. 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. 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. Range: 1 - 65535

vrf { *vrf-name* | **any** | **default** }	Configure vrf for the local ip-address. Possible values for vrf: • *vrf-name* of the vrf of the local ip-address • any: use this only when **local-ip** is configured as any • default: use this when the local ip-address belongs to default vrf
timeout *timeout-value*	Configure the inactivity timeout period (in seconds) 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 7.3.2	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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# history
Router(config-ipsla-op-hist)# samples 30
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# scan delete-factor 214
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# scan interval 120
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
Router(config-ipsla-mplslm-sched)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
Router(config-ipsla-sched)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 20
Router(config-ipsla-mplslm-sched)# schedule period 6000
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read

Examples The following sample output is from the **show ipsla application** command:

```
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 26: 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.

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 7.3.2	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 27: 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:

```
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 28: 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.

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla mpls discovery vpn** command:

```
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 29: show ipsla mpls discovery vpn Field Descriptions

Field	Description
BGP next hop	Identifier for the BGP next-hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next-hop neighbor to be used by the MPLS LSP ping or trace operation.
VRF	Names of the virtual routing and forwarding instances (VRFs) that contain routing entries for the specified BGP next-hop neighbor.
PfxCount	Count of the routing entries that participate in the VRF for the specified BGP next-hop neighbor.

show ipsla mpls lsp-monitor lpd

To display LSP Path Discovery (LPD) operational status, use the **show ipsla mpls lsp-monitor lpd** command in 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 7.3.2	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:

```
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 30: 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 7.3.2	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:

```
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 31: 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 mod.

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 mod

Command History

Release	Modification
Release 7.3.2	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.

```
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.

```
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 32: 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: • up—Indicates that the latest operation cycle was successful. • down—Indicates that the latest operation cycle was not successful. • 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:

```
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 33: 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.
Status	Status of the paths. Values can be as follows: • up—Indicates that all the paths were successful. • down—Indicates that all the paths were not successful. • partial—Indicates that only some paths were successful. • 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 7.3.2	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:

```
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 34: 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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

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:

```
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 35: 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.
LSP Selector	LSP selector address of the path.
Outgoing Interface	Outgoing interface of the path.
Nexthop Address	Next hop address of the path.
Downstream Label Stack	MPLS label stacks of the path.

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 7.3.2	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:

```
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:

```
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 36: 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:

```
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 37: 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.

```
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 38: 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.
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.

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 7.3.2	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:

```
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 39: 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.
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.

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 7.3.2	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:

```
Router# show ipsla twamp connection requests
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# source address 192.0.2.9
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# source port 11111
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
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:

```
Router# configure
Router(config)# ipsla operation 2
Router(config-ipsla-op)# type icmp echo
Router(config-ipsla-icmp-echo)# destination address 192.0.2.9
Router(config-ipsla-icmp-echo)# exit
Router(config-ipsla-op)# exit
Router(config-ipsla)# schedule operation 2
Router(config-ipsla-sched)# start 20:0:0 february 7 2008
Router(config-ipsla-sched)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
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:

```
Router# configure
Router(config)# ipsla operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics interval 60
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# statistics hourly
Router(config-ipsla-mplslm-stats)#
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
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:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# tag mplslm-tag
```

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: • 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. • 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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# target ipv4 192.168.1.4 255.255.255.255
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-trace)# target pseudowire 192.168.1.4 4211
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# target traffic-eng tunnel 101
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
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:

```
Router# configure
Router(config)# ipsla reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)# threshold type average 8
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
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:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 2
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# threshold type consecutive 2
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react  jitter-average
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:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 2
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# threshold type immediate
```

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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **threshold type xofy** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)# threshold type xofy 1 5
```

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 7.3.2	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.

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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
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:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# timeout 10000
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# tos 60
```

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 7.3.2	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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# ttl 200
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type icmp echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp echo
Router(config-ipsla-icmp-echo)#
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type icmp path-echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)#
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **type icmp path-jitter** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-jitter
Router(config-ipsla-icmp-path-jitter)#
```

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 7.3.2	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 258 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 261 command)
- Pseudowire (configured with the target pseudowire, on page 260 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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)#
```

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 7.3.2	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 258 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 261 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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
```

```
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)#
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type udp echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)#
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type udp jitter** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)#
```

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 7.3.2	This command was introduced.

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

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure a permanent port for the **type udp ipv4 address** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# responder
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 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# verify-data
```

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 7.3.2	This command was introduced.

Usage Guidelines

Use the **vrf** command to configure a non-default VPN routing and forwarding (VRF) table for an IP SLA operation. A VPN is commonly identified using the name of a VRF table. If you use the **vrf** command in the configuration of an IP SLA operation, the *vrf-name* value is used to identify the VPN for the particular operation.

The default VRF table is used if no value is specified with the **vrf** command. If you enter a VPN name for an unconfigured VRF, the IP SLA operation fails and the following information is displayed in the results for the show ipsla statistics, on page 239 command:

```
Latest operation return code  : VrfNameError
```

The **vrf** command is supported only to configure the following IP SLA operations:

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

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# vrf vpn2
```

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 7.3.2	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.

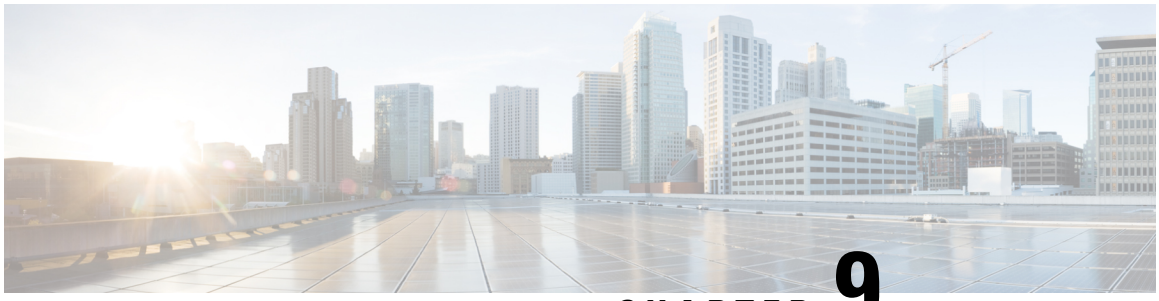
Task ID

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:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)# vrf vpn-lsp
```



CHAPTER 9

Traffic Monitoring Commands

This module describes the Cisco IOS XR Software commands to monitor traffic on the router.

For detailed information about monitoring packet drops concepts, configuration tasks, and examples, see the *Traffic Monitoring* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

hw-module profile packet-loss-alert

To enable log message alerts for traffic-impacting NPU interrupts, use the **hw-module profile packet-loss-alert** command in the XR Config mode.

hw-module profile packet-loss-alert { **3Min** | **5Min** }

Syntax Description

3Min	Specifies a 3 minute duration of packet loss to begin generating log messages. There are atleast 10 error interrupts per minute.
5Min	Specifies a 5 minute duration of packet loss to begin generating log messages. There are atleast 10 error interrupts per minute.

Command Default

This feature is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.1.1	This command was introduced

Usage Guidelines

Only line cards and routers with the Q100, Q200, P100 or G100 based Silicon One ASIC support this feature

Task ID

Task ID	Operation
profile	read, write

Example

Execute the **hw-module profile packet-loss-alert** command to enable system log alerts for packet loss:

```
Router# configure
Router(config)# hw-module profile packet-loss-alert 3Min
Router(config)# commit
```

show drops all

To display the packet drops, 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 packet drops all location all** command displays packet drops for all nodes on all locations

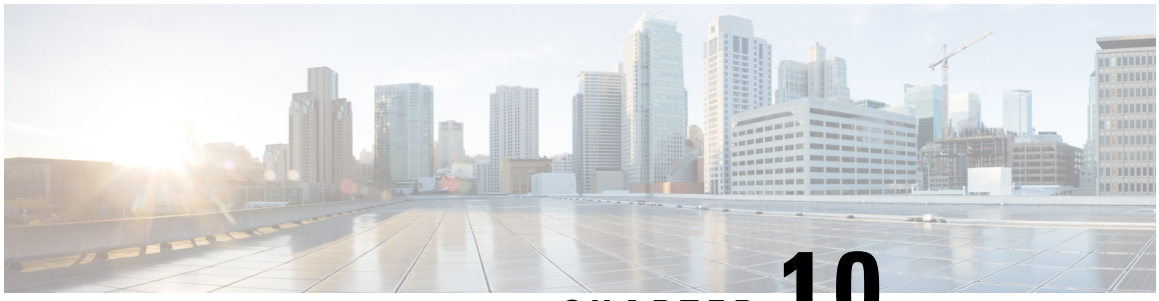
```
RP/0/RP0/CPU0:ios#show drops all location all
-----------------------------------------------
Printing Drop Counters for node 0/RP0/CPU0
-----------------------------------------------
```

```
-------------------
MODULE arp
-------------------


-------------------
MODULE mac
-------------------


-------------------
MODULE npu_traps
-------------------


Trap Type                                       NPU  Trap  Punt       Punt  Punt  Punt
Configured Hardware   Policer Avg-Pkt Packets                Packets
                                                ID   ID    Dest       VoQ   VLAN  TC   Rate(pps)
  Rate(pps)  Level   Size    Accepted             Dropped
================================================================================================


UNKNOWN_VLAN_OR_BUNDLE_MEMBER(D*)               0    4     RPLC_CPU   200   1586  0    67
      134        IFG     64      0                    1

-------------------
MODULE voq_drops
-------------------


-------------------
MODULE cef
-------------------


-------------------
MODULE fabric
-------------------


-------------------
MODULE lpts
-------------------


-------------------
MODULE spp
-------------------
```

The **show packet drops all ongoing location** command displays the packet drops since last executed.

```
RP/0/RP0/CPU0:ios#show drops all ongoing location all

-----------------------------------------------
Printing Drop Counters for node 0/RP0/CPU0
-----------------------------------------------


-------------------
MODULE arp
-------------------
```

```
-------------------
MODULE mac
-------------------


-------------------
MODULE npu_traps
-------------------


-------------------
MODULE voq_drops
-------------------


-------------------
MODULE cef
-------------------


-------------------
MODULE fabric
-------------------


-------------------
MODULE lpts
-------------------


-------------------
MODULE spp
-------------------
```



CHAPTER 10

Monitoring Fabric Links Commands

This module describes the Cisco IOS XR software commands related to monitoring fabric links.

For detailed information about monitoring fabric links concepts, configuration tasks, and examples, see the *Traffic Monitoring* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

hw-module fabric-tsmon-port-reset disable

To disable the maximum port-reset threshold value of five, use the **hw-module fabric-tsmon-port-reset disable** command in XR EXEC mode.

hw-module fabric-tsmon-port-reset disable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, keepalive monitoring is enabled on routers.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines

⚠

Caution We recommend that you troubleshoot and resolve the reason for the fabric port shutdown instead of using the **hw-module fabric-tsmon-port-reset disable** command to prevent the fabric port shutdown.

Use the **hw-module fabric-tsmon-port-reset disable** command to disable the maximum port-reset threshold value of five.

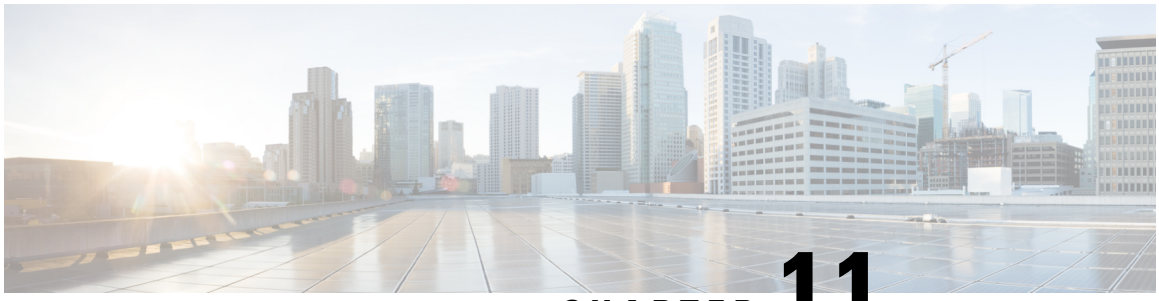
Task ID

Task ID	Operations
config-services	read, write
root-lr	read, write

Examples

The following example shows how to disable the maximum port-reset threshold value of five:

```
Router# configuration terminal
Router(config)# hw-module fabric-tsmon-port-reset disable
Router(config)# commit
```



CHAPTER 11

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

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** }

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.

Command Default

None

Command Modes

EXEC mode

Config mode

Command History

Release	Modification
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 40: 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 ipv6 nd show tech-support arp show tech-support ofa show tech-support routing bgp show tech-support routing isis show tech-support routing bfd show tech-support routing ospf show tech-support routing ospfv3 show tech-support mpls ldp show tech-support bcdl show tech-support bcdlv2 show tech-support rib show tech-support mpls lsd show tech-support cef show tech-support cef platform show tech-support gsp show tech-support l2rib show tech-support l2vpn show tech-support lpts show tech-support spp show tech-support clns show tech-support multicast address-family ipv4 show tech-support multicast address-family ipv6 show tech-support grpc show tech-support service-layer show tech-support appmgr show tech-support netconf show tech-support yserver show tech-support grid show tech-support tunnel-ip show tech-support pbr show tech-support bfdhwoff show tech-support flowspec

Custom Option	Release	List of commands outputs collected
		show tech-support access-lists ipv4 show tech-support access-lists ipv6 show tech-support ds show tech-support os show tech-support placed show tech-support qos pi show tech-support processmgr show tech-support spio show tech-support sysdb show tech-support telemetry model-driven show tech-support bundles show tech-support dhcp ipv4 base show tech-support dhcp ipv4 client show tech-support dhcp ipv4 proxy show tech-support dhcp ipv4 relay show tech-support dhcp ipv4 server show tech-support dhcp ipv4 snoop show tech-support dhcp ipv6 base show tech-support dhcp ipv6 client show tech-support dhcp ipv6 proxy show tech-support dhcp ipv6 relay show tech-support dhcp ipv6 server show tech-support ipinfra show tech-support protection-notif show tech-support raw show tech-support rsi show tech-support statsd show tech-support tcp nsr show tech-support udp show tech-support pfi show tech-support cfgmgr show tech-support tty show tech-support rdsfs

Custom Option	Release	List of commands outputs collected
	Release 24.2.11	

Custom Option	Release	List of commands outputs collected
		show tech-support aib show tech-support ipv6 nd show tech-support arp show tech-support ofa show tech-support routing bgp show tech-support routing isis show tech-support routing bfd show tech-support routing ospf show tech-support routing ospfv3 show tech-support mpls ldp show tech-support bcdl show tech-support bcdlv2 show tech-support rib show tech-support mpls lsd show tech-support cef show tech-support cef platform show tech-support gsp show tech-support l2rib show tech-support l2vpn show tech-support l2vpn platform show tech-support lpts show tech-support spp show tech-support clns show tech-support multicast address-family show tech-support multicast address-family show tech-support mgbl show tech-support service-layer show tech-support appmgr show tech-support grid show tech-support tunnel-ip show tech-support pbr show tech-support bfdhwoff show tech-support flowspec

Custom Option	Release	List of commands outputs collected
		show tech-support access-lists ipv4 show tech-support access-lists ipv6 show tech-support ds show tech-support os show tech-support placed show tech-support qos pi show tech-support processmgr show tech-support spio show tech-support sysdb show tech-support bundles show tech-support dhcp ipv4 show tech-support dhcp ipv4 show tech-support dhcp ipv4 show tech-support dhcp ipv4 show tech-support dhcp ipv4 show tech-support dhcp ipv4 show tech-support dhcp ipv6 show tech-support dhcp ipv6 show tech-support dhcp ipv6 show tech-support dhcp ipv6 show tech-support dhcp ipv6 show tech-support ipinfra show tech-support protection-notif show tech-support raw show tech-support rsi show tech-support statsd show tech-support tcp nsr show tech-support udp show tech-support pfi show tech-support cfgmgr show tech-support tty 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 platform-fwd show tech-support ofa show tech-support cef show tech-support cef platform show tech-support aib show tech-support grid show tech-support bcdl show tech-support bcdlv2 show tech-support mpls lsd show tech-support rib show tech-support fabric link-include show tech-support mpls traffic-eng show tech-support segment-routing traffic-eng show tech-support optics show tech-support qos platform show tech-support platform-pfc show tech-support qos pi show tech-support arp show tech-support ipv6 nd show tech-support gsp show tech-support access-lists platform show tech-support tunnel-ip show tech-support pbr show tech-support bfdhwoff show tech-support flowspec show tech-support ds show tech-support placed show tech-support service-layer show tech-support processmgr show tech-support os show tech-support grpc show tech-support sysdb show tech-support telemetry model-driven

Custom Option	Release	List of commands outputs collected
		show tech-support bundles show tech-support dhcp ipv4 base show tech-support dhcp ipv4 client show tech-support dhcp ipv4 proxy show tech-support dhcp ipv4 relay show tech-support dhcp ipv4 server show tech-support dhcp ipv4 snoop show tech-support dhcp ipv6 base show tech-support dhcp ipv6 client show tech-support dhcp ipv6 proxy show tech-support dhcp ipv6 relay show tech-support dhcp ipv6 server show tech-support ipinfra show tech-support protection-notif show tech-support raw show tech-support rsi show tech-support spio show tech-support statsd show tech-support tcp nsr show tech-support udp show tech-support pfi show tech-support static show tech-support cfgmgr show tech-support snmp ifmib show tech-support resmon
	Release 24.2.11	

Custom Option	Release	List of commands outputs collected
		show tech-support platform-fwd show tech-support ofa show tech-support cef show tech-support cef platform show tech-support aib show tech-support grid show tech-support bcdl show tech-support bcdlv2 show tech-support mpls lsd show tech-support rib show tech-support fabric link-include show tech-support mpls traffic-eng show tech-support mpls rsvp show tech-support mpls static show tech-support mpls oam show tech-support segment-routing traffic-eng show tech-support optics show tech-support qos platform show tech-support platform-pfc show tech-support qos pi show tech-support arp show tech-support ipv6 nd show tech-support gsp show tech-support l2vpn show tech-support l2vpn platform show tech-support access-lists platform show tech-support tunnel-ip show tech-support pbr show tech-support bfdhwoff show tech-support flowspec show tech-support ds show tech-support placed show tech-support service-layer

Custom Option	Release	List of commands outputs collected
		show tech-support processmgr show tech-support os show tech-support mgbl show tech-support sysdb show tech-support bundles show tech-support dhcp ipv4 base show tech-support dhcp ipv4 client show tech-support dhcp ipv4 proxy show tech-support dhcp ipv4 relay show tech-support dhcp ipv4 server show tech-support dhcp ipv4 snoop show tech-support dhcp ipv6 base show tech-support dhcp ipv6 client show tech-support dhcp ipv6 proxy show tech-support dhcp ipv6 relay show tech-support dhcp ipv6 server show tech-support ipinfra show tech-support protection-notif show tech-support raw show tech-support rsi show tech-support spio show tech-support statsd show tech-support tcp nsr show tech-support udp show tech-support pfi show tech-support static show tech-support cfgmgr show tech-support snmp ifmib show tech-support resmon

Custom Option	Release	List of commands outputs collected
System	Release 7.3.6	

Custom Option	Release	List of commands outputs collected
		show tech-support os show tech-support spi show tech-support fpd show tech-support fabric link-include show tech-support interface show tech-support ofa show tech-support optics show tech-support macsec show tech-support gsp show tech-support platform timing show tech-support ptp show tech-support frequency synchronization show tech-support ethernet controllers show tech-support ethernet interfaces show tech-support pfi show tech-support cfgmgr show tech-support sysdb show tech-support processmgr show tech-support grpc show tech-support linux networking show tech-support telemetry model-driven show tech-support parser show tech-support statsd show tech-support ctrace show tech-support control-ethernet show tech-support pmengine show tech-support ptah show tech-support ds show tech-support pam show tech-support placed show tech-support service-layer show tech-support shmwin show tech-support cpa

Custom Option	Release	List of commands outputs collected
		show tech-support install show tech-support keychain show tech-support alarm-mgr show tech-support ntp show tech-support pool show tech-support protection-notif show tech-support rdsfs show tech-support resmon show tech-support snmp show tech-support ssh show tech-support system-recovery show tech-support tacacs show tech-support tam show tech-support tty show tech-support type6 show tech-support ztp show tech-support bmc show tech-support bundles show tech-support snmp ifmib show tech-support ipinfra show tech-support cef show tech-support cef platform show tech-support rsi
	Release 24.2.11	

Custom Option	Release	List of commands outputs collected
		show tech-support os show tech-support spi show tech-support fpd show tech-support fabric link-include show tech-support interface show tech-support ofa show tech-support optics show tech-support macsec show tech-support gsp show tech-support platform timing show tech-support ptp show tech-support frequency synchronization show tech-support ethernet controllers show tech-support ethernet interfaces show tech-support control-ethernet show tech-support pfi show tech-support cfgmgr show tech-support sysdb show tech-support processmgr show tech-support mgbl show tech-support linux networking show tech-support parser show tech-support statsd show tech-support bundles show tech-support ctrace show tech-support control-ethernet show tech-support pmengine show tech-support ptah show tech-support ds show tech-support pam show tech-support placed show tech-support service-layer show tech-support shmwin

Custom Option	Release	List of commands outputs collected
		show tech-support cpa show tech-support install show tech-support keychain show tech-support alarm-mgr show tech-support ntp show tech-support pool show tech-support protection-notif show tech-support rdsfs show tech-support resmon show tech-support snmp show tech-support ssh show tech-support system-recovery show tech-support tacacs show tech-support tam show tech-support tty show tech-support type6 show tech-support ztp show tech-support bmc show tech-support snmp ifmib show tech-support ipinfra show tech-support cef show tech-support cef platform show tech-support rsi

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
.....................................................................................................................
```

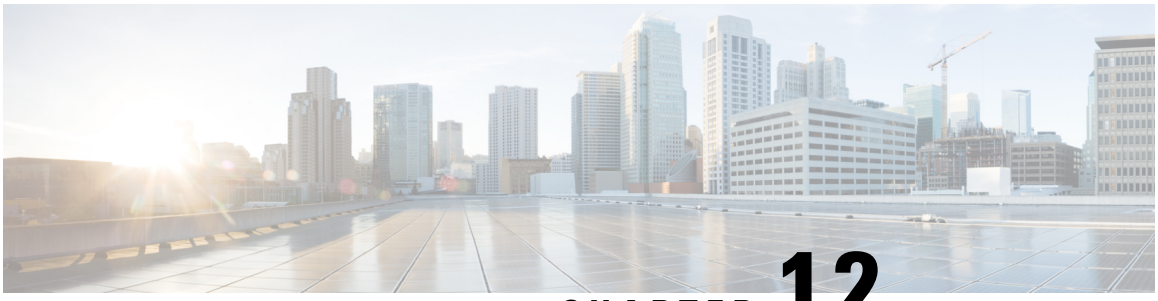
```
Fri Jun 16 20:05:45 UTC 2023 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-custom-traffic-2023-Jun-16.195852.UTC.tgz
++ Show tech end time: 2023-Jun-16.200546.UTC ++
```

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 ++
```



CHAPTER 12

Inbuilt Traffic Generator Commands

This module describes the Cisco IOS XR Software commands to set up and run the inbuilt traffic generator on the Network Processing Unit (NPU) of line cards of distributed systems and route processors of fixed routers.

For detailed information about the inbuilt traffic generator concepts, and examples, see the *Inbuilt Traffic Generator for Network Diagnostics* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

diagnostic packet-generator create

To create an instance of the inbuilt traffic generator, use the command **diagnostic packet-generator create** in EXEC mode.

diagnostic packet-generator create *traffic-generator-name* { **duration** *traffic-duration* | **rate** *packet-rate* | **filename** *packet-file* | **packet** *packet-details* | **traffic-class** *traffic-class* } { **ingress interface** *ingress-interface-name* [**member** *bundle-member-interface*] | **egress interface** *egress-interface-name* [[**npu** *npu*] | [**slice** *slice*]] | **raw** } **capture location** *location*

Syntax Description

traffic-generator-name	Specify a name for the traffic generator instance
duration *traffic-duration*	Specify the traffic duration in seconds
rate *packet-rate*	Specify the traffic-rate in pps
filename *packet-file*	Specify the file with the packet details. The file can be a pcap file with .pcap suffix or a text file with scapy script or hex string.

packet *packet-details*	Specify the packet details directly at command-line Maximum length for packets provided at command line is 255 characters. For larger packets, use the **filename** *packet-file* option.
traffic-class *traffic-class*	Specify the traffic-class
ingress	Specify the traffic generator instance to inject ingress packets
interface *ingress-interface-name*	Specify the ingress interface for packet injection
member *bundle-member-interface*	If the ingress interface is a bundle-interface, specify the member interface for packet injection. If nothing is provided, one of the existing members in the target location will be selected to inject packets.
egress	Specify the traffic generator instance to inject egress packets
interface *egress-interface-name*	Specify the egress interface for packet injection
npu *npu*	Specify the npu from which the packet will be injected. Default value: 0
slice *slice*	Specify the slice from which the packet will be injected. Default value: 0
raw	Specify the traffic generator instance to inject raw packets
capture	Enable packet capture
location *location*	Specify the slot location where you will create the traffic generator instance

Command Default

While creating an **ingress** traffic generator instance, if you did not specify the ethernet header of the packet to be injected, the software will generate a default ethernet header with the following source and destination MAC addresses:

- A default source MAC address of 00:00:00:00:00:01.
- The MAC address of the ingress interface as the destination MAC address.

If you provided a subinterface as the ingress interface, the software will include the VLAN header after the ethernet header.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines

Caution Don't run the inbuilt traffic generator on a live network unless you are fully aware of the impact of packets injected. Injecting packets into a live network may result in network outages.

Caution Raw traffic generator mode should be executed only by Cisco engineers. Improper use of raw mode could cause unexpected behavior, such as NPU lock-up.

Task ID

Task ID	Operation
diag	execute
root-system	execute
root-lr	execute
cisco-support	read, execute

Example

The following example shows how to create a traffic generator instance in ingress mode:

```
Router# diagnostic packet-generator create t1 rate 100 duration 60 packet
IP(src="32.0.0.1",dst="22.0.0.1",ttl=64)/UDP()/Raw(load="a"*100) ingress interface
FourHundredGigE0/0/0/1 capture location 0/RP0/CPU0
OK
```

The following example shows how to create a traffic generator instance in egress mode:

```
Router# diagnostic packet-generator create t1 rate 100 duration 60 packet
Ether(src="A:B:C:D:E:F",dst="1:2:3:4:5:6")/IP(src="32.0.0.1",dst="109.0.0.101",ttl=64)/Raw(load="f"*100)
 egress interface fourHundredGigE0/0/0/0 capture location 0/RP0/CPU0
OK
```

diagnostic packet-generator delete

To delete the inbuilt traffic generator instance, use the command **diagnostic packet-generator delete** in EXEC mode.

diagnostic packet-generator delete *traffic-generator-name* **location** *location*

Syntax Description

traffic-generator-name	Specify the name of the traffic generator instance
location *location*	Specify the slot-location of the traffic generator instance

Command Default

None

Command Modes XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines After completing the traffic testing, execute this command to delete the traffic generator instance and free up resources.

Task ID

Task ID	Operation
diag	execute
root-system	execute
root-lr	execute
cisco-support	read, execute

Example

The following example shows how to delete the inbuilt traffic generator instance:

```
Router# diagnostic packet-generator delete t1 location 0/RP0/CPU0
OK
```

diagnostic packet-generator start

To start injecting packets from the inbuilt traffic generator, use the command **diagnostic packet-generator start** in EXEC mode.

diagnostic packet-generator start *traffic-generator-name* **location** *location*

Syntax Description

traffic-generator-name	Specify the name of the traffic generator instance to start packet injection
location *location*	Specify the slot-location of the traffic generator instance

Command Default None

Command Modes XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines

Caution Don't run the inbuilt traffic generator on a live network unless you are fully aware of the impact of packets injected. Injecting packets into a live network may result in network outages.

Task ID

Task ID	Operation
diag	execute
root-system	execute
root-lr	execute
cisco-support	read, execute

Example

The following example shows how to start a previously created traffic generator instance:

```
Router# diagnostic packet-generator start t1 location 0/RP0/CPU0
OK
```

diagnostic packet-generator stop

To stop injecting packets from the inbuilt traffic generator, use the command **diagnostic packet-generator stop** in EXEC mode.

diagnostic packet-generator stop *traffic-generator-name* **location** *location*

Syntax Description

traffic-generator-name	Specify the name of the traffic generator instance to stop packet injection
location *location*	Specify the slot-location of the traffic generator instance

Command Default None

Command Modes XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines None

Task ID

Task ID	Operation
diag	execute
root-system	execute
root-lr	execute
cisco-support	read, execute

Example

The following example shows how to stop injecting packets from the inbuilt traffic generator:

```
Router# diagnostic packet-generator stop t1 location 0/RP0/CPU0
OK
```

show diagnostic packet-generator status

To view the status of the inbuilt traffic generator instance, use the command **show diagnostic packet-generator status** in EXEC mode.

show diagnostic packet-generator status *traffic-generator-name* **location** *location*

Syntax Description

traffic-generator-name	Specify the name of the traffic generator instance or **all**. If you specify **all**, the command displays the summary of all packet-generators, without packet details, in the target location.
location *location*	Specify the slot-location of the traffic generator

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
diag	execute
root-system	execute
root-lr	execute

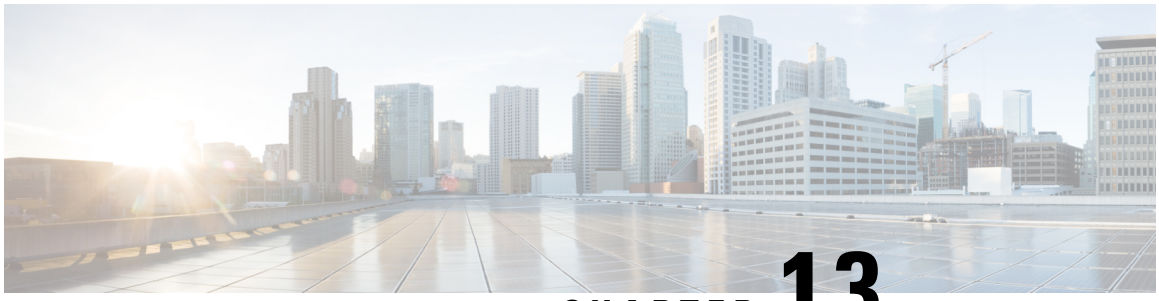
Task ID	Operation
cisco-support	read, execute

Example

The following example shows how to view the status of the traffic generator instance and the packet details:

```
Router# show diagnostic packet-generator status t1 location 0/RP0/CPU0
0/RP0/CPU0:
Name           Run_State    Type    Capture  Set_Rate(pps)  Applied_Rate(pps)  Duration(sec)
  TC  Phy_Interface  NPU  Slice  IFG  Packets        Bytes
==========================================================================================
T1             Running      Ingress True     100            101                60
    0   FH0/0/0/1      0    4      1    209            45144
------------------------------------------------------------------------------------------
Packet Details:
###[ Ethernet ]###
  dst       = 78:bf:d2:07:10:08
  src       = 00:00:00:00:00:01
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 128
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0x446b
     src       = 32.0.0.1
     dst       = 22.0.0.1
     \options   \
###[ UDP ]###
        sport     = domain
        dport     = domain
        len       = 108
        chksum    = 0xc3a5
###[ DNS ]###
           id        = 24929
           qr        = 0
           opcode    = 12
           aa        = 0
           tc        = 0
           rd        = 1
           ra        = 0
           z         = 1
           ad        = 1
           cd        = 0
           rcode     = format-error
           qdcount   = 24929
           ancount   = 24929
           nscount   = 24929
           arcount   = 24929
           qd        = ''
           an        = ''
           ns        = ''
```

```
              ar         = ''
###[ Raw ]###
                  load       =
'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa'
```



CHAPTER 13

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 8000 Series Routers*.

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 7.0.12	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 7.0.12	This command was introduced.
Release 7.0.14	Command options for platform and redundancy infrastructure services and counters were added.

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 7.0.12	This command was introduced.
Release 7.0.14	Health-check for the platform and redundancy infrastructure services and counters were added.

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 7.0.12	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 7.0.12	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 Default value: 10 Range for *drop-tolerance-value*: 0 - 100 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. Default value: 10 Range for *window-size-value*: 5-20 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. Range for *drop-tolerance-value*: 0-1000000 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 24.1.1	**window-size** and **tolerance** keywords are introduced **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
```

INDEX

S

T

V