System Monitoring Command Reference for Cisco NCS 6000 Series Routers

First Published: 2013-09-19

Last Modified: 2017-09-14

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

CHAPTER 3

Preface

The *System Monitoring Command Reference for Cisco NCS 6000 Series Routers* preface contains these sections:

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

Changes to This Document

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

Table 1: Changes to this Document

Data	Change Summary
January 2015	Initial release of the cumulative command reference document that covers all updates from Rel. 4.3.0 onwards.
November 2016	Republished with documentation updates for Release 6.1.2 features.
July 2017	Republished for Release 6.2.2
September 2017	Republished for Release 6.3.1

Communications, Services, and Additional Information

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

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

Cisco Bug Search Tool

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

Alarm Management and Logging Correlation Commands

This module describes the commands used to manage alarms and configure logging correlation rules for system monitoring on the router.

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

For detailed information about alarm management and logging correlation concepts, configuration tasks, and examples, see the *Implementing and Monitoring Alarms and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

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

For system logging concepts, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 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 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# logging suppress rule commit
RP/0/RP0/CPU0:router(config-suppr-rule)# alarm MBGL COMMIT SUCCEEDED
```

Related Commands

Command	Description
logging suppress rule, on page 31	Creates a logging suppression rule.

all-alarms

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

all-alarms

Syntax Description

This command has no keywords or arguments.

Command Default

No alarm types are configured by default.

Command Modes

Logging suppression rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging suppress rule, on page 31	Creates a logging suppression rule.

all-of-router

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

all-of-router

Syntax Description

This command has no keywords or arguments.

Command Default

No scope is configured by default.

Command Modes

Logging suppression apply rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	execute

Examples

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

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

Related Commands

Command	Description
logging suppress apply rule, on page 30	Applies and activates a logging suppression rule.

clear logging correlator delete

To delete all messages or messages specified by a correlation ID from the logging correlator buffer, use the **clear logging correlator delete** command in 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 5.0.0	This command was introduced.

Usage Guidelines

Use the show logging correlator buffer, on page 49 command to confirm that records have been cleared.

Use the logging correlator buffer-size, on page 17 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
```

Related Commands

Command	Description
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.

clear logging events delete

To delete messages from the logging events buffer, use the **clear logging events delete** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

Use the show logging events buffer, on page 56 command to verify that events have been cleared from the logging events buffer.

Use the logging events buffer-size, on page 22 command to configure the capacity of the logging events buffer.

Task ID

Task ID	Operations
logging	execute

Examples

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

```
RP/0/RP0/CPU0:router# clear logging events delete all-in-buffer
```

Related Commands

Command	Description
clear logging events reset, on page 11	Resets bi-state alarms.
show logging events buffer, on page 56	Displays messages in the logging events 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 5.0.0	This command was introduced.

Usage Guidelines

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

Use the show logging events buffer, on page 56 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
```

Related Commands

Command	Description
clear logging events delete, on page 7	Deletes all bi-state alarm messages, or messages specified by correlation ID, from the logging events buffer.
show logging events buffer, on page 56	Displays messages in the logging events buffer.

context-correlation

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

context-correlation
no context-correlation

Syntax Description

This command has no keywords or arguments.

Command Default

Correlation on context is not enabled.

Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

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
```

Related Commands

Command	Description
logging correlator rule, on page 18	Defines the rules for correlating messages.
show logging correlator rule, on page 52	Displays one or more predefined logging correlator rules.

logging correlator apply rule

To apply and activate a correlation rule and enter correlation apply rule configuration mode, use the **logging correlator apply rule** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Use the show logging correlator rule, on page 52 command to show the current apply settings for a given rule.

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

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

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

```
RP/0/RP0/CPU0:router(config)# logging correlator apply rule stateful1
RP/0/RP0/CPU0:router(config-corr-apply-rule)#?

  all-of-router  Apply the rule to all of the router
  clear          Clear the uncommitted configuration
  clear          Clear the configuration
  commit         Commit the configuration changes to running
  context        Apply rule to specified context
  describe       Describe a command without taking real actions
  do             Run an exec command
  exit           Exit from this submode
  location       Apply rule to specified location
  no             Negate a command or set its defaults
  pwd            Commands used to reach current submode
  root           Exit to the XR Config mode
  show           Show contents of configuration
RP/0/RP0/CPU0:router(config-corr-apply-rule)#
```

While in the submode, you can negate keyword options:

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# logging correlator apply rule rule1
RP/0/RP0/CPU0:router(config-corr-apply-rule)# location 0/2/CPU0
```

Related Commands

Command	Description
logging correlator rule, on page 18	Defines the rules for correlating messages.
show logging correlator rule, on page 52	Displays one or more predefined logging correlator rules.
show logging correlator ruleset, on page 54	Displays one or more predefined logging correlator rule sets.

logging correlator apply ruleset

To apply and activate a correlation rule set and enter correlation apply rule set configuration mode, use the **logging correlator apply ruleset** command in 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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Use the show logging correlator ruleset, on page 54 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
```

Related Commands

Command	Description
show logging correlator ruleset, on page 54	Displays one or more predefined logging correlator rule sets.

logging correlator buffer-size

To configure the logging correlator buffer size, use the **logging correlator buffer-size** command in 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 5.0.0	This command was introduced.

Usage Guidelines

The **logging correlator buffer-size** command configures the size of the correlation buffer. This buffer holds all the correlation records as well as the associated correlated messages. When the size of this buffer is exceeded, older correlations in the buffer are replaced with the newer incoming correlations. The criteria that are used to recycle these buffers are:

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

Use the show logging correlator info, on page 51 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 56 **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
```

Related Commands

Command	Description
show logging correlator info, on page 51	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.

logging correlator rule

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

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

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

```
RP/0/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 49 to display messages stored in the logging correlator buffer.

Use the show logging correlator rule, on page 52 command to verify correlation rule settings.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging correlator apply rule, on page 13	Applies and activates correlation rules.
nonrootcause, on page 32	Enters non-root-cause configuration mode and specifies a non-root-cause alarm.
reissue-nonbistate, on page 34	Reissues non-bistate alarm messages (events) from the correlator log after its root-cause alarm clears.
reparent, on page 35	Reparents non-root-cause messages to the next highest active root-cause in a hierarchical correlation when their immediate parent clears.
rootcause, on page 37	Specifies a root-cause message alarm.

Command	Description
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging correlator rule, on page 52	Displays one or more predefined logging correlator rules.
timeout, on page 69	Specifies the collection period duration time for the logging correlator rule message.
timeout-rootcause, on page 71	Specifies an optional parameter for an applied correlation rule.

logging correlator ruleset

To enter correlation rule set configuration mode and define a correlation rule set, use the **logging correlator ruleset** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

To apply a logging correlator rule set, use the logging correlator apply ruleset, on page 15 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
```

Related Commands

Command	Description
logging correlator apply ruleset, on page 15	Applies and activates a correlation rule set and enters correlation apply rule set configuration mode.
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging correlator ruleset, on page 54	Displays defined correlation rule set names.

logging events buffer-size

To configure the size of the logging events buffer, use the **logging events buffer-size** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

Use the show logging events info, on page 60 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
```

Related Commands

Command	Description
logging events level, on page 26	Specifies a severity level for logging alarm messages.
logging events threshold, on page 28	Specifies the event logging buffer capacity threshold that, when surpassed, will generate an alarm.

Command	Description
show logging correlator info, on page 51	Displays information about the size of the logging correlator buffer and available capacity.
show logging events buffer, on page 56	Displays messages in the logging events buffer.
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

logging events display-location

To enable the alarm source location display field for bistate alarms in the output of the **show logging** and **show logging events buffer** command, use the **logging events display-location** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/RP0/CPU0:router# show logging | inc Interface

Wed Aug 13 01:30:58.461 UTC
```

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

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

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

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

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

RP/0/RP0/CPU0:router# show logging | inc Interface

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

Related Commands

Command	Description
show logging events buffer, on page 56	Displays messages in the logging events buffer.

logging events level

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

logging events level *severity*
no logging events level

Syntax Description

severity	Severity level of events to be logged in the logging events buffer, including events of a higher severity level (numerically lower). Table 2: Alarm Severity Levels for Event Logging, on page 26lists 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 5.0.0	This command was introduced.

Usage Guidelines

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

Note Events of lower severity level represent events of higher importance.

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

Table 2: Alarm Severity Levels for Event Logging

Severity Level Keyword	Numeric Value	Logged System Messages
emergencies	0	System is unusable.
alerts	1	Critical system condition exists requiring immediate action.
critical	2	Critical system condition exists.
errors	3	Noncritical errors.
warnings	4	Warning conditions.
notifications	5	Notifications of changes to system configuration.
informational	6	Information about changes to system state.

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# logging events level warnings
```

Related Commands

Command	Description
logging events buffer-size, on page 22	Specifies the logging events buffer size.
logging events threshold, on page 28	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.

logging events threshold

To specify the logging events buffer threshold that, when surpassed, generates an alarm, use the **logging events threshold** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

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

Use the show logging events info, on page 60 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
```

Related Commands

Command	Description
logging events buffer-size, on page 22	Specifies the logging correlator buffer size.
logging events level, on page 26	Specifies a severity level for logging alarm messages.

Command	Description
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

logging suppress apply rule

To apply and activate a logging suppression rule, use the **logging suppress apply rule** command in 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 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
all-of-router, on page 5	Applies a logging suppression rule to suppress alarms originating from all sources on the router.
source, on page 68	Applies a logging suppression rule to alarms originating from a specific node on the router.

logging suppress rule

To create a logging suppression rule and enter the configuration mode for the rule, use the **logging suppress rule** command in the 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 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
alarm, on page 3	Specifies a type of alarm to be suppressed by a logging suppression rule.
all-alarms, on page 4	Configures a logging suppression rule to suppress all types of alarms.

nonrootcause

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

nonrootcause alarm *msg-category group-name msg-code*
no nonrootcause

Syntax Description

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 5.0.0	This command was introduced.

Usage Guidelines

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

Use the show logging events info, on page 60 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
```

```
RP/0/RP0/CPU0:router(config-corr-rule-st-nonrc)# ?
  alarm     Specify non-root cause alarm: Category/Group/Code combos
  clear     Clear the uncommitted configuration
  clear     Clear the configuration
  commit    Commit the configuration changes to running
  describe  Describe a command without taking real actions
  do        Run an exec command
  exit      Exit from this submode
  no        Negate a command or set its defaults
  pwd       Commands used to reach current submode
  root      Exit to the XR Config mode
  show      Show contents of configuration
```

Related Commands

Command	Description
logging events buffer-size, on page 22	Specifies the logging correlator buffer size.
logging events level, on page 26	Specifies a severity level for logging alarm messages.
logging events threshold, on page 28	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

reissue-nonbistate

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

reissue-nonbistate
no reissue-nonbistate

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to reissue nonbistate alarm messages:

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

Related Commands

Command	Description
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging events buffer, on page 56	Displays messages in the logging events buffer.

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 5.0.0	This command was introduced.

Usage Guidelines

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

Rule 1 with rootcause A and non-rootcause B

Rule 2 with rootcause B and non-rootcause C

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

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

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging correlator rule, on page 18	Defines the rules for correlating messages.
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

rootcause

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

rootcause *msg-category* *group-name* *msg-code*
no **rootcause**

Syntax Description

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 5.0.0	This command was introduced.

Usage Guidelines

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

Use the show logging events info, on page 60 command to display the root-cause and non-root-cause alarms for a correlation rule.

Task ID

Task ID	Operations
logging	read, write

Related Commands

Command	Description
logging events buffer-size, on page 22	Specifies the logging correlator buffer size.
logging events level, on page 26	Specifies a severity level for logging alarm messages.
logging events threshold, on page 28	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
timeout-rootcause, on page 71	Specifies an optional parameter for an applied correlation rule.

Command	Description
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

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 44 to view the router alarms in brief.

Use the show alarms detail, on page 46 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 44	Displays router alarms in brief.

Command	Description
show alarms detail, on page 46	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 39	Displays router alarms in brief and detail.
show alarms detail, on page 46	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 39	Displays router alarms in brief and detail.
show alarms brief, on page 44	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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
logging	read

Examples

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

```
RP/0/RP0/CPU0:router# show logging correlator buffer all-in-buffer

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

This table describes the significant fields shown in the display.

Table 3: show logging correlator buffer Field Descriptions

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

Related Commands

Command	Description
show logging correlator info, on page 51	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
show logging correlator rule, on page 52	Displays one or more predefined logging correlator rules.

show logging correlator info

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

show logging correlator info

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the logging correlator buffer-size, on page 17 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
```

Related Commands

Command	Description
logging correlator buffer-size, on page 17	Specifies the logging correlator buffer size.
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging correlator rule, on page 52	Displays one or more predefined logging correlator rules.

show logging correlator rule

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
logging	read

Related Commands

Command	Description
logging correlator apply rule, on page 13	Applies and activates correlation rules.
logging correlator rule, on page 18	Defines the rules for correlating messages.
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging correlator info, on page 51	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages

show logging correlator ruleset

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
logging	read

Examples

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

```
RP/0/RP0/CPU0:router# show logging correlator RuleSetOne RuleSetTwo

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

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

```
RP/0/RP0/CPU0:router# show logging correlator ruleset all
```

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

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

```
RP/0/RP0/CPU0:router# show logging correlator ruleset all summary
RuleSetOne
RuleSetTwo
RuleSetThree
```

This table describes the significant fields shown in the display.

Table 4: show logging correlator ruleset Field Descriptions

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

Related Commands

Command	Description
logging correlator apply rule, on page 13	Applies and activates correlation rules.
logging correlator rule, on page 18	Defines the rules for correlating messages.
show logging correlator buffer, on page 49	Displays messages in the logging correlator buffer.
show logging correlator info, on page 51	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
show logging correlator rule, on page 52	Displays defined correlation rules.

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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read

Examples

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

```
RP/0/RP0/CPU0:router# show logging events buffer all-in-buffer

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

#1     :    :RP/0//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//CPU0:Jan  9 08:58:21 2004:psarb[238]: %PLATFORM-PSARB-5-GO_BID : Card
 is going to bid state.
#3     :    :RP/0//CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-5-GO_ACTIVE : Card
 is becoming active.
#4     :    :RP/0//CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-6-RESET_ALL_LC_
CARDS : RP going active; resetting all linecards in chassis
#5     :    :RP/0//CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-GO_ACTIVE : this
card going active
#6     :    :RP/0//CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-FAILOVER_ENABLED :
Failover has been enabled by config
```

This table describes the significant fields shown in the display.

Table 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.

Related Commands

Command	Description
show logging events info, on page 60	Displays configuration and operational messages about the logging events buffer.

show logging events info

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

show logging events info

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read

Examples

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

```
RP/0/RP0/CPU0:router# show logging events info

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

This table describes the significant fields shown in the display.

Table 6: show logging events info Field Descriptions

Field	Description
Size (Current/Max)	The current and maximum size of the logging events buffer. The maximum size of the buffer is controlled by the logging events buffer-size, on page 22 command.
#Records	The number of event records stored in the logging events buffer.
Thresh	The configured logging events threshold value. This field is controlled by the logging events threshold, on page 28 command.
Filter	The lowest severity level for events that will be displayed. This field is controlled by the logging events level, on page 26 command.

Related Commands

Command	Description
logging events buffer-size, on page 22	Specifies the logging correlator buffer size.
logging events level, on page 26	Specifies a severity level for logging alarm messages.
logging events threshold, on page 28	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
show logging events buffer, on page 56	Displays information about messages in the logging events buffer according to type, time, or severity level.

show logging suppress rule

To display defined logging suppression rules, use the **show logging suppression rule** command in 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	read

Examples

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

```
RP/0/RP0/CPU0:router# show logging suppression rule test_suppression

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

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

Number of suppressed alarms : 0
```

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

```
RP/0/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
```

Related Commands

Command	Description
logging suppress apply rule, on page 30	Applies and activates a logging suppression rule.
logging suppress rule, on page 31	Creates a logging suppression rule.

show snmp correlator buffer

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read

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

```
RP/0/RP0/CPU0:router# show snmp correlator buffer correlationID 10
    Correlation ID : 10
    Rule : ospf-trap-rule
    Rootcause: 1.3.6.1.6.3.1.1.5.3
    Time : Dec 14 02:32:05
    Varbind(s):
       ifIndex.17 = 17
       ifDescr.17 = hundredGigE0/1/0/8
       ifType.17 = other(1)
       cieIfStateChangeReason.17 = down

        Nonroot : 1.3.6.1.2.1.14.16.2.2
        Time: Dec 14 02:32:04
        Varbind(s):
           ospfRouterId = 10.1.1.1
           ospfNbrIpAddr = 10.0.28.2
           ospfNbrAddressLessIndex = 0
           ospfNbrRtrId = 10.3.3.3
           ospfNbrState = down(1)
```

show snmp correlator info

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

show snmp correlator info

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read

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

```
RP/0/RP0/CPU0:router# show snmp correlator info

  Buffer-Size     Percentage-Occupied
      85720                  0.00
```

show snmp correlator rule

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read

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

```
RP/0/RP0/CPU0:router# show snmp correlator rule rule_1
Rule Name : rule_1
    Time out  : 888                 Rule State: RULE_APPLIED_ALL
          Root:  OID   : 1.3.6.1.2.1.11.0.2
                 vbind : 1.3.6.1.2.1.2.2.1.2 value /3\.3\.\d{1,3}\.\d{1,3}/
                 vbind : 1.3.6.1.2.1.5.8.3   index val
       Nonroot:  OID   : 1.3.6.1.2.1.11.3.3
```

show snmp correlator ruleset

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read

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

```
RP/0/RP0/CPU0:router# show snmp correlator ruleset test
 Rule Set Name :   test
   Rules: chris1                          : Not Applied
          chris2                          : Applied
```

source

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

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

Syntax Description

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

Command Default

No scope is configured by default.

Command Modes

Logging suppression apply rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
logging	execute

Examples

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

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

Related Commands

Command	Description
logging suppress apply rule, on page 30	Applies and activates a logging suppression rule.

timeout

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

timeout [*milliseconds*]
no timeout

Syntax Description

milliseconds	Range is 1 to 600000 milliseconds.

Command Default

Timeout period is not specified.

Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging correlator rule, on page 18	Defines the rules by which the correlator logs messages to the logging events buffer.
timeout-rootcause, on page 71	Specifies an optional parameter for an applied correlation rule.

timeout-rootcause

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

timeout-rootcause [*milliseconds*]
no timeout-rootcause

Syntax Description

milliseconds	Range is 1 to 7200000 milliseconds.

Command Default

Root-cause alarm timeout period is not specified.

Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

  When the root-cause message arrives before the root-cause timeout expires, then the correlation continues as normal using the remainder of the main rule timeout.
- When the root-cause message is not received before the root-cause timeout expires, then all the non-root-cause messages held during the root-cause timeout period are sent to syslog and the correlation is terminated.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging correlator rule, on page 18	Defines the rules by which the correlator logs messages to the logging events buffer.

Embedded Event Manager Commands

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

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

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

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

For detailed information about the EEM concepts, configuration tasks, and examples, see the *Configuring and Managing Embedded Event Manager Policies* module in *System Monitoring Configuration Guide for Cisco NCS 6000 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 5.0.0	This command was introduced.

Usage Guidelines

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

User Library

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

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

User Policy

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

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

Task ID

Task ID	Operations
eem	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# event manager directory user library disk0:/usr/lib/tcl
```

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

```
RP/0/RP0/CPU0:router(config)# event manager directory user policy disk0:/usr/fm_policies
```

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.
show event manager directory user, on page 85	Displays the directory name for storing user library and policy files.

event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Use the show event manager environment, on page 86 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
```

Related Commands

Command	Description
show event manager environment, on page 86	Displays the name and value for all the EEM environment variables.

event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in 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	(Optional) Specifies the type of policy.
system	(Optional) Registers a system policy defined by Cisco.
user	(Optional) Registers a user-defined policy.

Command Default

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

Command Modes

XR Config mode

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Note AAA authorization (such as the **aaa authorization** command with the **eventmanager** and **default** keywords) must be configured before the EEM policies can be registered. The **eventmanager** and **default** keywords must be configured for policy registration. See the *Configuring AAA Services on* module of *System Security Configuration Guide for Cisco NCS 6000 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 81 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
```

Related Commands

Command	Description
event manager environment, on page 76	Specifies a directory for storing user library files.
event manager refresh-time, on page 81	Specifies the time between the system attempts to contact the AAA server and refresh the username reauthentication.
show event manager environment, on page 86	Displays the name and value for all EEM environment variables.
show event manager policy available, on page 93	Displays EEM policies that are available to be registered.
show event manager policy registered, on page 95	Displays the EEM policies that are already registered.

event manager refresh-time

To define the time between user authentication refreshes in Embedded Event Manager (EEM), use the **event manager refresh-time** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
eem	read, write

Examples

This example shows how to set the refresh time:

```
RP/0/RP0/CPU0:router(config)# event manager refresh-time 1900
```

event manager run

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

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

Syntax Description

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

Command Default

No registered EEM policies are run.

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Use the event manager policy, on page 78 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//CPU0:Sep 20 10:26:31.169 : user-plocy.tcl[65724]: The reqinfo of arg2 is parameter2.

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

RP/0//CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_type_string
is none.
RP/0//CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_pub_sec is
1190283990.
```

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

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

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.

event manager scheduler suspend

To suspend the Embedded Event Manager (EEM) policy scheduling execution immediately, use the **event manager scheduler suspend** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
eem	read, write

Examples

This example shows how to disable policy scheduling:

```
RP/0/RP0/CPU0:router(config)# event manager scheduler suspend
```

This example shows how to enable policy scheduling:

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

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.

show event manager directory user

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager directory user library
disk0:/fm_user_lib_dir

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

Related Commands

Command	Description
event manager directory user, on page 74	Specifies the name of a directory that is to be used for storing either the user library or the policy files.

show event manager environment

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager environment

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

This table describes the significant fields in the display.

Table 7: show event manager environment Field Descriptions

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

Related Commands

Command	Description
event manager environment, on page 76	Specifies a directory to use for storing user library files.

show event manager metric hardware

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager metric hardware location 0/RP0/CPU0

=====================================

node: 0/RP0/CPU0

Most recent online: Mon Sep 10 21:45:02 2007
Number of times online: 1
Cumulative time online: 0 days, 09:01:07

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

This table describes the significant fields shown in the display.

Table 8: show event manager metric hardware location Field Descriptions

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

Related Commands

Command	Description
show processes	Displays information about active processes.

show event manager metric process

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

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

Syntax Description

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

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager metric process all location all

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

most recent 10 process end times and types:

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

most recent 10 process end times and types:

cumulative process available time: 21 hours 1 minutes 31 seconds 41 milliseconds
cumulative process unavailable time: 0 hours 0 minutes 0 seconds 0 milliseconds
process availability:  1.000000000
number of abnormal ends within the past 60 minutes (since reload): 0
number of abnormal ends within the past 24 hours (since reload): 0
number of abnormal ends within the past 30 days (since reload): 0
```

This table describes the significant fields shown in the display.

Table 9: show event manager metric process Field Descriptions

Field	Description
job id	Number assigned as the job identifier.
node name	Node with the process running.
process name	Name of the process running on the node.
instance	Instance or thread of a multithreaded process.
comp id	Component of which the process is a member.
version	Specific software version or release of which the process is a member.
last event type	Last event type on the node.

Field	Description
recent end type	Most recent end type.
recent start time	Last time the process was started.
recent normal end time	Last time the process was stopped normally.
recent abnormal end time	Last time the process was terminated abnormally.
recent abnormal end type	Reason for the last abnormal process termination. For example, the process was terminated or crashed.
number of times started	Number of times the process has been started.
number of times ended normally	Number of times the process has been stopped normally.
number of times ended abnormally	Number of times the process has stopped abnormally.
most recent 10 process start times	Times of the last ten process starts.
cumulative process available time	Total time the process has been available.
cumulative process unavailable time	Total time the process has been out of service due to a restart, termination, communication problems, and so on.
process availability	Uptime percentage of the process (time running—the duration of any outage).
number of abnormal ends within the past 60 minutes	Number of times the process has stopped abnormally within the last 60 minutes.
number of abnormal ends within the past 24 hours	Number of times the process has stopped abnormally within the last 24 hours.
number of abnormal ends within the past 30 days	Number of times the process has stopped abnormally within the last 30 days.

Related Commands

Command	Description
show processes	Displays information about active processes.

show event manager policy available

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager policy available

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

This table describes the significant fields shown in the display.

Table 10: show event manager policy available Field Descriptions

Field	Description
No.	Number of the policy.

Field	Description
Type	Type of policy.
Time Created	Time the policy was created.
Name	Name of the policy.

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.
show event manager policy registered, on page 95	Displays the EEM policies that are already registered.

show event manager policy registered

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager policy registered

No.       Type    Event Type          Time Registered               Name
1         system  proc abort          Wed Jan 16 23:44:56 2004      test1.tcl
 version 00.00.0000 instance 1 path {cdp}
 priority normal maxrun_sec 20 maxrun_nsec 0
2         system  timer cron          Wed Jan 16 23:44:58 2004      test2.tcl
 name {crontimer1}
 priority normal maxrun_sec 20 maxrun_nsec 0
3         system  proc abort          Wed Jan 16 23:45:02 2004      test3.tcl
 path {cdp}
 priority normal maxrun_sec 20 maxrun_nsec 0
4         system  syslog              Wed Jan 16 23:45:41 2004      test4.tcl
 occurs 1 pattern {test_pattern}
 priority normal maxrun_sec 90 maxrun_nsec 0
5         system  timer cron          Wed Jan 16 23:45:12 2004      test5.tcl
 name {crontimer2}
 priority normal maxrun_sec 30 maxrun_nsec 0
6         system  wdsysmon            Wed Jan 16 23:45:15 2004      test6.tcl
 timewin_sec 120 timewin_nsec 0 sub1 mem_tot_used {node {localhost} op gt
 val 23000}
 priority normal maxrun_sec 40 maxrun_nsec 0
7         system  wdsysmon            Wed Jan 16 23:45:19 2004      test7.tcl
 timewin_sec 120 timewin_nsec 0 sub1 mem_proc {node {localhost} procname
 {wdsysmon} op gt val 80 is_percent FALSE}
 priority normal maxrun_sec 40 maxrun_nsec 0
```

This table describes the significant fields displayed in the example.

Table 11: show event manager policy registered Field Descriptions

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

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.

show event manager refresh-time

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

show event manager refresh-time

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
eem	read

Examples

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

```
RP/0/RP0/CPU0:router# show event manager refresh-time
Output:
1800 seconds
```

Related Commands

Command	Description
event manager refresh-time, on page 81	Specifies the time between the system attempts to contact the AAA server, and refreshes the username reauthentication.

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 History

Release	Modification
Release 5.0.0	This command was introduced.

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 12: 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.

Related Commands

Command	Description
event manager policy, on page 78	Registers an EEM policy with the EEM.

IP Service Level Agreement Commands

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

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

For detailed information about IP SLA concepts, configuration tasks, and examples, see the *Implementing IP Service Level Agreements* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

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

Command History

Release	Modification
Release 5.2.3	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.

If the **action** command is used in IP SLA operation mode, the action defined applies to the specific operation being configured.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold, on page 159	Sets the lower-limit and upper-limit values.
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

ageout

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

ageout *seconds*
no ageout

Syntax Description

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

Command Default

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

Command Modes

IP SLA schedule configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

buckets (statistics hourly)

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

buckets *hours*
no buckets

Syntax Description

hours	Number of hours for which statistics are maintained for the IP SLA operations. Range is 0 to 25 in IP SLA operation statistics configuration mode.

Command Default

The default value is 2.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
statistics, on page 156	Sets the statistics collection parameters for the operation.

buckets (statistics interval)

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

buckets *bucket-size*
no buckets

Syntax Description

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

Command Default

The default value is 100.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

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

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# buckets 50
```

Related Commands

Command	Description
statistics, on page 156	Sets the statistics collection parameters for the operation.

control disable

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

control disable
no control disable

Syntax Description

This command has no keywords or arguments.

Command Default

Control packets are enabled by default.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	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 is required on the remote device.

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

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

datasize request

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

datasize request *size*
no datasize request

Syntax Description

size	Specifies the following ranges and default values that are protocol dependent: • For a UDP jitter operation, range is 28 to 1500 B.

Command Default

For a UDP jitter operation, the default value is 32 B.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
type udp jitter, on page 172	Configures an IP SLA UDP jitter operation.

destination address (IP SLA)

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

destination address *ipv4-address*
no destination address

Syntax Description

ipv4-address	IP address of the target device.

Command Default

None

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

destination port

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

destination port *port*
no destination port

Syntax Description

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

Command Default

None

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

The **destination port** command 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 IP SLA UDP jitter configurations.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

distribution count

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

distribution count *slot*
no distribution count

Syntax Description

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

Command Default

The default value is 1.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# distribution count 15
```

Related Commands

Command	Description
buckets (statistics hourly), on page 106	Sets the number of hours in which statistics are kept.
distribution interval, on page 114	Sets the time interval (in milliseconds) for each statistical distribution.

Command	Description
statistics, on page 156	Sets the statistics collection parameters for the operation.

distribution interval

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

distribution interval *interval*
no distribution interval

Syntax Description

interval	Number of milliseconds used for each statistics distribution that is kept. Range is 1 to 100. Default is 20.

Command Default

The default value is 20.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
buckets (statistics hourly), on page 106	Sets the number of hours in which statistics are kept.
distribution count, on page 112	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
statistics, on page 156	Sets the statistics collection parameters for the operation.

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.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# frequency 300
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

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 History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
key-chain, on page 118	Configures MD5 authentication for IP SLA control messages.
low-memory, on page 120	Configures a low-water memory mark.
operation, on page 121	Configures an IP SLA operation.
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
reaction trigger, on page 129	Defines a second IP SLA operation to make the transition from a pending state to an active state when one of the trigger-type options is defined with the **reaction operation** command.
responder, on page 130	Enables the IP SLA responder for UDP jitter operations.

Command	Description
schedule operation, on page 132	Schedules an IP SLA operation.

key-chain

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

key-chain *key-chain-name*
no key-chain

Syntax Description

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 5.2.3	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

life

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

life {**forever**}
no life

Syntax Description

forever	Schedules the operation to run indefinitely.

Command Default

None

Command Modes

IP SLA schedule configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

low-memory

low-memory *value*
no low-memory

Syntax Description

value	Low-memory watermark value. Range is 0 to 4294967295.

Command Default

The default value is 20 MB (free memory).

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# low-memory 102400
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
show ipsla application, on page 134	Displays the information for the IP SLA application.

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 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
schedule operation, on page 132	Schedules an IP SLA operation.

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.

Command Default

The default packet count is 10.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
packet interval, on page 123	Specifies the interval between packets.

packet interval

To specify the interval between packets, use the **packet interval** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

packet interval *interval*
no packet interval

Syntax Description

interval	Interpacket interval in milliseconds. Range is 10 to 60000 (in milliseconds).

Command Default

The default packet interval is 20 ms.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
packet count, on page 122	Specifies the number of packets that are to be transmitted during a probe.

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

Command History

Release	Modification
Release 5.2.3	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.

This table lists the Supported Reaction Configuration, by IP SLA Operation.

Table 13: Supported Reaction Configuration, by IP SLA Operation

Operation	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	ICMP Path Jitter	MPLS LSP Ping	MPLS LSP Trace
Failure	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y
RTTAvg	--	--	--	--	--	--	--
Timeout	Y	Y	Y	Y	Y	Y	Y
connectionLoss	--	--	Y	Y	--	Y	Y
verifyError	--	--	Y	Y	--	--	--
jitterSDAvg	--	--	Y	--	--	--	--
jitterDSAvg	--	--	Y	--	--	--	--
jitterAvg	--	--	Y	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--
PacketLoss	--	--	Y	--	--	--	--

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react rtt
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react timeout
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react verify-error
RP/0/RP0/CPU0:router(config-ipsla-react-cond)#
```

Related Commands

Command	Description
action (IP SLA), on page 103	Specifies what action or combination of actions the operation performs when you configure the **react** command or when threshold events occur.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
threshold, on page 159	Sets the lower-limit and upper-limit values.

Command	Description
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

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 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

reaction trigger

To define a second IP SLA operation to make the transition from a pending state to an active state when one of the trigger-type options is defined with the **reaction operation** command, use the **reaction trigger** command in IP SLA configuration mode. To remove the reaction trigger when the *triggering-operation* argument does not trigger any other operation, use the **no** form of this command.

reaction trigger *triggering-operation triggered-operation*
no reaction trigger *triggering-operation triggered-operation*

Syntax Description

triggering-operation	Operation that contains a configured action-type trigger and can generate reaction events. Range is 1 to 2048.
triggered-operation	Operation that is started when the *triggering-operation* argument generates a trigger reaction event. Range is 1 to 2048.

Command Default

No triggered operation is configured.

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

Both the *triggering-operation* and *triggered-operation* arguments must be configured. The triggered operation must be in the pending state.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction trigger 1 2
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

responder

To enable the IP SLA responder for UDP jitter operations, use the **responder** command in IP SLA configuration mode. To disable the responder, use the **no** form of this command.

responder
no responder

Syntax Description

This command has no keywords or arguments.

Command Default

The IP SLA **responder** command is disabled.

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

An IP address and port are configured and identified as a permanent port (for example, a port to which the responder is permanently listening). If no IP address and port are configured, the responder handles only dynamic ports (for example, ports that are listened to when requested by a remote operation).

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enable the IP SLA responder:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# responder
RP/0/RP0/CPU0:router(config-ipsla-resp)#
```

Related Commands

Command	Description
type udp ipv4 address, on page 173	Configures a permanent port in the IP SLA Responder for UDP jitter operations.

recurring

To indicate that the operation starts automatically at the specified time and for the specified duration every day, use the **recurring** command in IP SLA schedule configuration mode. To not start the operation everyday, use the **no** form of this command.

recurring
no recurring

Syntax Description

This command has no keywords or arguments.

Command Default

Recurring is disabled.

Command Modes

IP SLA schedule configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

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 5.2.3	This command was introduced.

Usage Guidelines

The **schedule operation** command enters the IP SLA schedule configuration mode. You can configure more schedule configuration parameters to schedule the operation. When an operation is scheduled, it continues collecting information until the configured life expires.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
ageout, on page 105	Specifies the number of seconds to keep the operation in memory when it is not actively collecting information.
operation, on page 121	Configures an IP SLA operation.
life, on page 119	Specifies the length of time to execute.

Command	Description
recurring, on page 131	Indicates that the operation starts automatically at the specified time and for the specified duration every day.
start-time , on page 154	Determines the time when the operation starts.

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 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

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

```
RP/0/RP0/CPU0:router#show ipsla application

Estimated system max number of entries: 2048
Number of Entries configured: 143
Number of active Entries : 111
Number of pending Entries : 0
Number of inactive Entries : 32

Supported Operation Types: 1

        Type of Operation: UDP JITTER

Number of configurable probes : 1905
SA Agent low memory water mark: 20480 (KB)
```

This table describes the significant fields shown in the display.

Table 14: show ipsla application Field Descriptions

Field	Description
Estimated system max number of entries	Maximum number of operations that are configured in the system. The low-memory configured parameter and the available memory in the system are given.

Field	Description
Number of Entries configured	Total number of entries that are configured, such as active state, pending state, and inactive state.
Number of active Entries	Number of entries that are in the active state. The active entries are scheduled and have already started a life period.
Number of pending Entries	Number of entries that are in pending state. The pending entries have a start-time scheduled in the future. These entries either have not started the first life, or the entries are configured as recurring and completed one of its life.
Number of inactive Entries	Number of entries that are in the inactive state. The inactive entries do not have a start-time scheduled. Either the start-time has never been scheduled or life has expired. In addition, the entries are not configured as recurring.
Supported Operation Types	Types of operations that are supported by the system.
Number of configurable probes	Number of remaining entries that can be configured. The number is just an estimated value and it may vary over time according to the available resources.
SA Agent low memory water mark	Available memory for the minimum system below which the IP SLA feature does not configure any more operations.

Related Commands

Command	Description
low-memory, on page 120	Configures a low-water memory mark.
operation, on page 121	Configures an IP SLA operation.

show ipsla history

To display the history collected for all IP SLA operations or for a specified operation, use the **show ipsla history** command in XR EXEC mode.

show ipsla history [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLA operation.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

By default, history statistics are not collected. To have any data displayed by using the **show ipsla history** command, you must configure the history collection.

This table lists the response return values that are used in the **show ipsla history** command.

Table 15: Response Return Values for the show ipsla history Command

Code	Description
1	Okay
2	Disconnected
3	Over Threshold
4	Timeout
5	Busy
6	Not Connected
7	Dropped
8	Sequence Error
9	Verify Error
10	Application Specific

If the default tabular format is used, the response return description is displayed as code in the Sense column. The Sense field is always used as a return code.

Task ID

Task ID	Operations
monitor	read

Examples

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

```
RP/0/RP0/CPU0:router# show ipsla history 1

Point by point History
Multiple Lines per Entry
Line 1:
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = RTT (milliseconds)
Sense   = Response return code
Line 2 has the Target Address
Entry LifeI       BucketI    SampleI    SampleT        CompT       Sense      TargetAddr
1     0           0          0          1134419252539  9           1          192.0.2.6
1     0           1          0          1134419312509  6           1          192.0.2.6
1     0           2          0          1134419372510  6           1          192.0.2.6
1     0           3          0          1134419432510  5           1          192.0.2.6
```

This table describes the significant fields shown in the display.

Table 16: show ipsla history Field Descriptions

Field	Description
Entry number	Entry number.
LifeI	Life index.
BucketI	Bucket index.
SampleI	Sample index.
SampleT	Sample start time.
CompT	Completion time in milliseconds.
Sense	Response return code.
TargetAddr	IP address of intermediate hop device or destination device.

Related Commands

Command	Description
show ipsla statistics aggregated, on page 143	Displays the statistical errors for all the IP SLA operations or for a specified operation.

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 5.2.3	This command was introduced.

Usage Guidelines

The output of the **show ipsla responder statistics port** command is available only for specific intervals of time in which only nonpermanent ports are being used at the responder. The reason is that the responder closes the nonpermanent ports after each operation cycle. However, if both permanent and nonpermanent ports are used, the output always contains rows for the permanent ports. The rows for the nonpermanent ports are displayed only if those nonpermanent ports are enabled at the instant the command is issued.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla responder statistics port** command:

```
RP/0/RP0/CPU0:router# show ipsla responder statistics all port

Port Statistics
---------------

Local Address  Port   Port Type   Probes   Drops   CtrlProbes   Discard
172.16.5.1     3001   Permanent   0        0       0
172.16.5.1     10001  Permanent   728160   0       24272
172.16.5.5     8201   Dynamic     12132    0       12135        ON
172.16.5.1     4441   Dynamic     207216   0       3641         ON
```

This table describes the significant fields shown in the display.

Table 17: 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 5.2.3	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 UDP jitter operation:

```
RP/0/RP0/CPU0:router# show ipsla statistics

Entry number: 101
    Modification time: 16:39:36.608 GMT Fri Nov 28 2014
    Start time       : 16:39:36.633 GMT Fri Nov 28 2014
    Number of operations attempted: 10
    Number of operations skipped  : 0
    Current seconds left in Life  : Forever
    Operational state of entry    : Active
    Operational frequency(seconds): 60
    Connection loss occurred      : FALSE
    Timeout occurred              : FALSE
    Latest RTT (milliseconds)     : 3
    Latest operation start time   : 16:48:37.653 GMT Fri Nov 28 2014
    Next operation start time     : 16:49:37.653 GMT Fri Nov 28 2014
    Latest operation return code  : OK
    RTT Values:
      RTTAvg  : 3          RTTMin: 3          RTTMax : 4
      NumOfRTT: 10         RTTSum: 33         RTTSum2: 111
    Packet Loss Values:
      PacketLossSD       : 0          PacketLossDS : 0
      PacketOutOfSequence: 0          PacketMIA    : 0
      PacketLateArrival  : 0          PacketSkipped: 0
      Errors             : 0          Busies       : 0
      InvalidTimestamp   : 0
    Jitter Values :
      MinOfPositivesSD: 1          MaxOfPositivesSD: 1
      NumOfPositivesSD: 2          SumOfPositivesSD: 2
      Sum2PositivesSD : 2
      MinOfNegativesSD: 1          MaxOfNegativesSD: 1
      NumOfNegativesSD: 1          SumOfNegativesSD: 1
      Sum2NegativesSD : 1
      MinOfPositivesDS: 1          MaxOfPositivesDS: 1
      NumOfPositivesDS: 1          SumOfPositivesDS: 1
      Sum2PositivesDS : 1
      MinOfNegativesDS: 1          MaxOfNegativesDS: 1
      NumOfNegativesDS: 1          SumOfNegativesDS: 1
      Sum2NegativesDS : 1
      JitterAve: 1         JitterSDAve: 1      JitterDSAve: 1
      Interarrival jitterout: 0             Interarrival jitterin: 0
    One Way Values :
      NumOfOW: 0
      OWMinSD : 0          OWMaxSD: 0          OWSumSD: 0
      OWSum2SD: 0          OWAveSD: 0
      OWMinDS : 0          OWMaxDS: 0          OWSumDS: 0
      OWSum2DS: 0          OWAveDS: 0
```

This table describes the significant fields shown in the display.

Table 18: show ipsla statistics Field Descriptions

Field	Description
Entry number	Entry number.
Modification time	Latest time the operation was modified.
Start time	Time the operation was started.
Number of operations attempted	Number of operation cycles that were issued.
Number of operations skipped	Number of operation cycles that were not issued because one of the cycles extended over the configured time interval.
Current seconds left in Life	Time remaining until the operation stops execution.
Operational state of entry	State of the operation, such as active state, pending state, or inactive state.
Connection loss occurred	Whether or not a connection-loss error happened.
Timeout occurred	Whether or not a timeout error happened.
Latest RTT (milliseconds)	Value of the latest RTT sample.
Latest operation start time	Time the latest operation cycle was issued.
Latest operation return code	Return code of the latest operation cycle
RTTAvg	Average RTT value that is observed in the last cycle.
RTTMin	Minimum RTT value that is observed in the last cycle.

Field	Description
RTTMax	Maximum RTT value that is observed in the last cycle.
NumOfRTT	Number of successful round trips.
RTTSum	Sum of all successful round-trip values in milliseconds.
RTTSum2	Sum of squares of the round-trip values in milliseconds.
Path Idx	Path index number.
Path Sense	Response return code for the path. (See Table 15: Response Return Values for the show ipsla history Command, on page 136, in **show ipsla history** command.)
Outgoing Interface	Outgoing interface of the path.
Nexthop Address	Next hop address of the path.

Related Commands

Command	Description
show ipsla statistics aggregated, on page 143	Displays the statistical errors for all the IP SLA operations or for a specified operation.

show ipsla statistics aggregated

To display the hourly statistics for all the IP SLA operations or specified operation, use the **show ipsla statistics aggregated** command in XR EXEC mode.

show ipsla statistics aggregated [**detail**] [*operation-number*]

Syntax Description

detail	Displays detailed information.
operation-number	(Optional) Number of IP SLA operations. Range is 1 to 2048.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 5.2.3	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 following sample output is from the **show ipsla statistics aggregated** command in which operation 10 is a UDP jitter operation:

```
RP/0/RP0/CPU0:router# show ipsla statistics aggregated

        Captured Statistics
        Each Entry per Line
Column Description per Entry:
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)
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
101   1417192777884 1   1   0   0          0          0             0           0
 0
101   1417192777884 1   1   1   0          0          0             0           0
 0
101   1417192777884 1   1   2   2          58         0             176         4
 1
101   1417192777884 1   1   3   8          258        0             852         5
 2
101   1417192777884 1   1   4   0          0          0             0           0
 0
```

This table describes the significant fields shown in the display.

Table 19: show ipsla statistics aggregated Field Descriptions

Field	Description
Busies	Number of times that the operation cannot be started because the previously scheduled run was not finished.
Entry Number	Entry number.
Hop in Path Index	Hop in path index.
Errors	Number of internal errors.
Jitter Values	Jitter statistics appear on the specified lines. Jitter is defined as interpacket delay variance.
NumOfJitterSamples	Number of jitter samples that are collected. The number of samples are used to calculate the jitter statistics.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
SumOfNegativesSD	Sum of the negative jitter values from the source to the destination.
Sum2PositivesDS	Sum of squares of the positive jitter values from the destination to the source.
Sum2PositivesSD	Sum of squares of the positive jitter values from the source to the destination.
Sum2NegativesDS	Sum of squares of the negative jitter values from the destination to the source.
Sum2NegativesSD	Sum of squares of the negative jitter values from the source to the destination.
Target Address	Target IP address.

The output of the **show ipsla statistics aggregated detail** command varies depending on operation type. The following sample output is from the **show ipsla statistics aggregated detail** command in tabular format, when the output is split over multiple lines:

```
RP/0/RP0/CPU0:router# show ipsla statistics aggregated detail 2

Captured Statistics
        Multiple Lines per Entry
Line1:
Entry    = Entry number
StartT   = Start time of entry (hundredths of seconds)
Pth      = Path index
Hop      = Hop in path index
Dst      = Time distribution index
Comps    = Operations completed
SumCmp   = Sum of RTT (milliseconds)

Line2:
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry StartT        Pth Hop Dst Comps      SumCmp
      SumCmp2H      SumCmp2L    TMax       TMin
2     1134423910701 1   1   0   12         367
      0             1231        6          6
2     1134423851116 1   1   1   2          129
      0             2419        41         41
2     1134423070733 1   1   2   1          101
      0             1119        16         16
2     0             1   1   3   0          0
      0             0           0          0
```

This table describes the significant fields shown in the display.

Table 20: show ipsla statistics aggregated detail Field Descriptions

Field	Description
Entry	Entry number.

Field	Description
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.

Related Commands

Command	Description
show ipsla statistics, on page 140	Displays the operational data for the IP SLA operation.
show ipsla statistics enhanced aggregated, on page 149	Displays the statistical errors for all the IP SLA operations or for a specified operation.

show ipsla statistics enhanced aggregated

To display the enhanced history statistics for all collected enhanced history buckets for the specified IP SLA operation, use the **show ipsla statistics enhanced aggregated** command in XR EXEC mode.

show ipsla statistics enhanced aggregated [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Operation number for which to display the enhanced history distribution statistics.
interval *seconds*	(Optional) Specifies the aggregation interval in seconds for which to display the enhanced history distribution statistics.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 5.2.3	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 jitter operation:

```
RP/0/RP0/CPU0:router# show ipsla statistics enhanced aggregated 20

Entry number: 101
Interval : 120 seconds
  Bucket : 1
    Start Time Index: 16:39:37.884 GMT Fri Nov 28 2014
    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  : 3          RTTMin: 1          RTTMax : 5
      NumOfRTT: 20         RTTSum: 63         RTTSum2: 213
    Packet Loss Values:
      PacketLossSD       : 0          PacketLossDS : 0
      PacketOutOfSequence: 0          PacketMIA    : 0
      PacketLateArrival  : 0          PacketSkipped: 0
      Errors             : 0          Busies       : 0
      InvalidTimestamp   : 0
    Jitter Values :
      MinOfPositivesSD: 1          MaxOfPositivesSD: 2
      NumOfPositivesSD: 7          SumOfPositivesSD: 9
      Sum2PositivesSD : 13
      MinOfNegativesSD: 1          MaxOfNegativesSD: 1
      NumOfNegativesSD: 7          SumOfNegativesSD: 7
      Sum2NegativesSD : 7
      MinOfPositivesDS: 1          MaxOfPositivesDS: 1
      NumOfPositivesDS: 2          SumOfPositivesDS: 2
      Sum2PositivesDS : 2
      MinOfNegativesDS: 1          MaxOfNegativesDS: 1
      NumOfNegativesDS: 2          SumOfNegativesDS: 2
      Sum2NegativesDS : 2
      JitterAve: 1         JitterSDAve: 1      JitterDSAve: 1
      Interarrival jitterout: 0              Interarrival jitterin: 0
    One Way Values :
      NumOfOW: 0
      OWMinSD : 0          OWMaxSD: 0          OWSumSD: 0
      OWSum2SD: 0          OWAveSD: 0
      OWMinDS : 0          OWMaxDS: 0          OWSumDS: 0
      OWSum2DS: 0          OWAveDS: 0
  Bucket : 2
    Start Time Index: 16:41:36.657 GMT Fri Nov 28 2014
    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  : 3          RTTMin: 2          RTTMax : 4
      NumOfRTT: 20         RTTSum: 61         RTTSum2: 189

  ...
```

This table describes the significant fields shown in the display.

Table 21: 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.

Field	Description
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.

Related Commands

Command	Description
show ipsla statistics, on page 140	Displays the operational data for the IP SLA operation.
show ipsla statistics aggregated, on page 143	Displays the statistical errors for all the IP SLA operations or for a specified operation.

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 jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# source address 192.0.2.9
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

source port

To identify the port of the source device, use the **source port** command in the appropriate configuration mode. To use the unused port number, use the **no** form of this command.

source port *port*
no source port

Syntax Description

port *port*	Identifies the port number of the source device. Range is 1 to 65535.

Command Default

IP SLA uses an unused port that is allocated by system.

Command History

Releas	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

The **source port** command is supported only to configure UDP operations.

The specified source port should not be used in other IPSLA operations configured on the same source IP address and source VRF.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# source port 11111
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

start-time

To determine the time when the operation 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

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **start-time** command option for the schedule operation:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# start-time after 01:00:00
```

Related Commands

Command	Description
life, on page 119	Specifies the length of time to execute.
operation, on page 121	Configures an IP SLA operation.
recurring, on page 131	Indicates that the operation starts automatically at the specified time and for the specified duration every day.
schedule operation, on page 132	Schedules an IP SLA operation.

statistics

To set the statistics collection parameters for the operation, use the **statistics** command in the appropriate configuration mode. To remove the statistics collection or use the default value, use the **no** form of this command.

statistics {**hourly** | **interval** *seconds*}
no statistics {**hourly** | **interval** *seconds*}

Syntax Description

hourly	Sets the distribution for statistics configuration that is aggregated for over an hour.
interval *seconds*	Collects statistics over a specified time interval. Interval (in seconds) over which to collect statistics. Range is 1 to 3600 seconds.

Command Default

None

Command Modes

IP SLA operation UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

If the **statistics** command is used in IP SLA operation mode, it configures the statistics collection for the specific operation being configured.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

The following example shows how to collect statistics for a specified time interval, using the **statistics** command in an IP SLA UDP jitter operation:

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

```
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics interval 60
RP/0/RP0/CPU0:router(config-ipsla-op-stats)#
```

Related Commands

Command	Description
buckets (statistics hourly), on page 106	Sets the number of hours in which statistics are kept.
buckets (statistics interval), on page 107	Refers to the data buckets in which the enhanced history statistics are kept.
distribution count, on page 112	Sets the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation.
distribution interval, on page 114	Sets the time interval (in milliseconds) for each statistical distribution.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

tag (IP SLA)

To create a user-specified identifier for an IP SLA operation, use the **tag** command in the appropriate configuration mode. To unset the tag string, use the **no** form of this command.

tag [*text*]
no tag

Syntax Description

text	(Optional) Specifies a string label for the IP SLA operation.

Command Default

No tag string is configured.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

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 5.2.3	This command was introduced.

Usage Guidelines

The **threshold** command is supported only when used with the **react** command and **jitter-average** and **packet-loss** keywords.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **jitter-average** keyword for the **threshold** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **packet-loss** keyword for the **threshold** command:

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

```
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

threshold type average

To take action on average values to violate a threshold, use the **threshold type average** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type average *number-of-probes*
no threshold type

Syntax Description

number-of-probes	When the average of the last five values for the monitored element exceeds the upper threshold or the average of the last five values for the monitored element drops below the lower threshold, the action is performed as defined by the **action** command. Range is 1 to 16.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

The **threshold type average** command is supported only when used with the **react** command and **jitter-average**, **packet-loss**, and **rtt** keywords.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of probes for the **react** command with the **jitter-average** keyword for the **threshold type average** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type average 8
```

The following example shows how to set the number of probes for the **react** command with the **packet-loss** keyword for the **threshold type average** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react packet-loss dest-to-source
```

```
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type average 8
```

Related Commands

Command	Description
action (IP SLA), on page 103	Specifies what action or combination of actions the operation performs.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold, on page 159	Sets the lower-limit and upper-limit values.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

threshold type consecutive

To take action after a number of consecutive violations, use the **threshold type consecutive** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type consecutive *occurrences*
no threshold type

Syntax Description

occurrences	When the reaction condition is set for a consecutive number of occurrences, there is no default value. The number of occurrences is set when specifying the threshold type. The number of consecutive violations is 1 to 16.

Command Default

No default behavior or values

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type consecutive 8
```

Related Commands

Command	Description
action (IP SLA), on page 103	Specifies what action or combination of actions the operation performs.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

Command	Description
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold, on page 159	Sets the lower-limit and upper-limit values.
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

threshold type immediate

To take action immediately upon a threshold violation, use the **threshold type immediate** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type immediate
no threshold type

Syntax Description

This command has no keywords or arguments.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 5.2.3	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.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react  jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type immediate
```

Related Commands

Command	Description
action (IP SLA), on page 103	Specifies what action or combination of actions the operation performs.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

Command	Description
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold, on page 159	Sets the lower-limit and upper-limit values.
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type xofy, on page 167	Takes action upon X violations in Y probe operations.

threshold type xofy

To take action upon X violations in Y probe operations, use the **threshold type xofy** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type xofy *x-value y-value*
no threshold type

Syntax Description

x-value y-value	When the reaction conditions, such as threshold violations, are met for the monitored element after some *x* number of violations within some other *y* number of probe operations (for example, *x* of *y*), the action is performed as defined by the **action** command. Default is 5 for both *x-value* and *y-value;* for example, **xofy** 5 5. Range is 1 to 16.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react jitter-average
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# threshold type xofy 1 5
```

Related Commands

Command	Description
action (IP SLA), on page 103	Specifies what action or combination of actions the operation performs.
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

Command	Description
reaction operation, on page 128	Configures certain actions that are based on events under the control of the IP SLA agent.
react, on page 124	Specifies an element to be monitored for a reaction.
threshold, on page 159	Sets the lower-limit and upper-limit values.
threshold type average, on page 161	Takes action on average values to violate a threshold.
threshold type consecutive, on page 163	Takes action after a number of consecutive violations.
threshold type immediate, on page 165	Takes action immediately upon a threshold violation.

timeout (IP SLA)

To set the probe or control timeout interval, use the **timeout** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

timeout *milliseconds*
no timeout

Syntax Description

milliseconds	Sets the amount of time (in milliseconds) that the IP SLA operation waits for a response from the request packet. Range is 1 to 604800000.

Command Default

None.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	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.

Note The IP SLA responder needs at least one second to open a socket and program Local Packet Transport Services (LPTS). Therefore, configure the IP SLA timeout to at least 2000 milli seconds.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# timeout 10000
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.

Command	Description
schedule operation, on page 132	Schedules an IP SLA operation.

tos

To set the type of service (ToS) in a probe packet, use the **tos** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

tos *number*
no tos

Syntax Description

number	Type of service number. Range is 0 to 255.

Command Default

The type of service number is 0.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

The ToS value is an 8-bit field in IP headers. The field contains information, such as precedence and ToS. The information is useful for policy routing and for features like Committed Access Rate (CAR) in which routers examine ToS values. When the type of service is defined for an operation, the IP SLA probe packet contains the configured tos value in the IP header.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# tos 60
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

type udp jitter

To use the UDP jitter operation type, use the **type udp jitter** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type udp jitter
no type udp jitter

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IP SLA operation configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

type udp ipv4 address

To configure a permanent port in the IP SLA responder for UDPjitter 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 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# responder
RP/0/RP0/CPU0:router(config-ipsla-resp)# type udp ipv4 address 192.0.2.11 port 10001
```

Related Commands

Command	Description
responder, on page 130	Enables the IP SLA responder for a UDPjitter operation.

verify-data

To check each IP SLA response for corruption, use the **verify-data** command in the appropriate configuration mode. To disable data corruption checking, use the **no** form of this command.

verify-data
no verify-data

Syntax Description

This command has no keywords or arguments.

Command Default

The **verify-data** command is disabled.

Command Modes

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

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

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.
schedule operation, on page 132	Schedules an IP SLA operation.

vrf (IP SLA)

To enable the monitoring of a Virtual Private Network (VPN) in an 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 UDP jitter configuration

Command History

Release	Modification
Release 5.2.3	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 140 command:

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

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# vrf vpn2
```

Related Commands

Command	Description
operation, on page 121	Configures an IP SLA operation.

Command	Description
schedule operation, on page 132	Schedules an IP SLA operation.
type udp jitter, on page 172	Configures an IP SLA UDP jitter operation.

Logging Services Commands

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

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

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *System Monitoring Command Reference for Cisco NCS 6000 Series Routers*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

archive-length

To specify the length of time that logs are maintained in the logging archive, use the **archive-length** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

archive-length *weeks*
no archive-length

Syntax Description

weeks	Length of time (in weeks) that logs are maintained in the archive. Range is 0 to 4294967295.

Command Default

weeks: 4 weeks

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **archive-length** command to specify the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the log archival period to 6 weeks:

```
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# archive-length 6
```

archive-size

To specify the amount of space allotted for syslogs on a device, use the **archive-size** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

archive-size *size*
no archive-size

Syntax Description

size	Amount of space (in MB) allotted for syslogs. The range is 0 to 2047.

Command Default

size: 20 MB

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **archive-length** command to specify the maximum total size of the syslog archives on a storage device. If the size is exceeded, then the oldest file in the archive is deleted to make space for new logs.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the allotted space for syslogs to 50 MB:

```
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# archive-size 50
```

clear logging

To clear system logging (syslog) messages from the logging buffer, use the **clear logging** command in XR EXEC mode.

clear logging

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **clear logging** command to empty the contents of the logging buffer. When the logging buffer becomes full, new logged messages overwrite old messages.

Use the logging buffered, on page 192 command to specify the logging buffer as a destination for syslog messages, set the size of the logging buffer, and limit syslog messages sent to the logging buffer based on severity.

Use the show logging, on page 221 command to display syslog messages stored in the logging buffer.

Task ID

Task ID	Operations
logging	execute

Examples

This example shows how to clear the logging buffer:

```
RP/0/RP0/CPU0:router# clear logging

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

Related Commands

Command	Description
logging buffered, on page 192	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits syslog messages sent to the logging buffer based on severity.
show logging, on page 221	Displays syslog messages stored in the logging buffer.

device

To specify the device to be used for logging syslogs, use the **device** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

device {**disk0** | **disk1** | **harddisk**}
no device

Syntax Description

disk0	Uses disk0 as the archive device.
disk1	Uses disk1 as the archive device.
harddisk	Uses the harddisk as the archive device.

Command Default

None

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **device** command to specify where syslogs are logged. The logs are created under the directory <device>/var/log. If the device is not configured, then all other logging archive configurations are rejected. Similarly, the configured device cannot be removed until the other logging archive configurations are removed.

It is recommended that the syslogs be archived to the harddisk because it has more capacity.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to specify disk1 as the device for logging syslog messages:

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

discriminator (logging)

To create a syslog message discriminator, use the **discriminator** command in XR Config mode. To disable the syslog message discriminator, use the **no** form of this command.

discriminator {**match1** | **match2** | **match2** | **match3** | **nomatch1** | **nomatch2** | **nomatch3**} *value*

Syntax Description

match1	Specifies the first match keyword to filter the syslog messages.
match2	Specifies the second match keyword to filter the syslog messages.
match3	Specifies the third match keyword to filter the syslog messages.
nomatch1	Specifies the first keyword that does not match the syslog messages.
nomatch2	Specifies the second keyword that does not match the syslog messages.
nomatch3	Specifies the third keyword that does not match the syslog messages.
value	A string when matched in the syslog message, is included as the discriminator. If the pattern contains spaces, you must enclose it in quotes (" "). Regular expressions can also be used for value.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 5.3.2	This command was introduced.
Release 6.0.1	Discriminator for logging file was added.

Usage Guidelines

The discriminator can be set to system log messages which is sent to different destination like logging buffer, logging console, logging monitorand remote server.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to set the discriminator for logging buffer:

```
RP/0/RP0/CPU0:router(config)# logging buffered discriminator match1 sample
```

This example shows how to set the discriminator for logging console:

```
RP/0/RP0/CPU0:router(config)# logging console discriminator match1 sample
```

This example shows how to set the discriminator for logging monitor:

```
RP/0/RP0/CPU0:router(config)# logging monitor discriminator match1 sample
```

This example shows how to set the discriminator for logging file:

```
RP/0/RP0/CPU0:router(config)# logging file file1 discriminator match1 sample
```

This example shows how to set the discriminator for remote server:

```
RP/0/RP0/CPU0:router(config)# logging 10.0.0.0 vrf vrf1 discriminator match1 sample
```

file-size

To specify the maximum file size for a log file in the archive, use the **file-size** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

file-size *size*
no file-size

Syntax Description

size	Maximum file size (in MB) for a log file in the logging archive. The range is 1 to 2047.

Command Default

size: 1 MB

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **file-size** command to specify the maximum file size that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the maximum log file size to 10 MB:

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

frequency (logging)

To specify the collection period for logs, use the **frequency** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

frequency {**daily** | **weekly**}
no frequency

Syntax Description

daily	Logs are collected daily.
weekly	Logs are collected weekly.

Command Default

Logs are collected daily.

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **frequency** command to specify if logs are collected daily or weekly.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to specify that logs are collected weekly instead of daily:

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

logging

To specify a system logging (syslog) server host as the recipient of syslog messages, use the **logging** command in 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* } { [**severity** { **alerts** | **all** | **none** | **critical** | **debugging** | **emergencies** | **error** | **info** | **notifications** }] [**operator** *operation*] [**port** *number*] [**vrf** *name*] }

no logging { *IP-address* | *hostname* } { [**severity** { **alerts** | **all** | **none** | **critical** | **debugging** | **emergencies** | **error** | **info** | **notifications** }] [**operator** *operation*] [**port** *number*] [**vrf** *name*] }

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

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

Command Default

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

Command History

Release	Modification
Release 5.0.0	This command was introduced.
Release 7.4.1	The **all** and **none** keywords were added under the **logging severity** command form.

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 215 command to limit the messages sent to snmp server.

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

Examples

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

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

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

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

RP/0/RP0/CPU0:router(config)#do show run logging
Wed Nov 14 03:48:10.816 PST
logging A.B.C.D vrf default severity info
```

Note Default level is severity info.

Related Commands

Command	Description
logging trap, on page 215	Limits the messages sent to snmp server.

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{**archive-length** | **archive-size** | **device** | **file-size** | **frequency** | **severity** | **threshold**}
no logging archive

Syntax Description

archive-length	Maximum no of weeks that the log is maintained. Minimum number of week is 1 and the maximum number of weeks are 256. Recommended is 4 weeks.
archive-size	Total size of the archive. Value range from 1 MB to 2047 MB. Recommended is 20 MB.
device	Use configured devices (disk0 | disk1 | harddisk) as the archive device. Recommended is harddisk.
file-size	Maximum file size for a single log file. Value range from 1 MB to 2047 MB. Recommended is 1 MB.
frequency	Collection interval (daily or weekly) for logs. Recommend is daily.
severity	Specifies the filter levels for log messages to archive. • 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) Recommended is informational (severity=6).
threshold	Percentage threshold at which a syslog is generated.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Release	Modification
Release 5.3.2	The threshold keyword was added.

Usage Guidelines

Use the **logging archive** command to configure attributes for archiving syslogs. This command enters logging archive configuration mode and allows you to configure the commands.

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

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enter logging archive configuration mode and change the device to be used for logging syslogs to disk1:

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

logging buffered

To specify the logging buffer as a destination for system logging (syslog) messages, use the **logging buffered** command in XR Config mode. To remove the **logging buffered** command from the configuration file and cancel the use of the buffer, use the **no** form of this command.

logging buffered {*sizeseverity*}
no logging buffered {*sizeseverity*}

Syntax Description

size	Size of the buffer, in bytes. Range is 307200 to 125000000 bytes. The default is 307200 bytes.
severity	Severity level of messages that display on the console. Possible severity levels and their respective system conditions are listed under Table 22: Severity Levels for Messages, on page 192in the "Usage Guidelines" section. The default is **debugging**.

Command Default

size: 307200 bytes

severity: **debugging**

Command History

Release	Modification
Release 5.0.0	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 change the size of the buffer.

The value specified for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the console terminal. See Table 22: Severity Levels for Messages, on page 192for a list of the possible severity level keywords for the *severity* argument.

This table describes the acceptable severity levels for the *severity* argument.

Table 22: 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

Level Keywords	Level	Description	Syslog Definition
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational message only	LOG_INFO
debugging	7	Debugging message	LOG_DEBUG

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the severity level of syslog messages logged to the buffer to **notifications**:

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

Related Commands

Command	Description
archive-size, on page 180	Clears messages from the logging buffer.
show logging, on page 221	Displays syslog messages stored in the logging buffer.

logging console

To enable logging of system logging (syslog) messages logged to the console by severity level, use the **logging console** command in 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 Table 22: Severity Levels for Messages, on page 192 under the “Usage Guidelines” section for the logging buffered, on page 192 command.
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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **logging console** command to prevent debugging messages from flooding your screen.

The **logging console** is for the console terminal. The value specified for the *severity* argument causes messages at that level and at numerically lower levels (higher severity levels) to be displayed on the console.

Use the **logging console disable** command to disable console logging completely.

Use the **no logging console** command to return the configuration to the default setting.

Use the show logging, on page 221 command to display syslog messages stored in the logging buffer.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to change the level of messages displayed on the console terminal to **alerts** (1), which means that **alerts** (1) and **emergencies** (0) are displayed:

```
RP/0/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
```

Related Commands

Command	Description
show logging, on page 221	Displays syslog messages stored in the logging buffer.

logging console disable

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

logging consoledisable
no logging consoledisable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, logging is enabled.

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **logging console disable** command to disable console logging completely.

Use the **no logging console disable** command to return the configuration to the default setting.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to disable syslog messages:

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

logging 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages.

Use the **no logging events link-status** command to enable the logging of link-status messages for physical links only, which is the default behavior.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to disable the logging of physical and logical link-status messages:

```
RP/0/RP0/CPU0:router(config)# logging events link-status disable
```

logging facility

To configure the type of syslog facility in which system logging (syslog) messages are sent to syslog servers, use the **logging facility** command in XR Config mode. To remove the **logging facility** command from the configuration file and disable the logging of messages to any facility type, use the **no** form of this command.

logging facility [*type*]
no logging facility

Syntax Description

type	(Optional) Syslog facility type. The default is **local7**. Possible values are listed under Table 23: Facility Type Descriptions , on page 198in the "Usage Guidelines" section.

Command Default

type: **local7**

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Table 23: 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

Facility Type	Description
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Use the logging, on page 187 command to specify a syslog server host as a destination for syslog messages.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to configure the syslog facility to the **kern** facility type:

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

Related Commands

Command	Description
logging, on page 187	Specifies a syslog server host as a destination for syslog messages.

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. See discriminator (logging), on page 183
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 6.0.1	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 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 in Table 22: Severity Levels for Messages, on page 192 under the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **warnings**

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

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

Use the show logging history, on page 226 command to display the history table, which contains table size, message status, and message text data.

Use the logging history size, on page 205 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
```

Related Commands

Command	Description
logging history size, on page 205	Changes the number of messages stored in the history table.
show logging history, on page 226	Displays information about the state of the syslog history table.

logging history size

To change the number of system logging (syslog) messages that can be stored in the history table, use the **logging history size** command in 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the logging history, on page 203 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
```

Related Commands

Command	Description
logging history, on page 203	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
show logging history, on page 226	Displays information about the state of the syslog history table.

logging hostnameprefix

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the logging, on page 187 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
```

Related Commands

Command	Description
logging, on page 187	Specifies a syslog server host as a destination for syslog messages.

logging ipv4/ipv6

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

logging {**ipv4** | **ipv6**} {**dscp** *dscp-value* | **precedence** {*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

EXEC mode

Command History

Release	Modification
Release 5.1.1	The **ipv4** and **ipv6** keywords were added.

Usage Guidelines

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

You may provide these PHB values:

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

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

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

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

AF11 stands for:

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

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

AF12 stands for:

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

- Dropped second in AF1 class

Class Selector (CS) provides backward compatibility bits,

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

CS1 stands for:

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

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

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

Task ID

Task ID	Operation
logging	read, write

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 History

Release	Modification
Release 5.0.0	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
```

Related Commands

Command	Description
show logging, on page 221	Displays syslog messages stored in the logging buffer.

logging monitor

To specify terminal lines other than the console terminal as destinations for system logging (syslog) messages and limit the number of messages sent to terminal lines based on severity, use the **logging monitor** command in 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**. Settings for the severity levels and their respective system conditions are listed under Table 22: Severity Levels for Messages, on page 192 in the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **debugging**

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the terminal monitor, on page 228 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
```

Related Commands

Command	Description
terminal monitor, on page 228	Enables the display of syslog messages for the current terminal session.

logging source-interface

To set all system logging (syslog) messages being sent to syslog servers to contain the same IP address, regardless of which interface the syslog message uses to exit the router, use the **logging source-interface** command in 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the logging, on page 187 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 0/1/0/0
```

Related Commands

Command	Description
logging, on page 187	Specifies a syslog server host as a destination for syslog messages.

logging suppress deprecated

To prevent the logging of messages to the console to indicate that commands are deprecated, use the **logging suppress deprecated** command in 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 5.0.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

If you use the **logging suppress duplicates** command during debugging sessions, you might not see all the repeated messages and could miss important information related to problems that you are attempting to isolate and resolve. In such a situation, you might consider disabling this command.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging, on page 187	Specifies a syslog server host as a destination for syslog messages.
logging buffered, on page 192	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits the syslog messages sent to the logging buffer based on severity.
logging monitor, on page 211	Specifies terminal lines other than the console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.

logging trap

To specify the severity level of messages logged to snmp server, use the **logging trap** command in 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 22: Severity Levels for Messages, on page 192 in the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **informational**

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **logging trap** command to limit the logging of messages sent to snmp servers to only those messages at the specified level.

Table 22: Severity Levels for Messages, on page 192 under the "Usage Guidelines" section for the logging buffered, on page 192 command lists the syslog definitions that correspond to the debugging message levels.

Use the logging, on page 187 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
```

Related Commands

Command	Description
logging, on page 187	Specifies a syslog server host as a destination for syslog messages.

process shutdown pam_manager

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

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

Syntax Description

location all	Disables PAM agents for all RPs.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operation
network	read, write

This example shows how to disable PAM for all RPs:

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

Related Commands

Command	Description
process start pam_manager, on page 217	Re-enables platform automated monitoring (PAM) by restarting the required process agents.

process start pam_manager

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

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

Syntax Description

location all	Restarts PAM agents for all RPs.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

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

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

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

Task ID

Task ID	Operation
network	read, write

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

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

Related Commands

Command	Description
process shutdown pam_manager, on page 216	

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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Time stamps can be added to either debugging or syslog messages independently. The **uptime** keyword adds time stamps in the format hhhh:mm:ss, indicating the elapsed time in hours:minutes:seconds since the networking device last rebooted. The **datetime** keyword adds time stamps in the format mmm dd hh:mm:ss, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*), which indicates that the date and time have not been set and should be verified.

The **no** form of the **service timestamps** command causes messages to be time-stamped in the default format.

Entering the **service timestamps** form of this command without any keywords or arguments is equivalent to issuing the **service timestamps debug uptime** form of this command.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enable time stamps on debugging messages, which show the elapsed time since the networking device last rebooted:

```
RP/0/RP0/CPU0:router(config)# service timestamps debug uptime
```

This example shows how to enable time stamps on syslog messages, which show the current time and date relative to the local time zone, with the time zone name included:

```
RP/0/RP0/CPU0:router(config)# service timestamps log datetime localtime show-timezone
```

severity

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

severity {*severity*}
no severity

Syntax Description

severity	Severity level for determining which messages are logged to the archive. Possible severity levels and their respective system conditions are listed under Table 22: Severity Levels for Messages, on page 192 in the "Usage Guidelines" section. The default is **informational**.

Command Default

Informational

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Table 22: Severity Levels for Messages, on page 192 describes the acceptable severity levels for the *severity* argument.

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0: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 the alarm-location information. The **trace** option shows trace data for the alarm location components.
correlator*options*	(Optional) Displays the content and information about correlation buffer. The various options available are: • buffer: Displays the 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 as follows: • *month*—The month of the year. The values for the *month* argument are: • january • february • march • april • may • june • july • august • september • october • november • december • *day*—Day of the month. Range is 01 to 31. • *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is 00 to 59.
events *options*	Displays the content and information about event buffer.The various options available are: • buffer: Displays the 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 the contents of logging history.
last *entries*	Displays last <n> entries. The number of entries can range from 1 to 500.

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

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **show logging** command to display the state of syslog error and event logging on the processor console. The information from the command includes the types of logging enabled and the size of the buffer.

Task ID

Task ID	Operations
logging	read

Examples

This is the sample output from the **show logging** command with the **process** keyword and *name* argument. Syslog messages related to the init process are displayed in the sample output.

```
RP/0/RP0/CPU0:router# show logging process init

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level , 59 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 0 messages logged
Buffer logging: level debugging, 75 messages logged

Log Buffer (16384 bytes):

LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
SP/0/1/SP:May 24 22:18:54.925 : init[65541]: %INIT-7-MBI_STARTED : total time 7.159 seconds

SP/0/1/SP:May 24 22:20:16.737 : init[65541]: %INIT-7-INSTALL_READY : total time 88.984
seconds
SP/0/SM1/SP:May 24 22:18:40.993 : init[65541]: %INIT-7-MBI_STARTED : total time 7.194 seconds

SP/0/SM1/SP:May 24 22:20:17.195 : init[65541]: %INIT-7-INSTALL_READY : total time 103.415
seconds
SP/0/2/SP:May 24 22:18:55.946 : init[65541]: %INIT-7-MBI_STARTED : total time 7.152 seconds

SP/0/2/SP:May 24 22:20:18.252 : init[65541]: %INIT-7-INSTALL_READY : total time 89.473
seconds
```

This is the sample output from the **show logging** command using both the **process***name* keyword argument pair and **location** *node-id* keyword argument pair. Syslog messages related to the “init” process emitted from node 0/1/CPU0 are displayed in the sample output.

```
RP/0/RP0/CPU0:router# show logging process init location 0/1/CPU0

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level , 59 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 0 messages logged
```

```
Buffer logging: level debugging, 75 messages logged

Log Buffer (16384 bytes):
LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
```

This table describes the significant fields shown in the display.

Table 24: show logging Field Descriptions

Field	Description
Syslog logging	If enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, the host captures and saves the messages.
Console logging	If enabled, the level and the number of messages logged to the console are stated; otherwise, this field displays "disabled."
Monitor logging	If enabled, the minimum level of severity required for a log message to be sent to the monitor terminal (not the console) and the number of messages logged to the monitor terminal are stated; otherwise, this field displays "disabled."
Trap logging	If enabled, the minimum level of severity required for a log message to be sent to the syslog server and the number of messages logged to the syslog server are stated; otherwise, this field displays "disabled."
Buffer logging	If enabled, the level and the number of messages logged to the buffer are stated; otherwise, this field displays "disabled."

Related Commands

Command	Description
clear logging, on page 181	Clears messages from the logging buffer.

show logging history

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

show logging history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Use the logging history, on page 203 command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Use the logging history size, on page 205 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 25: 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.

Field	Description
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.

Related Commands

Command	Description
logging history, on page 203	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
logging history size, on page 205	Changes the number of syslog messages that can be stored in the history table.

terminal monitor

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

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

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

Note Syslog messages are not sent to terminal lines unless the logging monitor, on page 211 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
```

Related Commands

Command	Description
logging monitor, on page 211	Specifies terminal lines other than console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.

threshold (logging)

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

threshold *percent*
no threshold

Syntax Description

percent	Threshold percentage. The range is from 1 to 99.

Command Default

100 percent

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Usage Guidelines

Use this **threshold** command to specify the percentage threshold. When the total archived files' size exceeds the percentage threshold of the configured archive-size, then the syslog of critical severity is generated. If the size is exceeded, then the oldest file in the archive is deleted to make space for new logs.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to set the threshold percent:

```
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# threshold 70
```

Onboard Failure Logging Commands

This module describes the Cisco IOS XR software commands used to configure onboard failure logging (OBFL) for system monitoring on the router. OBFL gathers boot, and environmental factors failure data for field-replaceable units (FRUs), and stores the information in the nonvolatile memory of the FRU. This information is used for troubleshooting, testing, and diagnosis if a failure or other error occurs.

Because OBFL is on by default, data is collected and stored as soon as the card is installed. If a problem occurs, the data can provide information about historical environmental conditions, uptime, downtime, errors, and other operating conditions.

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

Caution OBFL is activated by default in all cards and should not be deactivated. OBFL is used to diagnose problems in FRUs and to display a history of FRU data.

Related Documents

For detailed information about OBFL concepts, configuration tasks, and examples, see the *Onboard Failure Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

For alarm management and logging correlation commands, see the *Alarm Management and Logging Correlation Commands* module in the *System Monitoring Command Reference for Cisco NCS 6000 Series Routers*.

For detailed information about alarm and logging correlation concepts, configuration tasks, and examples, see the *Implementing Alarm Logs and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

show logging onboard

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

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

Syntax Description

fpd	Displays the OBFL FPD data information.
inventory	Displays the OBFL inventory data information.
temperature	Displays temperature information.
uptime	Displays the OBFL uptime.
voltage	Displays voltage information.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **show logging onboard** command to display all logging messages for OBFL.

To narrow the output of the command, enter the **show logging onboard** command with one of the optional keywords.

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

Task ID

Task ID	Operations
logging	read

Examples

This example displays uptime information from the OBFL feature:

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

Online Diagnostic Commands

This chapter describe all the online diagnostic commands.

diagnostic monitor location

To disable health-monitoring (HM) diagnostic testing for a specified location, use **diagnostic monitor location** command in System Admin Config mode. To enable HM testing (default condition), use the **no** form of this command.

diagnostic monitor location *node-name* **test** *test-name* **disable**
no diagnostic monitor location *node-name* **test** *test-name* **disable**

Syntax Description

node-name	Location where diagnostic monitoring has to disabled/enabled.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.
disable	Disables diagnostic monitoring for a specified location.

Command Default

By default, the health-monitoring tests are enabled in the system.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows how to enable health-monitoring diagnostic testing for 0/7:

```
sysadmin-vm:0_RP0(config)# diagnostic monitor location 0/7 test filesystem_test disable
```

diagnostic monitor interval

To configure health-monitoring (HM) diagnostic testing for a specific interval at a specified location, use **diagnostic monitor interval** command in System Admin Config mode. To reverse the configuration and restore the system to its original state, use the **no** form of this command.

diagnostic monitor interval location *node-name* **test** *test-name* **days** *number-of-days* **time** *hours:minutes:seconds*
no diagnostic monitor interval location *node-name* **test** *test-name* **days** *number-of-days* **time** *hours:minutes:seconds*

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.
number-of-days	Interval between each test run.
hours:minutes:seconds	The *number-of-days* variable specifies the number of days between each test run. The range is from 0 through 20. The *hours:minutes:seconds* variable specifies the test interval. Hour is a number in the range from 0 through 23, minutes is a number in the range from 0 through 59, and seconds is a number in the range from 0 through 59.

Command Default

No default behavior or values.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

A diagnostic test internally defines a minimum interval time that is required for it to complete one round of testing. The configuration will be rejected if you configure the HM testing for an interval time less than the minimum interval time. For example, the filesystem_test has a minimum interval of 10 seconds and the configured interval time must be greater than or equal to 10 seconds.

Examples

This example shows how to set the health-monitoring diagnostic testing at an interval of 1 hour, 2 minutes, and 3 seconds at 0/7 location:

```
sysadmin-vm:0_RP0(config)# diagnostic monitor interval location 0/7 test filesystem_test
days 0 time 1:2:3
```

diagnostic monitor threshold

To configure the health-monitoring (HM) diagnostic test failure threshold, use **diagnostic monitor threshold** command in System Admin Config mode. To reverse the configuration and restore the system to its original state, use the **no** form of this command.

diagnostic monitor threshold location *node-name* **test** *test-name* **failure-count** *failures*
no diagnostic monitor threshold location *node-name* **test** *test-name* **failure-count** *failures*

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.
failure count *failures*	Number of test failures allowed. The given range is 1 to 99.

Command Default

No default behavior or values.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows how to set the failure threshold to 5 test failures at 0/7 location:

```
sysadmin-vm:0_RP0(config)# diagnostic monitor threshold location 0/7 test filesystem_test
failure-count 5
```

diagnostic schedule start

To configure a scheduled diagnostic test, use **diagnostic schedule start** command in System Admin Config mode. To disable the diagnostic schedule, use the **no** form of this command.

diagnostic schedule start location *node-name* **test** *test-name* **on** *month day-of-month year hour:minutes*
diagnostic schedule start location *node-name* **test** *test-name* **weekly** *day-of-week hour:minutes*
diagnostic schedule start location *node-name* **test** *test-name* **daily** *hour:minutes*
no diagnostic schedule start location *node-name* **test** *test-name* **on** *month day-of-month year hour:minutes*

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.
on *month day-of-month year hour:minutes* **weekly** *day-of-week hour:minutes* **daily** *hour:minutes*	Schedules an exact date. *month* is from January to December. *day-of-month* is from 1 to 31. *year* is from 2013 to 2099. *day-of-week* is from Monday to Sunday. *hour:minutes* is the interval time in the range from 0 through 23 and 0 through 59.

Command Default

No default behavior or values.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows how to schedule a test:

- on daily basis:

```
sysadmin-vm:0_RP0(config)# diagnostic schedule start location 0/7 test filesystem_test daily
 01:00
```

- on weekly basis:

```
sysadmin-vm:0_RP0(config)# diagnostic schedule start location 0/7 test filesystem_test
weekly SUN 01:00
```

- on monthly basis:

```
sysadmin-vm:0_RP0(config)# diagnostic schedule start location 0/7 test filesystem_test on
OCT 10 2017 01:00
```

diagnostic start

To start a specific diagnostic test, use **diagnostic start** command in System Admin EXEC mode.

diagnostic start location *node-name* **test** *test-name* **| all**

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported.
all	Keyword all starts all the tests. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows how to start a test at location 0/7:

```
sysadmin-vm:0_RP0# diagnostic start location 0/7 test filesystem_test

Thu Oct  5  08:39:30.342 UTC
Test started successfully
```

diagnostic stop

To stop a diagnostic test that is already in progress, use **diagnostic stop** command in System Admin EXEC mode.

diagnostic stop location *node-name* **test** *test-name* **| all**

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported.
all	Keyword all starts all the tests. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

This command is used for tests that take long time to run. Before running this stop command, check if the test is running, terminate the test using this command, and then clean-up the related data.

Examples

This example shows how to stop a test running at location 0/7:

```
sysadmin-vm:0_RP0# diagnostic stop location 0/7 test filesystem_test

Thu Oct  5  08:39:30.342 UTC
```

show diagnostic content

To display test information including test name, test attributes, HM interval, and threshold, use **show diagnostic content** command in System Admin EXEC mode.

show diagnostic content location *node-name*

Syntax Description

node-name	Location where diagnostic monitoring has to be configured.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows how to stop a test running at location 0/7:

```
sysadmin-vm:0_RP0# show diagnostic content location 0/7

Thu Oct  5  08:42:10.454 UTC

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/*   - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/*   - Only applicable to standby unit / NA
X/*   - Not a health monitoring test / NA
F/*   - Fixed monitoring interval test / NA
E/*   - Always enabled monitoring test / NA
A/I   - Monitoring is active / Monitoring is inactive

                                                         Test Interval     thre-
ID   Test Name                              Attributes   (day hh:mm:ss)    shold
==== ================================= ============ ================= =====

1    filesystem_test                        *B*N**FEA     000 00:03:00       5
sysadmin-vm:0_RP0#
```

show diagnostic result

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

show diagnostic result location *node-name* **test** *test-name* **| all detail**

Syntax Description

node-name	Location where diagnostic monitoring has to disabled/enabled.
test-name	Name of the diagnostic test. Currently, only filesystem_test is supported.
all	Keyword all starts all the tests. You can use **show diagnostic content** command in System Admin EXEC mode to see a list of test names and other associated attributes.
detail	Displays detailed results.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows output sample of a test running at location 0/7:

```
sysadmin-vm:0_RP0# show diagnostic result location 0/7

Thu Oct  5  08:43:50.845 UTC

Test results: (P = Pass, F = Fail, U = Untested, T = Timedout, A = Aborted, S = Stopped)
___________________________________________________________________________

1) filesystem_test -------> P

sysadmin-vm:0_RP0#
sysadmin-vm:0_RP0# show diagnostic result details location 0/7
Thu Oct  5  08:43:57.776 UTC

Test results: (P = Pass, F = Fail, U = Untested, T = Timedout, A = Aborted, S = Stopped)
___________________________________________________________________________

1) filesystem_test -------> P
Error code ------------------> 0 (DIAG_SUCCESS)
Test type -------------------> HEALTH MONITOR
HM test count ---------------> 7
ONDEMAND test count ---------> 1
SCHED test count ------------> 0
Total run count -------------> 8
Last test execution time ----> Thu Oct  5 08:42:30 2017
First test failure time -----> n/a
Last test failure time ------> n/a
Last test pass time ---------> Thu Oct  5 08:42:30 2017
```

```
Total failure count ---------> 0
Consecutive failure count ---> 0
Additional information ------> test completed and passed
___________________________________________________________________________

sysadmin-vm:0_RP0#
```

show diagnostic status

To display running tests, use **show diagnostic status** command in System Admin EXEC mode.

show diagnostic status

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

This command is not applicable to health-monitoring tests.

Examples

This example shows output sample of a running test status:

```
sysadmin-vm:0_RP0# show diagnostic status location_index

Thu Oct  5  08:44:51.182 UTC

<BU> - Bootup Diagnostics,   <HM>   - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCHD> - Scheduled Diagnostics
===========================================================================
Location    Current Running Test  Status                                  Run by
---------------------------------------------------------------------------
0/RP0       N/A                                                      N/A
---------------------------------------------------------------------------

0/RP1       N/A                                                      N/A
---------------------------------------------------------------------------

0/7         N/A                                                      N/A
---------------------------------------------------------------------------

0/RP0/CPU0  N/A                                                      N/A
---------------------------------------------------------------------------

0/RP1/CPU0  N/A                                                      N/A
---------------------------------------------------------------------------

0/7/CPU0    N/A                                                      N/A
---------------------------------------------------------------------------
sysadmin-vm:0_RP0#
```

show logging onboard

To display the onboard diagnostic logs stored in the persistent memory, use **show logging onboard** command in System Admin EXEC mode.

show logging onboard diag_result location *node-name*

Syntax Description

node-name	Location for which diagnostic logs have to be displayed. The available locations can be obtained by using '?' in the command prompt.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows output sample of the show logging onboard command:

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

Thu Oct  5  08:45:43.340 UTC

OBFL Diag Test Result Information For : 0/7
  NOTE: Read Operation in progress; Incomplete Data Displayed
  -----------------------------------------------------------------------------------
       DIAG RESULTS INFORMATION
  -----------------------------------------------------------------------------------
   Time Stamp (UTC)    |     Logging info
   mm/dd/yyyy hh:mm:ss |
  -----------------------------------------------------------------------------------
    Logging Time: 10/05/2017 07:39:12
    0) filesystem_test ----> .
    Error code -------------------> 0 (DIAG_SUCCESS_CAL)
    Total run count --------------> 11
    Last test execution time -----> 10/05/2017 07:39:12
    First test failure time ------>  n/a
    Last test failure time ------->  n/a
    Last test pass time ----------> 10/05/2017 07:39:12
    Consecutive failure count ----> 0

    Logging Time: 10/05/2017 14:07:28
```

show run diagnostic

To display all diagnostic related configurations, use **show run diagnostic** command in System Admin EXEC mode.

show run diagnostic

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Examples

This example shows output sample of the show run diagnostic command:

```
sysadmin-vm:0_RP0# show run diagnostic
Thu Oct  5  08:46:19.371 UTC
diagnostic monitor interval location 0/7
!
diagnostic monitor threshold location 0/7
 test filesystem_test
  failure-count 5
 !
!
diagnostic schedule start location 0/7
 test filesystem_test
  daily 01:00
  !
  on JAN 7 2017 01:00
  !
  weekly SUN 01:00
  !
 !
!
```

Performance Management Commands

This module describes the performance management and monitoring commands available on the router. These commands are used to monitor, collect, and report statistics, and to adjust statistics gathering for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) protocol, generic interfaces, and individual nodes.

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

For detailed information about performance management concepts, configuration tasks, and examples, see the *Implementing Performance Management* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

monitor controller fabric

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

monitor controller fabric {*plane-id* | **all**}

Syntax Description

plane-id	Plane ID number of the fabric plane to be monitored. The range is 0 to 7.
all	Monitors all fabric planes.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **monitor controller fabric** command to display controller fabric counters. The display refreshes every 2 seconds.

The interactive commands that are available during a controller fabric monitoring session are described in this table.

Table 26: Interactive Commands Available for the monitor controller fabric Command

Command	Description
c	Resets controller fabric counters to 0.
f	Freezes the display screen, thereby suspending the display of fresh counters.
t	Thaws the display screen, thereby resuming the display of fresh counters.
q	Terminates the controller fabric monitoring session.
s	Enables you to jump to a nonsequential fabric plane. You are prompted to enter the plane ID of the fabric to be monitored.

Task ID

Task ID	Operations
fabric	read
basic-services	execute
monitor	read

Examples

This is sample output from the **monitor controller fabric** command. The output in this example displays fabric controller counters from fabric plane 0.

```
RP/0//CPU0:router# monitor controller fabric 0

rack3-3 Monitor
Time: 00:00:24 SysUptime: 03:37:57 Controller fabric for 0x0 Controller Fabric Stats:
Delta In Cells 0 ( 0 per-sec) 0 Out Cells 0 ( 0 per-sec) 0 CE Cells 0 ( 0 per-sec) 0 UCE
Cells 0 ( 0 per-sec) 0 PE Cells 0 ( 0 per-sec) 0 Quit='q', Freeze='f', Thaw='t',
Clear='c', Select controller='s'
```

monitor interface

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

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

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 History

Release	Modification
Release 5.0.0	This command was introduced.
Release 7.5.4	The argument *full-name* was introduced.

Usage Guidelines

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

Use the **monitor interface** command without any keywords or arguments to display interface counters for all interfaces. The display refreshes every 2 seconds.

Use the **monitor interface** command with the *type interface-path-id* arguments to display counters for a single interface. For example: **monitor** *interface hundredGigE0/1/0/8*

To display more than one selected interface, enter the **monitor interface** command with multiple *type interface-path-id* arguments. For example: **monitor interface** *hundredGigE0/2/0/0 hundredGigE0/5/0/1 hundredGigE0/5/0/2*

To display a range of interfaces, enter the **monitor interface** command with a wildcard. For example: **monitor** *interface hundredGigE0/5/**

You can display up to 32 specific interfaces and ranges of interfaces.

The interactive commands that are available during an interface monitoring session are described in this table.

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 27: Interactive Commands Available for the monitor interface Command (Functional Summary)

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

Use the following keys to display statistics for a different interface:	
i	Enables you to jump to a nonsequential interface. You are prompted to enter the interface type and interface path ID to be monitored.
p	Displays the previous sequential interface in the list of available interfaces.
n	Displays the next sequential interface in the list of available interfaces.
q	Terminates the interface monitoring session.

Task ID

Task ID	Operations
basic-services	execute
monitor	read

Examples

When more than one interface is specified, the statistics for each interface are displayed on a separate line. This display format appears anytime more than one interface is specified. For example:

- To display statistics for all interfaces, enter the command **monitor interface** .
- To display all the interfaces for an interface type, such as all HundredGigE interface, enter the command and wildcard **monitor interface HundredGigE *** .
- To display statistics for three specified interfaces, enter the command **monitor interface HundredGigE 0/0/0/0 HundredGigE 0/0/0/1 HundredGigE 0/0/0/0** .

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

```
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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **performance-mgmt apply monitor** command to apply a statistics template and enable monitoring. This command captures one cycle of a sample to analyze an instance of an entity. Rather than collect statistics for all instances, which is the purpose of the **performance-mgmt apply statistics** command, the **performance-mgmt apply monitor** command captures statistics for a specific entity instance for one sampling period.

The *type* and *interface-path-id* arguments are only to be used with the **interface data-rates** or **interface generic-counter** keyword.

For information about creating templates, see the performance-mgmt apply statistics, on page 259 command.

Task ID

Task ID	Operations
monitor	read, write, execute

Examples

This example shows how to enable the BGP protocol monitoring using the criterion set in the default template:

```
RP/0/RP0/CPU0:router(config)#performance-mgmt apply monitor bgp 10.0.0.0 default
```

This example shows how to enable monitoring for data rates according to the criterion set in the default template:

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

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

```
RP/0/RP0/CPU0:router(config)#performance-mgmt apply monitor node memory location 0/1/cpu0
default
```

This example shows how to enable monitoring for counters according to the criterion set in the default template:

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

Related Commands

Command	Description
performance-mgmt apply statistics, on page 259	Applies a statistics template and enables statistics collection.
performance-mgmt statistics, on page 269	Creates a template to use for collecting performance management statistics.
show running performance-mgmt, on page 292	Displays a list of templates and the template being applied.

performance-mgmt apply statistics

To apply a statistics template and enable statistics collection, use the **performance-mgmt apply statistics** command in 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, on page 292 command to display a list of available templates.
default	Applies the default template.

Command Default

Statistics collection is disabled.

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **performance-mgmt apply statistics** command to apply a statistics template and enable statistics collection. Only one template for each entity can be enabled at a time. After samples are taken, the data is sent to a directory on an external TFTP server, and a new collection cycle starts. The directory where data is copied to is configured using the performance-mgmt resources tftp-server, on page 267 command. The statistics data in the directory contains the type of entity, parameters, instances, and samples. They are in binary format and must be viewed using a customer-supplied tool, or they can be queried as they are being collected using XML.

Use the **performance-mgmt apply statistics** command to collect data for all the instances on a continuous basis. To analyze a particular instance for a limited period of time, use the performance-mgmt apply monitor, on page 256 command.

Use the **no** form of the command to disable statistics collection. Because only one performance management statistics collection can be enabled for any given entity at any given time, you are not required to specify the template name with the **default** keyword or **template** keyword and *template-name* argument when disabling a performance management statistics collection.

For information about creating templates, see the performance-mgmt statistics, on page 269 command.

⚠

Caution Each particular collection enabled requires a certain amount of resources. These resources are allocated for as long as the collection is enabled.

Task ID

Task ID	Operations
monitor	read, write, execute

Examples

This example shows how to start statistics collection for BGP using the template named bgp1:

```
RP/0//CPU0:router(config)#performance-mgmt apply statistics bgp template bgp1
```

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

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

This example shows how to enable CPU statistics collection based on the settings set in the default template:

```
RP/0//CPU0:router(config)#performance-mgmt apply statistics node cpu location all default
```

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

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

Related Commands

Command	Description
performance-mgmt apply monitor, on page 256	Applies a statistics template to gather one sampling-size set of samples for a particular instance.
performance-mgmt apply thresholds, on page 262	Applies a threshold template and enables threshold monitoring.
performance-mgmt resources tftp-server, on page 267	Configures a destination TFTP server for statistics collections.
performance-mgmt statistics, on page 269	Creates a template to use for collecting performance management statistics.
show running performance-mgmt, on page 292	Displays a list of templates and the template being applied.

performance-mgmt apply thresholds

To apply a thresholds template and enable threshold collection, use the **performance-mgmt apply thresholds** command in 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 292 command to display a list of available templates.
default	Applies the default template.

Command Default

Threshold collection is disabled.

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **performance-mgmt apply thresholds** command to apply a threshold template and enable threshold collection. Several templates can be configured, but only one template for each entity can be enabled at a time.

Use the **no** form of the command to disable threshold collection. Because only one performance management threshold monitoring template can be enabled for any given entity at any given time, you are not required to specify the template name with the **default** keyword or **template** keyword and *template-name* argument when disabling a performance management statistics collection.

For information about creating threshold templates, see the performance-mgmt thresholds, on page 272 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//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//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//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//CPU0:router(config)#performance-mgmt apply thresholds interface basic-counters stats3
```

Related Commands

Command	Description
performance-mgmt thresholds, on page 272	Creates a template to use for threshold collection.
show running performance-mgmt, on page 292	Displays a list of templates and the template being applied.

performance-mgmt regular-expression

To apply a defined regular expression group to one or more statistics or threshold template, use the **performance-mgmt regular-expression** *regular-expression-name* command in 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
monitor	read, write

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

```
RP/0/RP0/CPU0:router# performance-mgmt regular-expression reg1 index 10
```

performance-mgmt resources dump local

To configure the local filesystem on which the statistics data is dumped, use the **performance-mgmt resources dumplocal** command in XR Config mode. To stop dumping of statistics data on the local filesystem, use the **no** form of this command.

performance-mgmt resources dump local
no performance-mgmt resources dump local

Syntax Description

dump	Configures data dump parameters.
local	Sets the local filesystem on which statistics data is dumped. **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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
monitor	read, write

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

```
RP/0/RP0/CPU0:router# performance-mgmt resources dump local
```

performance-mgmt resources memory

To configure memory consumption limits for performance management (PM), use the **performance-mgmt resources memory** command in XR Config mode. To restore the default memory consumption limits, use the **no** form of this command.

performance-mgmt resources memory max-limit *kilobytes* **min-reserved** *kilobytes*
no performance-mgmt resources memory

Syntax Description

max-limit *kilobytes*	Specifies the maximum amount of memory (specified with the *kilobytes* argument) that the PM statistics collector can use for serving data collection requests. Range is 0 to 4294967295 kilobytes.The default is 50000 kilobytes.
min-reserved *kilobytes*	Specifies a minimum amount of memory (specified with the *kilobytes* argument) that must remain available in the system after allowing a new PM data collection request. Range is 0 to 4294967295 kilobytes. The default is 10000 kilobytes.

Command Default

max-limit—50000 *kilobytes*

min-reserved—10000 kilobytes

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **performance-mgmt resource memory** command to ensure that the total memory consumed by data buffers in PM does not exceed a maximum limit and that any new PM data request does not cause available memory in the system to fall below a certain threshold.

Task ID

Task ID	Operations
monitor	read, write

Examples

This example shows how to ensure that the total memory consumed by PM data buffers does not exceed 30,000 kilobytes and that any new PM data request does not cause available memory in the system to fall below 5000 kilobytes:

```
RP/0//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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **performance-mgmt resources tftp-server** command to configure a TFTP resource for performance management. By creating a directory name on the TFTP server, you create a place where statistics can be collected when statistics collection is enabled.

Use the **no** form of this command to disable the TFTP resource.

Note Files copied to the TFTP server contain a timestamp in their name, which makes them unique. For that reason the TFTP server used should support creation of files as data is transferred, without requiring users to manually create them at the TFTP server host in advance.

Task ID

Task ID	Operations
monitor	read, write

Examples

This example shows how to specify a TFTP server with the IP address 192.168.134.254 as the performance management resource and a directory named /user/perfmgmt/tftpdump as the destination for PM statistic collections:

```
RP/0//CPU0:router(config)#performance-mgmt resources tftp-server 192.168.134.254 directory
 /user/perfmgmt/tftpdump
```

Related Commands

Command	Description
performance-mgmt apply statistics, on page 259	Applies a statistics template and enables statistics collection.
performance-mgmt apply thresholds, on page 262	Applies a threshold template and enables threshold monitoring.

performance-mgmt statistics

To create a template to use for collecting performance management statistics, use the **performance-mgmt statistics** command in 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 292 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

If you have not yet created a directory for the statistics, use the performance-mgmt resources tftp-server, on page 267 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 259 command, the samples are collected and sent to that directory for later retrieval.

The statistics collected contain type of entity, parameters, instances, and samples. The collection files on the TFTP server are in binary format and must be viewed using a customer-supplied tool or they can be queried as they are being collected using XML.

Task ID

Task ID	Operations
monitor	read, write

Examples

This example shows how to create a template named int_data_rates for data rate statistics collection, how to set the sample size to 25, and how to set the sample interval to 5 minutes:

```
RP/0//CPU0:router(config)#performance-mgmt statistics interface data-rates int_data_rates
RP/0//CPU0:router(config_stats-if-rate)# sample-size 25
RP/0//CPU0:router(config_stats-if-rate)# sample-interval 5
```

Related Commands

Command	Description
performance-mgmt apply statistics, on page 259	Applies a statistics template and enables statistics collection.
performance-mgmt resources tftp-server, on page 267	Configures resources for the performance management system that are independent of any particular entity.
performance-mgmt thresholds, on page 272	Configures a template for collecting threshold statistics.
show running performance-mgmt, on page 292	Displays a list of templates and the template being applied.

performance-mgmt thresholds

To configure a template for threshold checking, use the **performance-mgmt thresholds** command in 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*] [*delta*] [**rearm** { **toggle** | **window** *window-size* }]
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 292 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 29: Attribute Values, on page 274for 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.
delta	(Optional) The feature invokes an alarm when the difference between the current and the previous counter value satisfies the threshold condition.
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.

Command Default

None

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the *percent* argument to specify a value that is relative to the previous sample's interval value. When you use the *percent* argument with a *value* of 50, the calculation is performed in this manner, assuming that your current sampled value is sample1 (S1) and the value sampled in the previous sampling period is sample 0 (S0):

```
(S1 - S0) GT 50% of S0
```

For example, if you wanted to check for an increase of 50 percent in the counter BGPInputErrors, you could use the following *attribute* and *operation* with the *percent* argument:

```
BGPInputErrors GT 50
```

This table shows threshold behavior, assuming the values for BGPInputErrors are at consecutive samplings.

Table 28: 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 29: Attribute Values

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

Entity	Attributes	Description
	OutOctets	Bytes sent (64-bit).
	OutPackets	Packets sent (64-bit).
	OutputQueueDrops	Output queue drops (64-bit).
	OutputTotalDrops	Outbound correct packets discarded (64-bit).
	OutputTotalErrors	Outbound incorrect packets discarded (64-bit).
interface data-rates	Bandwidth	Bandwidth, in kbps.
	InputDataRate	Input data rate in kbps.
	InputPacketRate	Input packets per second.
	InputPeakRate	Peak input data rate.
	InputPeakPkts	Peak input packet rate.
	OutputDataRate	Output data rate in kbps.
	OutputPacketRate	Output packets per second.
	OutputPeakPkts	Peak output packet rate.
	OutputPeakRate	Peak output data rate.

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

Entity	Attributes	Description
mpls ldp	AddressMsgsRcvd	Address messages received.
	AddressMsgsSent	Address messages sent.
	AddressWithdrawMsgsRcvd	Address withdraw messages received.
	AddressWithdrawMsgsSent	Address withdraw messages sent.
	InitMsgsSent	Initial messages sent.
	InitMsgsRcvd	Initial messages received.
	KeepaliveMsgsRcvd	Keepalive messages received.
	KeepaliveMsgsSent	Keepalive messages sent.
	LabelMappingMsgsRcvd	Label mapping messages received.
	LabelMappingMsgsSent	Label mapping messages sent.
	LabelReleaseMsgsRcvd	Label release messages received.
	LabelReleaseMsgsSent	Label release messages sent.
	LabelWithdrawMsgsRcvd	Label withdraw messages received.
	LabelWithdrawMsgsSent	Label withdraw messages sent.
	NotificationMsgsRcvd	Notification messages received.
	NotificationMsgsSent	Notification messages sent.
	TotalMsgsRcvd	Total messages received.
	TotalMsgsSent	Total messages sent.
node cpu	AverageCPUUsed	Average system percent CPU utilization.
	NoProcesses	Number of processes.
node memory	CurrMemory	Current application memory (in bytes) in use.
	PeakMemory	Maximum system memory (in MB) used since bootup.
node process	AverageCPUUsed	Average percent CPU utilization.
	NumThreads	Number of threads.
	PeakMemory	Maximum dynamic memory (in KB) used since startup time.

Entity	Attributes	Description
ospf v2protocol	InputPackets	Total number of packets received
	OutputPackets	Total number of packets sent
	InputHelloPackets	Number of Hello packets received
	OutputHelloPackets	Number of Hello packets sent
	InputDBDs	Number of DBD packets received
	InputDBDsLSA	Number of LSA received in DBD packets
	OutputDBDs	Number of DBD packets sent.
	OutputDBDsLSA	Number of LSA sent in DBD packets
	InputLSRequests	Number of LS requests received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSRequests	Number of LS requests sent.
	OutputLSRequestsLSA	Number of LSA sent in LS requests.
	InputLSAUpdates	Number of LSA updates received.
	InputLSAUpdatesLSA	Number of LSA received in LSA updates.
	OutputLSAUpdates	Number of LSA updates sent.
	OutputLSAUpdatesLSA	Number of LSA sent in LSA updates.
	InputLSAAcks	Number of LSA acknowledgements received.
	InputLSAAcksLSA	Number of LSA received in LSA acknowledgements.
	OutputLSAAcks	Number of LSA acknowledgements sent.
	OutputLSAAcksLSA	Number of LSA sent in LSA acknowledgements.
	ChecksumErrors	Number of packets received with checksum errors.

Entity	Attributes	Description
ospf v3protocol	InputPackets	Total number of packets received.
	OutputPackets	Total number of packets sent.
	InputHelloPackets	Number of Hello packets received.
	OutputHelloPackets	Number of Hello packets sent.
	InputDBDs	Number of DBD packets received.
	InputDBDsLSA	Number of LSA received in DBD packets.
	OutputDBDs	Number of DBD packets sent.
	OutputDBDsLSA	Number of LSA sent in DBD packets.
	InputLSRequests	Number of LS requests received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSRequests	Number of LS requests sent.
	OutputLSRequestsLSA	Number of LSA sent in LS requests.
	InputLSAUpdates	Number of LSA updates received.
	InputLSRequestsLSA	Number of LSA received in LS requests.
	OutputLSAUpdates	Number of LSA updates sent.
	OutputLSAUpdatesLSA	Number of LSA sent in LSA updates.
	InputLSAAcks	Number of LSA acknowledgements received.
	InputLSAAcksLSA	Number of LSA received in LSA acknowledgements.
	OutputLSAAcks	Number of LSA acknowledgements sent
	OutputLSAAcksLSA	Number of LSA sent in LSA acknowledgements.

Task ID

Task ID	Operations
monitor	read, write

Examples

This example shows how to create a template for monitoring BGP thresholds, which checks if the number of connections dropped exceeds 50 for any BGP peers. The **toggle rearm** keywords are included so that once the threshold is passed, the event will not be reported unless the value of ConnDropped is reset:

```
RP/0/RP0/CPU0:router(config)# performance-mgmt thresholds bgp template bgp_thresh1
RP/0/RP0/CPU0:router(config-threshold-bgp)# ConnDropped GT 50 rearm toggle
```

This example shows how to create a template for monitoring node CPU utilization that checks if there is a 25 percent increase at any given interval:

```
RP/0/RP0/CPU0:router(config)# performance-mgmt thresholds node cpu template cpu_thresh1
RP/0/RP0/CPU0:router(config-threshold-bgp)# AverageCPUUsed GT 25
```

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
```

Related Commands

Command	Description
performance-mgmt apply thresholds, on page 262	Enables threshold monitoring for BGP.
performance-mgmt resources tftp-server, on page 267	Configures a TFTP resource for performance management.
show running performance-mgmt, on page 292	Displays a list of templates and the template being applied.

show performance-mgmt bgp

To display performance management (PM) data from Border Gateway Protocol (BGP) entity instance monitoring or statistics collections, use the **show performance-mgmt bgp** command in 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

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

```
RP/0/RP0/CPU0:router# show performance-mgmt monitor bgp 10.0.0.0 all-samples

BGP Neighbor: 10.0.0.0 Sample no: 1
----------------------------------------------
InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
```

```
ErrorsReceived: 0 ErrorsSent: 0 BGP Neighbor: 10.0.0.0 Sample no: 2
---------------------------------------------- InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
ErrorsReceived: 0 ErrorsSent: 0 BGP Neighbor: 10.0.0.0 Sample no: 3
--------------------------------------------------- InputMessages: 0 OutputMessages: 0
InputUpdateMessages: 0 OutputUpdateMessages: 0 ConnEstablished: 0 ConnDropped: 0
ErrorsReceived: 0 ErrorsSent: 0
```

This table describes the significant fields in the display.

Table 30: show performance-mgmt bgp Field Descriptions

Field	Description
ConnDropped	Number of times the connection was dropped.
ConnEstablished	Number of times the connection was established.
ErrorsReceived	Number of error notifications received on the connection.
ErrorsSent	Number of error notifications sent on the connection.
InputMessages	Number of messages received.
InputUpdateMessages	Number of update messages received.
OutputMessages	Number of messages sent.
OutputUpdateMessages	Number of update messages sent.

show performance-mgmt interface

To display performance management (PM) data from interface entity instance monitoring or statistics collections, use the **show performance-mgmt interface** command in XR EXEC mode.

show performance-mgmt {**monitor** | **statistics**} **interface** {**basic-counters** | **data-rates** | **generic-counters**} {*type interface-path-id* | **all**} {*sample-id* | **all-samples** | **last-sample**}

Syntax Description

monitor	Displays the data collected for an entity instance monitoring collection. The data gathered is from one sample cycle from one instance of an interface data entity collection template. **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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

This is sample output from the **show performance-mgmt 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 31: 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.

Field	Description
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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

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

```
 RP/0/RP0/CPU0:router# show performance-mgmt monitor mpls ldp 192.0.2.45 last-sample
LDP Neighbor: 192.0.2.45 Sample no: 2
-------------------------------------------------------
```

```
TotalMsgsSent: 131,

TotalMsgsRcvd: 131 InitMsgsSent: 1, InitMsgsRcvd: 1 AddressMsgsSent: 1, AddressMsgsRcvd:
1 AddressWithdrawMsgsSent: 0, AddressWithdrawMsgsRcvd: 0 LabelMappingMsgsSent: 6,
LabelMappingMsgsRcvd: 7 LabelWithdrawMsgsSent: 0, LabelWithdrawMsgsRcvd: 0
LabelReleaseMsgsSent: 0, LabelReleaseMsgsRcvd: 0 NotificationMsgsSent: 0
NotificationMsgsRcvd: 0
```

This table describes the significant fields shown in the display.

Table 32: 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

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

```
 RP/0/RP0/CPU0:router# show performance-mgmt monitor node process location 0//CPU0 process
               614587 last-sample
Node ID:
Sample no: 1 ---------------------------------------------- Process ID: 614587
---------------------------------------------- PeakMemory: 908 AverageCPUUsed: 0
NoThreads: 5
```

This table describes the significant fields shown in the display.

Table 33: 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# show performance-mgmt statistics ospf v2protocol 100 all-samples

Mon Aug 3 06:41:15.785 PST
OSPF Instance: 100 Sample no: 1
-----------------------------------------------------------------------
InputPackets: 12323 OutputPackets: 12045
InputHelloPackets: 11281 OutputHelloPackets: 11276
InputDBDs: 18 OutputDBDs: 20
```

```
InputDBDsLSA: 508 OutputDBDsLSA: 530
InputLSRequests: 1 OutputLSRequests: 2
InputLSRequestsLSA: 11 OutputLSRequestsLSA: 0
InputLSAUpdates: 989 OutputLSAUpdates: 109
InputLSAUpdatesLSA: 28282 OutputLSAUpdatesLSA: 587
InputLSAAcks: 34 OutputLSAAcks: 638
InputLSAAcksLSA: 299 OutputLSAAcksLSA: 27995
ChecksumErrors: 0
```

show 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 History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

This example shows the list of statistic and threshold templates, the configuration of each template, and at the end, which templates are enabled for collection:

```
RP/0/RP0/CPU0:router(config)#show running performance-mgmt

performance-mgmt resources tftp-server 192.168.134.254 directory muckier/jagrelo/pmtest
performance-mgmt statistics bgp template template3
 sample-size 5
 sample-interval 60
!
performance-mgmt statistics node cpu template template4
 sample-size 30
 sample-interval 2
!
performance-mgmt statistics interface generic-counters template template2
 sample-size 3
 sample-interval 10
!
```

```
performance-mgmt statistics interface data-rates template template1
 sample-size 10
 sample-interval 5
!
performance-mgmt statistics node memory template template5
 sample-size 30
 sample-interval 2
!
performance-mgmt statistics node process template template6
 sample-size 10
 sample-interval 5
!
performance-mgmt thresholds node cpu template template20
 AverageCpuUsed GT 75
 sample-interval 5
!
performance-mgmt apply statistics interface generic-counters template2
performance-mgmt apply statistics node memory global template5
performance-mgmt apply statistics node process 0/0/CPU0 template6
performance-mgmt apply thresholds node cpu global template20
```

show health sysdb

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

XML schema is supported for the CLI commands.

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

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

Syntax Description

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

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cisco-support	read
interface	read

Examples

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

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

Statistics Service Commands

This module describes the Cisco IOS XR software commands related to the collection of interface statistics (StatsD) for system monitoring on the router. Interface statistics on the router are found in hardware (most of the time) and software (exception packets). The counters are always local (relative to the CPU) to the node on which the interface is homed. The Cisco IOS XR software provides an efficient mechanism to collect these counters from various application-specific integrated circuits (ASICs) or NetIO and assemble an accurate set of statistics for an interface. After the statistics are produced, they can be exported to interested parties (command-line interface [CLI], Simple Network Management Protocol [SNMP], and so forth).

The Cisco IOS XR software statistics collection system provides a common framework to be used by all interface owners to export the statistics for interfaces they own. The system also defines a common set of statistics that are relevant to all interfaces and thereby provides a consistent and constant set of counters that are always associated and maintained with any interface on the router.

The statistics collection system includes the statistics manager, the statistics server, one or more statistics collectors, and the necessary libraries. Each node on a router houses one statistics server.

In addition to the statistics server, each node (that has interfaces) has one or more statistics collectors. Statistics collectors are platform specific and can obtain various hardware and software counters to satisfy requests from the statistics server.

The statistics manager does not attempt to produce statistics for interfaces for which no statistics collector has registered. Requests for statistics on interfaces for which no statistics collector has registered results in an error returned to the requestor by the statistics manager.

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

clear counters

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

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

Syntax Description

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

Counters for all interfaces are cleared.

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Use the **clear counters** command to clear all the statistics counters displayed by the **show interfaces** command. If no optional arguments are supplied or if the **all** keyword is specified, then the counters for all interfaces are cleared. If an interface type is specified, then only the counters for that interface are cleared.

The **clear counters** command with the **all** option clears counters on all interfaces. When you enter this command, the system prompts you for confirmation. You must then press Enter or the *y* key for the **clear counters** command to take effect.

Note This command does not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those counters displayed with the **show interfaces** command.

Task ID

Task ID	Operations
interface	execute

Examples

This example shows how to clear counters on all interfaces:

```
RP/0/RP0/CPU0:router# clear counters interface all
```

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

load-interval

To specify the interval for load calculation of an interface, use the **load-interval** command in interface configuration mode. To reset the load interval to the default setting, use the **no** form of this command.

load-interval *seconds*
no load-interval *seconds*

Syntax Description

seconds	Number of seconds for load calculation of an interface. The value range is from 0 to 600 seconds and in increments of 30 (such as 30, 60, 90, and so on). The default is 300 seconds.

Command Default

seconds: 300 seconds (5 minutes)

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

When load interval is set to zero, load calculation is disabled. If you set the load interval, you must use a multiple of 30 (up to 600 seconds).

Task ID

Task ID	Operations
interface	read/write

Examples

This example shows how to configure the load interval to 30 seconds:

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