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 CRS 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 CRS 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 CRS 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 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 EXEC mode.

clear logging

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.7.0	Removed the **internal** keyword.

Usage Guidelines

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

Use the logging buffered, on page 15 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 47 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 15	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 47	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 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 Global Configuration 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

Global Configuration 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 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 Global Configuration mode. To remove the **logging** command from the configuration file and delete a syslog server from the list of syslog server hosts, use the **no** form of this command.

logging { *IP-address* | *hostname* } { [**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*] }

Syntax Description

IP-address | *hostname*	IP address or hostname of the host to be used as a syslog server.
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.
alerts	Specifies Immediate action needed
critical	Specifies Critical conditions
debugging	Specifies Debugging messages
emergencies	Specifies System is unusable
error	Specifies Error conditions
info	Specifies Informational messages
notifications	Specifies Normal but significant conditions
warning	Specifies Warning conditions
vrf *vrf-name*	Name of the VRF. Maximum length is 32 alphanumeric characters.

Command Default

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

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 4.1.0	The vrf keyword was added.

Release	Modification
Release 4.3	The severity keyword was added.
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 43 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 43	Limits the messages sent to snmp server.

logging archive

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

logging archive{**archive-length** | **archive-size** | **device** | **file-size** | **frequency** | **severity** | **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

Global Configuration mode

Command History

Release	Modification
Release 3.2	This command was introduced.
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 Global Configuration mode. To remove the **logging buffered** command from the configuration file and cancel the use of the buffer, use the **no** form of this command.

logging buffered {*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 1: Severity Levels for Messages, on page 15in the “Usage Guidelines” section. The default is **debugging**.

Command Default

size: 307200 bytes

severity: **debugging**

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 4.0.0	The value of size argument is changed from 4096 to 307200.

Usage Guidelines

Use the **logging buffered** command to copy messages to the logging buffer. The logging buffer is circular, so newer messages overwrite older messages after the buffer is filled. This command is related to the **show logging buffer** command, which means that when you execute a **logging buffered warnings** command, it enables the logging for all the levels below the configured level, including log for LOG_ERR, LOG_CRIT, LOG_ALERT, LOG_EMERG, and LOG_WARNING messages. Use the **logging buffer size** to change the size of the buffer.

The value specified for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the console terminal. See Table 1: Severity Levels for Messages, on page 15for a list of the possible severity level keywords for the *severity* argument.

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

Table 1: 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

Level Keywords	Level	Description	Syslog Definition
errors	3	Error condition	LOG_ERR
warnings	4	Warning condition	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational message only	LOG_INFO
debugging	7	Debugging message	LOG_DEBUG

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
archive-size, on page 4	Clears messages from the logging buffer.
show logging, on page 47	Displays syslog messages stored in the logging buffer.

logging console

To enable logging of system logging (syslog) messages logged to the console by severity level, use the **logging console** command in Global Configuration mode. To return console logging to the default setting, use the **no** form of this command.

logging console {*severity* | **disable**}
no logging console

Syntax Description

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 1: Severity Levels for Messages, on page 15 under the "Usage Guidelines" section for the logging buffered, on page 15 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 Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.3.0	Added the **disable** keyword. The command **no logging console** was changed to reset console logging to the default setting.

Usage Guidelines

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

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

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

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

Use the show logging, on page 47 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 47	Displays syslog messages stored in the logging buffer.

logging console disable

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

logging consoledisable
no logging consoledisable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, logging is enabled.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to disable syslog messages:

```
RP/0/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 Global Configuration mode. To disable the logging of link status messages, use the **no** form of this command.

logging events link-status {**disable** | **software-interfaces**}
no logging events link-status [{**disable** | **software-interfaces**}]

Syntax Description

disable	Disables the logging of link-status messages for all interfaces, including physical links.
software-interfaces	Enables the logging of link-status messages for logical links as well as physical links.

Command Default

The logging of link-status messages is enabled for physical links.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced
Release 3.5.0	The **logical** and **physical** keywords were replaced by the **software-interfaces** and **disable** keywords.

Usage Guidelines

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

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

Note Enabling the logging events link-status (interface), on page 22 command on a specific interface overrides the global configuration set using the **logging events link-status** command described in this section.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

Related Commands

Command	Description
logging events link-status (interface), on page 22	Enables the logging of link-status system logging (syslog) messages on a specific interface for virtual interfaces and subinterfaces.

logging events link-status (interface)

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

logging events link-status
no logging events link-status

Syntax Description

This command has no keywords or arguments.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

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

Note Enabling the **logging events link-status** command on a specific interface overrides the global configuration set using the logging events link-status, on page 20 command in global configuration mode.

Task ID

Task ID	Operations
logging	read, write

Examples

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

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

LC/0/4/CPU0:Jun 29 12:51:26.887 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface POS0/4/0/0, changed state to Up

LC/0/4/CPU0:Jun 29 12:51:26.897 : ifmgr[142]:
```

```
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface POS0/4/0/0, changed state to Up


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

LC/0/4/CPU0:Jun 29 12:51:32.375 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface POS0/4/0/0, changed state to Down

LC/0/4/CPU0:Jun 29 12:51:32.376 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface POS0/4/0/0, changed state to
Down
```

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

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

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

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

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

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

RP/0/RP0/CPU0:Jun 29 14:06:02.109 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Down
```

This example shows the same process for a subinterface:

```
RP/0/RP0/CPU0:router(config)# int gigabitEthernet 0/5/0/0.1
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# no shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# logging events link-status
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:46.710 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface GigabitEthernet0/5/0/0.1, changed
```

```
 state to Administratively Down

LC/0/5/CPU0:Jun 29 14:06:46.726 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/5/0/0.1, changed state to
Administratively Down

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

LC/0/5/CPU0:Jun 29 14:06:52.229 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/5/0/0.1, changed state to Up


LC/0/5/CPU0:Jun 29 14:06:52.244 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface GigabitEthernet0/5/0/0.1, changed
 state to Down
```

logging facility

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

logging facility [*type*]
no logging facility

Syntax Description

type	(Optional) Syslog facility type. The default is **local7**. Possible values are listed under Table 2: Facility Type Descriptions , on page 25in the “Usage Guidelines” section.

Command Default

type: **local7**

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

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

Table 2: Facility Type Descriptions

Facility Type	Description
auth	Authorization system
cron	Cron/at facility
daemon	System daemon
kern	Kernel
local0	Reserved for locally defined messages
local1	Reserved for locally defined messages
local2	Reserved for locally defined messages
local3	Reserved for locally defined messages
local4	Reserved for locally defined messages
local5	Reserved for locally defined messages
local6	Reserved for locally defined messages
local7	Reserved for locally defined messages

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

Use the logging, on page 11 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 11	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 Global Configuration 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 7
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

Global Configuration 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 Global Configuration 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

Global Configuration 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 Global Configuration mode. To remove the **logging history** command from the configuration and return the logging of messages to the default level, use the **no** form of this command.

logging history *severity*
no logging history

Syntax Description

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 1: Severity Levels for Messages, on page 15 under the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **warnings**

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 51 command to display the history table, which contains table size, message status, and message text data.

Use the logging history size, on page 32 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 32	Changes the number of messages stored in the history table.
show logging history, on page 51	Displays information about the state of the syslog history table.

logging history size

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

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

Syntax Description

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

Command Default

number: 1 message

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 30 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 30	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
show logging history, on page 51	Displays information about the state of the syslog history table.

logging hostnameprefix

To append a hostname prefix to system logging (syslog) messages logged to syslog servers, use the **logging hostnameprefix** command in Global Configuration mode. To remove the **logging hostnameprefix** command from the configuration file and disable the logging host name prefix definition, use the **no** form of this command.

logging hostnameprefix *hostname*
no logging hostnameprefix

Syntax Description

hostname	Hostname that appears in messages sent to syslog servers.

Command Default

No hostname prefix is added to the messages logged to the syslog servers.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 11 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 11	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 Global Configuration mode. To remove the **logging localfilesize** command from the configuration file and restore the system to the default condition, use the **no** form of this command.

logging localfilesize *bytes*
no logging localfilesize *bytes*

Syntax Description

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

Command Default

bytes: 32000 bytes

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 47	Displays syslog messages stored in the logging buffer.

logging monitor

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

logging monitor [*severity*]
no logging monitor

Syntax Description

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 1: Severity Levels for Messages, on page 15 in the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **debugging**

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 53 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 53	Enables the display of syslog messages for the current terminal session.

logging source-interface

To set all system logging (syslog) messages being sent to syslog servers to contain the same IP address, regardless of which interface the syslog message uses to exit the router, use the **logging source-interface** command in Global Configuration mode. To remove the **logging source-interface** command from the configuration file and remove the source designation, use the **no** form of this command.

logging source-interface *type interface-path-id*
no logging source-interface

Syntax Description

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

Command Default

No source IP address is specified.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 11 command to specify a syslog server host as a destination for syslog messages.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to specify that the IP address for Packet-over-SONET/SDH (POS) interface 0/1/0/1 be set as the source IP address for all messages:

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

Related Commands

Command	Description
logging, on page 11	Specifies a syslog server host as a destination for syslog messages.

logging suppress deprecated

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

logging suppress deprecated
no logging suppress deprecated

Syntax Description

This command has no keywords or arguments.

Command Default

Console messages are displayed when deprecated commands are used.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
logging	read, write

Examples

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

```
RP/0/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 Global Configuration mode. To remove the **logging suppress duplicates** command from the configuration file and disable the filtering process, use the **no** form of this command.

logging suppress duplicates
no logging suppress duplicates

Syntax Description

This command has no keywords or arguments.

Command Default

Duplicate messages are logged.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	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 11	Specifies a syslog server host as a destination for syslog messages.
logging buffered, on page 15	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 38	Specifies terminal lines other than the console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.

logging trap

To specify the severity level of messages logged to snmp server, use the **logging trap** command in Global Configuration mode. To restore the default behavior, use the **no** form of this command.

logging trap [*severity*]
no logging trap

Syntax Description

severity	(Optional) Severity level of messages logged to the snmp server, including events of a higher severity level (numerically lower). The default is **informational**. Settings for the severity levels and their respective system conditions are listed under Table 1: Severity Levels for Messages, on page 15 in the "Usage Guidelines" section for the **logging buffered** command.

Command Default

severity: **informational**

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 4.3	Change in the behavior of logging trap and logging severity for snmp and syslog servers.

Usage Guidelines

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

Table 1: Severity Levels for Messages, on page 15 under the "Usage Guidelines" section for the logging buffered, on page 15 command lists the syslog definitions that correspond to the debugging message levels.

Use the logging, on page 11 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 11	Specifies a syslog server host as a destination for syslog messages.

service timestamps

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

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

Syntax Description

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.
year	(Optional) Adds year information to timestamp.
disable	(Optional) Causes messages to be time-stamped in the default format.
uptime	(Optional) Specifies that syslog messages are time-stamped with the time that has elapsed since the networking device last rebooted.

Command Default

Messages are time-stamped in the month day hh:mm:ss by default.

The default for the **service timestamps log datetime localtime** and **service timestamps debug datetime localtime** forms of the command with no additional keywords is to format the time in the local time zone, without milliseconds and time zone information.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 4.3	The keyword year was added.

Usage Guidelines

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

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

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

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enable time stamps on debugging messages, which show the elapsed time since the networking device last rebooted:

```
RP/0/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
```

```
RP/0/RP0/CPU0:router(config)# service timestamps log datetime year
```

severity

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

severity {*severity*}
no severity

Syntax Description

severity	Severity level for determining which messages are logged to the archive. Possible severity levels and their respective system conditions are listed under Table 1: Severity Levels for Messages, on page 15 in the "Usage Guidelines" section. The default is **informational**.

Command Default

Informational

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Table 1: Severity Levels for Messages, on page 15 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 EXEC mode.

show logging [{**local location** *node-id* | [**location** *node-id*] [**start** *month day hh* **:** *mm* **:** *ss*] [**process** *name*] [**string** *string*] [**end** *month day hh* **:** *mm* **:ss**]}]

Syntax Description

end *month day hh* **:** *mm* **:** *ss*	(Optional) Displays syslog messages with a time stamp equal to or lower than the time stamp specified with the *monthday hh* **:** *mm* **:** *ss* argument. The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are as follows: • *month*—The month of the year. The values for the *month* argument are: • january • february • march • april • may • june • july • august • september • october • november • december • *day*—Day of the month. Range is 01 to 31. • *hh* **:**—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is 00 to 59.
local location *node-id*	(Optional) Displays system logging (syslog) messages from the specified local buffer. The *node-id* argument is entered in the *rack/slot/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.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	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 3: 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 5	Clears messages from the logging buffer.

show logging history

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

show logging history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	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 30 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 32 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 4: 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.

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

Related Commands

Command	Description
logging history, on page 30	Changes the severity level of syslog messages stored in the history file and sent to the SNMP server.
logging history size, on page 32	Changes the number of syslog messages that can be stored in the history table.

terminal monitor

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

terminal monitor [**disable**]

Syntax Description

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

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 2.0	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 38 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 38	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
```