A through Z Commands

logging alarm

To enable the system to send alarm messages to logging devices and to configure the alarm severity threshold, use the logging alarm command in global configuration mode. To prevent the system from sending alarm messages to a logging device, use the **no** form of this command.

logging alarm [*severity*]

no logging alarm [*severity*]

Syntax Description

severity	Specifies the alarm severity threshold for generating alarm messages. All alarms at and above the specified threshold generate alarm messages. One of the following values: • 1 or critical—Service-affecting condition. • 2 or major—Immediate action needed. • 3 or minor—Minor warning conditions. • 4 or informational--Informational messages.

Command Default

Alarm messages are not sent to a logging device.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

All alarms at and above the specified threshold generate alarm messages. If alarm severity is not specified, alarm messages for all alarm severity levels are sent to logging devices.

Examples

The following example sends messages only about critical alarms to logging devices:

```
Router(config)# logging alarm 1
```

The following example sends messages about major and critical alarms to logging devices:

```
Router(config)# logging alarm major
```

Related Commands

Command	Description
show facility-alarm	Displays the status of a generated alarm.

logging buffered

To enable system message logging to a local buffer, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. To return the buffer size to its default value, use the **default** form of this command.

logging buffered [**discriminator** *discriminator-name*] [*buffer-size*] [*severity-level*]

no logging buffered

default logging buffered

Syntax Description

discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discriminator-name	(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
buffer-size	(Optional) Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.
severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**—Warning conditions [[**5** | **notifications**]—Normal but significant conditions [[**6** | **informational**]—Informational messages [[**7** | **debugging**]—Debugging messages The default logging level varies by platform but is generally 7. Level 7 means that messages at all levels (0-7) are logged to the buffer. **Note** Every time you set the desired buffer severity level, the buffer size is set to default. Therefore, enter the value for the buffer size after setting the buffer severity level.

Command Default Varies by platform. For most platforms, logging to the buffer is disabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1(17)T	The *severity-level* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discriminator-name* argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50SY.

Usage Guidelines This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a severity-level causes messages at that level and numerically lower levels to be logged in an internal buffer.

The optional **discriminator** keyword and *discriminator-name* argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.

When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. To prevent the router from running out of memory, do not make the buffer size too large. You can use the **show memory** EXEC command to view the free processor memory on the router; however, the memory value shown is the maximum available and should not be approached. The **default logging buffered** command resets the buffer size to the default for the platform.

Note On Catalyst 6500 standalone switches and Catalyst 6500 virtual switches, the default logging buffered size is 8192.

To display messages that are logged in the buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer.

The **show logging** command displays the addresses and levels associated with the current logging setup and other logging statistics.

The table below shows a list of levels and corresponding syslog definitions.

Table 1: Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Examples

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

The following example shows how to use a message discriminator named buffer1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging buffered discriminator buffer1 critical
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging buffered xml	Enables system message logging (syslog) and sends XML-formatted logging messages to the XML-specific system buffer.
show logging	Displays the syslog.

logging buffered filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to the standard syslog buffer, use the **logging buffered filtered** command in global configuration mode. To disable all logging to the buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered filtered [*severity-level*]

no logging buffered filtered

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**] —Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged.

Command Default

Logging to the buffer is enabled.

ESM filtering of system logging messages sent to the buffer is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before filtered output can be sent to the buffer.

When ESM filtering is enabled, all messages sent to the buffer have the configured syslog filter modules applied. To return to standard logging to the buffer, use the plain form of the **logging buffered** command (without the **filtered** keyword). To disabled all logging to the buffer, use the **no logging buffered** command, with or without the **filtered** keyword.

The buffer is circular, so newer messages overwrite older messages as the buffer is filled. To change the size of the buffer, use the **logging buffered** *buffer-size* command, then issue the **logging buffered filtered** command to start (or restart) filtered logging.

To display the messages that are logged in the buffer, use the **show logging** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

The following example shows how to enable ESM filtered logging to the buffer:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging buffer filtered
```

Related Commands

Command	Description
clear logging	Clears all messages from the system message logging (syslog) buffer.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.

Command	Description
logging filter	Specifies the name and location of a syslog filter module to be applied to generated system logging messages.
logging on	Globally controls (enables or disables) system message logging.
show logging	Displays the state of system message logging, followed by the contents of the logging buffer.

logging buffered xml

To enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer, use the **logging buffered xml** command in global configuration mode . To disable the XML syslog buffer and return the size of the buffer to the default, use the **no** form of this command.

logging buffered xml [*xml-buffer-size*]

no logging buffered xml [*xml-buffer-size*]

Syntax Description

xml-buffer-size	(Optional) Size of the buffer, from 4,096 to 4,294,967,295 bytes (4 kilobytes to 2 gigabytes). The default size varies by platform. This value is ignored if entered as part of the **no** form of this command.

Command Default

XML formatting of system logging messages is disabled.

The default XML syslog buffer size is the same size as the standard syslog buffer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Standard logging is enabled by default, but XML-formatted system message logging is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered xml** command.

The **logging buffered xml** command copies logging messages to an internal XML buffer. The XML syslog buffer is separate from the standard syslog buffer (created using the **logging buffered** command).

The buffer is circular, so newer messages overwrite older messages as the buffer is filled.

The severity level for logged messages is determined by the setting of the **logging buffered** command. If the **logging buffered** command has not been used, the default severity level for that command is used. The default

severity level varies by platform, but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. For more information on severity levels, see the documentation of the **logging buffered** command.

When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** command in EXEC mode to view the free processor memory on the router; however, this value is the maximum available and should not be approached.

To return the size of the XML logging buffer to the default, use the **no logging buffered xml** command.

To display the messages that are logged in the buffer, use the **show logging xml** command in EXEC mode. The first message displayed is the oldest message in the buffer.

Examples

In the following example, the user enables logging to the XML syslog buffer and sets the XML syslog buffer size to 14 kilobytes:

```
Router(config)# logging buffered xml 14336
```

Related Commands

Command	Description
clear logging xml	Clears all messages from the XML-specific system message logging (syslog) buffer.
logging buffered	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
logging on	Globally controls (enables or disables) system message logging.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

logging cns-events

To enable extensible markup language (XML)-formatted system event message logging to be sent through the Cisco Networking Services (CNS) event bus, use the **logging cns-events** command in global configuration mode. To disable the ability to send system logging event messages through the CNS event bus, use the **no** form of this command.

logging cns-events [*severity-level*]

no logging cns-events

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**] **—**System is unusable [**1** | **alerts**]**—**Immediate action needed [**2** | **critical**]**—**Critical conditions [**3** | **errors**]**—**Error conditions [**4** | **warnings**]**—**Warning conditions [**5** | **notifications**]**—**Normal but significant conditions [**6** | **informational**]**—**Informational messages [**7** | **debugging**]**—**Debugging messages

Command Default

Level 7: debugging

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Before you configure this command you must enable the CNS event agent with the **cns event** command because the CNS event agent sends out the CNS event logging messages. The generation of many CNS event logging messages can negatively impact the publishing time of standard CNS event messages that must be sent to the network.

If the **debug cns event** command is active when the **logging cns-events** command is configured, the logging of CNS events is disabled.

Examples

In the following example, the user enables XML-formatted CNS system error message logging to the CNS event bus for messages at levels 0 through 4:

```
Router(config)# logging cns-events 4
```

Related Commands

Command	Description
cns event	Configures CNS event gateway, which provides CNS event services to Cisco IOS clients.
debug cns event	Displays CNS event agent debugging messages.

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console [**discriminator** *discr-name*] [*severity-level*]

no logging console

Syntax Description

discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages Level 7 is the default.

Command Default

The default varies by platform. In general, the default is to log all messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **logging console** command includes all the TTY lines in the device, not only the console TTY. For example, if you are running the **debug ip rip** command from a Telnet session to a VTY TTY on a router and you configure **no logging console**, the debugging messages will not appear in your Telnet command-line interface (CLI) session.

Specifying a level causes messages at that level and numerically lower levels to be sent to the console (TTY lines).

The optional **discriminator** keyword and *discr-name* argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.

Caution The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup and other logging statistics.

The table below shows a list of levels and corresponding syslog definitions.

Table 2: Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO

Level	Level Keyword	Syslog Definition
7	**debugging**	LOG_DEBUG

Note The behavior of the **log** keyword that is supported by some access lists such as IP extended, IP expanded, and IPX extended depends on the setting of the **logging console** command. The **log** keyword takes effect only if the logging console level is set to 6 or 7. If you change the default to a level lower than 6 and specify the **log** keyword with the **IP access list** (extended) command, no information is logged or displayed.

Examples

The following example shows how to change the level of messages sent to the console terminal (TTY lines) to **alerts**, meaning that messages at levels 0 and 1 are sent:

```
Router(config)# logging console alerts
```

The following example shows how to use a discriminator named msglog1 to filter alerts, meaning that messages at levels 0 and 1 are filtered:

```
Router(config)# logging console discriminator msglog1 alerts
```

Related Commands

Command	Description
access-list (extended)	Defines an extended XNS access list.
logging facility	Configures the syslog facility in which error messages are sent.

logging console filtered

To enable Embedded Syslog Monitor (ESM) filtered system message logging to the console connections, use the **logging console filtered** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

logging console filtered [*severity-level*]

no logging console

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged.

Command Default

Logging to the console is enabled.

ESM filtering of system logging messages sent to the console is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging console filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the console have the configured syslog filter modules applied. To disable filtered logging to the console and return to standard logging, use the standard **logging console** command (without the **filtered**keyword). To disable all logging to the console, use the **no logging console** command, with or without the **filtered** keyword.

Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging console filtered 3
```

Related Commands

Command	Description
logging console	Enables standard system message logging (syslog) to all console (CTY) connections and sets the severity level.
logging filter	Specifies the name and location of a syslog filter module to be applied to generated system logging messages.
logging on	Globally controls (enables or disables) system message logging.
show logging	Displays the state of system message logging, followed by the contents of the logging buffer.

logging console guaranteed

To guarantee the system message logging to the console, use the **logging console guaranteed** command in global configuration mode. To disable guaranteed logging to the console, use the **no** form of this command.

logging console guaranteed

no logging console guaranteed

Syntax Description

This command has no arguments or keywords.

Command Default

Guaranteed logging to the console is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Guaranteed output of debugging information is useful. By default, guaranteed system message logging to the console is enabled.

If the amount of console debugging is too large, Cisco IOS software will periodically stop all functions except providing the debug message output. This guaranteed output of debugging information can be useful, but it can also cause certain time-critical functions of Cisco IOS software to fail. To disable the guarantee of console logging, use the **no** form of the command.

Note Guaranteed console logging is not applicable to syslog.

Examples

The following example shows how to enable the guaranteed console logging:

```
Router(config)# logging console guaranteed
```

Related Commands

Command	Description
logging console	Enables standard system message logging (syslog) to all console (TTY) connections and sets the severity level.
show logging	Displays the state of system message logging, followed by the contents of the logging buffer.

logging console xml

To enable XML-formatted system message logging to the console connections, use the **logging console xml** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

logging console xml [*severity-level*]

no logging console xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages

Command Default

Logging to the console is enabled.

XML-formatted logging to the console is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To return system logging messages to standard text (without XML formatting), issue the standard **logging console** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4:

```
Router(config)# logging console xml 4
```

Related Commands

Command	Description
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging count

To enable the error log count capability, use the **logging count** command in global configuration mode. To disable the error log count capability, use the **no** form of this command.

logging count

no logging count

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging count** command counts every syslog message and time-stamps the occurrence of each message.

Examples

In the following example, syslog messages are logged to the system buffer and the logging count capability is enabled:

```
Router(config)# logging buffered notifications
Router(config)# logging count
Router(config)# end
Router# show logging count

Facility       Message Name                     Sev Occur   Last Time

================================================================================
SYS            BOOTTIME                          6    1     00:00:12
SYS            RESTART                           5    1     00:00:11
SYS            CONFIG_I                          5    3     1d00h
-------------  -------------------------------  ------------------------------
SYS TOTAL                                              5
LINEPROTO      UPDOWN                            5   13 00:00:19
-------------  -------------------------------  ------------------------------
LINEPROTO TOTAL                                       13
LINK           UPDOWN                            3    1 00:00:18
LINK           CHANGED                           5   12 00:00:09
```

```
-------------  --------------------------------  ------------------------------
LINK TOTAL                                             13
SNMP           COLDSTART                          5    1 00:00:11
-------------  --------------------------------  ------------------------------
SNMP TOTAL
```

Related Commands

Command	Description
show logging	Displays the state of system logging (syslog).

logging discriminator

To create a syslog message discriminator, use the **logging discriminator** command in global configuration mode. To disable the syslog message discriminator, use the **no** form of this command.

logging discriminator *discr-name* [**[facility] [mnemonics] [msg-body]** {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num*| **includes** *sev-num*}] [**rate-limit** *msglimit*]

no logging discriminator *discr-name*

Syntax Description

discr-name	String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
facility	(Optional) Message subfilter for the facility pattern in an event message.
mnemonics	(Optional) Message subfilter for the mnemonic pattern in an event message.
msg-body	(Optional) Message subfilter for the msg-body pattern in an event message.
drops	Drops messages that match the pattern, including the specified regular expression.
includes	Delivers messages that match the pattern, including the specified regular expression string.
string	(Optional) Expression used for message filtering.
severity	(Optional) Message subfilter by severity level or group.
sev-num	(Optional) Integer that identifies the severity level or multiple levels. Multiple levels must be separated with a comma (,).
rate-limit	(Optional) Specifies a number of messages to be processed within a unit of time.
msglimit	(Optional) Integer in the range of 1 to 10000 that identifies the number of messages not to be exceeded.

Command Default

The logging discriminator function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you enter a discriminator name that was previously specified, your entry is treated as a modification to the discriminator. The modification becomes effective when the configuration is completed. All associated sessions will use the modified value. When you remove a discriminator, the associations of all entries in the logging host list are removed.

When you issue the**no logging discriminator** command and the discriminator name is not found, an error message is generated. If the discriminator name is valid and actively associated with syslog sessions, the effect is immediate; the next syslog message to be processed will go through.

Subfilters are checked in the following order. If a message is dropped by any of the subfilters, the remaining checks are skipped.

1. Severity level or levels specified
2. Facility within the message body that matches a regular expression
3. Mnemonic that matches a regular expression
4. Part of the body of a message that matches a regular expression
5. Rate-limit

Examples

The following example shows how to enable the logging discriminator named msglog01 to filter messages with a severity level of 5.

```
Router(config)# logging discriminator msglog01 severity includes 5
```

Related Commands

Command	Description
logging monitor	Enables system message logging to the terminal lines (monitor connections).

logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** command in global configuration mode. To revert to the default of **local7**, use the **no** form of this command.

logging facility *facility-type*

no logging facility

Syntax Description

facility-type	Syslog facility. See the "Usage Guidelines" section of this command reference entry for descriptions of acceptable keywords.

Command Default

local7

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The table below describes the acceptable keywords for the *facility-type* argument.

Table 3: logging facility facility-type Argument

Facility-type keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for locally defined messages

Facility-type keyword	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

Examples

In the following example, the user configures the syslog facility to the kernel facility type:

```
Router(config)# logging facility kern
```

Related Commands

Command	Description
logging console	Limits messages logged to the console based on severity.

logging filter

To specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), use the **logging filter** command in global configuration mode. To remove a module from the filter chain, use the **no** form of this command.

logging filter *filter-url* [*position*] [**args** *filter-arguments*]

no logging filter *filter-url*

Syntax Description

filter-url	Specifies the location of the syslog filter module (script file), using the standard Cisco IOS File System URL syntax. • The location can be a local memory location, such as **flash:** or **slot0:**, or a remote file server system, such as **tftp:**, **ftp:**, or **rcp:**. • The *filter-url* should include the name of the syslog filter module, such as email.tcl or email.txt.
position	(Optional) An integer that specifies the order in which the syslog filter modules should be executed. The valid value for this argument is *n* + 1, where *n* is the current number of configured filters. • If this argument is omitted, the specified module will be positioned as the last module in the chain (the *n*th+1 position).
args *filter-arguments*	(Optional) Adds values to be passed by the ESM file chain. The ESM filter modules will determine what arguments you should use.

Command Default

No ESM filters are applied to system logging messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.

Release	Modification
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to enable the Embedded Syslog Manager by specifying the filter that should be applied to logging messages generated by the system. Repeat this command for each syslog filter module that should be used.

Syslog filter modules are Tool Command Language (Tcl) script files. These files can be stored as plain text files (.txt) or as precompiled Tcl scripts (.tcl). When you position (order) the modules, remember that the output of each filter module is used as input for the next filter module in the chain.

Note Cisco 1921, 1905, and 1906C Series Routers do not support **flash** for the location of the syslog filter module.

By default, syslog filter modules are executed in the order in which they appear in the system configuration file. The *position* argument can be used to order the filter modules manually. You can also reorder the filter modules at any time by reentering the **logging filter** command and specifying a different position for a given filter module.

The optional **args** *filter-arguments* syntax can be added to pass arguments to the specified filter. Multiple arguments can be specified. The number and type of arguments should be defined in the syslog filter module. For example, if the syslog filter module is designed to accept a specific e-mail address as an argument, you could pass the e-mail address using the **args user@host.com** syntax. Multiple arguments are typically delimited by spaces.

To remove a module from the list of modules to be executed, use the **no** form of this command. Modules not referenced in the configuration will not be executed, regardless of their “position” number.

Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Device(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Device(config)# logging filter slot0:/email.tcl user@example.com
Device(config)# logging filter slot0:/email_guts.tcl
Device(config)# logging console filtered 3
```

Related Commands

Command	Description
logging buffer filtered	Enables ESM filtered system message logging to the system logging buffer.
logging console filtered	Enables ESM filtered system message logging to all console connections.
logging host	Enables system message logging to a remote host (syslog collector).
logging monitor filtered	Enables ESM filtered system message logging to all monitor (TTY) connections.
show logging	Displays the status of system message logging, followed by the contents of the logging buffer.

logging history

To limit syslog messages sent to the router's history table and to an SNMP network management station based on severity, use the **logging history** command in global configuration mode . To return the logging of syslog messages to the default level, use the **no** form of this command with the previously configured severity level argument.

logging history [*severity-level-name*| *severity-level-number*]

no logging history [*severity-level-name*| *severity-level-number*]

Syntax Description

severity-level-name	Name of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.
severity-level-number	Number of the severity level. Specifies the lowest severity level for system error message logging. See the "Usage Guidelines" section of this command for available keywords.

Command Default

Logging of error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher."

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The sending of syslog messages to an SNMP network management station (NMS) occurs when you enable syslog traps with the **snmp-server enable traps syslog** global configuration mode command.

Because SNMP traps are potentially unreliable, at least one syslog message, the most recent message, is stored in a history table on the router. The history table, which contains table size, message status, and message text

data, can be viewed using the **show logging history** command. The number of messages stored in the table is governed by the **logging history size** global configuration mode command.

Severity levels are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a *level* causes messages at that severity level and numerically lower levels to be stored in the router's history table and sent to the SNMP network management station. For example, specifying the level **critical** causes messages as the critical (3), alert (2), and emergency (1) levles to be saved to the logging history table.

The table below provides a description of logging severity levels, listed from higest severity to lowest severity, and the arguments used in the **logging history** command syntax. Note that you can use the level name or the level number as the *level* argument in this command.

Table 4: Syslog Error Message Severity Levels

Severity Level Name	Severity Level Number	Description	Syslog Definition
emergencies	**0**	System unusable	LOG_EMERG
alerts	**1**	Immediate action needed	LOG_ALERT
critical	**2**	Critical conditions	LOG_CRIT
errors	**3**	Error conditions	LOG_ERR
warnings	**4**	Warning conditions	LOG_WARNING
notifications	**5**	Normal but significant condition	LOG_NOTICE
informational	**6**	Informational messages only	LOG_INFO
debugging	**7**	Debugging messages	LOG_DEBUG

Examples

In the following example, the system is initially configured to the default of saving severity level 4 or higher. The **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Router# show logging history

Syslog History Table:10 maximum table entries,
! The following line shows that system-error-message-logging is set to the
! default level of “warnings” (4).
saving level warnings or higher
 23 messages ignored, 0 dropped, 0 recursion drops

 1 table entries flushed
 SNMP notifications not enabled
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up

    timestamp: 2766
```

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# logging history 1
Router(config)# snmp-server enable traps syslog

Router(config)# end
Router#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Router# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications enabled, 0 notifications sent
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Router#
```

Related Commands

Command	Description
logging history size	Sets the maximum number of syslog messages that can be stored in the router's syslog history table.
logging on	Controls (enables or disables) the logging of error messages.
show logging	Displays the state of system logging (syslog) and contents of the local logging buffer.
show logging history	Displays information about the system logging history table.
snmp-server enable traps syslog	Controls (enables or disables) the sending of SYSLOG MIB notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

logging history size

To change the number of syslog messages stored in the router's history table, use the **logging history size** command in global configuration mode. To return the number of messages to the default value, use the **no** form of this command.

logging history size *number*

no logging history size

Syntax Description

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

Command Default

One message

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the history table is full (that is, it contains the maximum number of message entries specified with the **logging history size** command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

Examples

In the following example, the user sets the number of messages stored in the history table to 20:

```
logging history size 20
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and the SNMP network management station based on severity.
show logging	Displays the state of logging (syslog).

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host {{*ip-address*| *hostname*} [**vrf** *vrf-name*]| **ipv6** {*ipv6-address*| *hostname*}} [**discriminator** *discr-name*| [**filtered** [**stream** *stream-id*]| **xml**]] [**transport** {[**beep [audit]** [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [*cipher-num*] **trustpoint** *trustpt-name*]]| **tcp [audit]| udp**} [**port** *port-num*]] **[sequence-num-session]** [**session-id** {**hostname| ipv4| ipv6**| **string** *custom-string*}]

no logging host {{*ip-address*| *hostname*}| **ipv6** {*ipv6-address*| *hostname*}}

Syntax Description

ip-address	IP address of the host that will receive the system logging (syslog) messages.
hostname	Name of the IP or IPv6 host that will receive the syslog messages.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding instance (VRF) that connects to the syslog server host. Name of the VRF that connects to the syslog server host.
ipv6	Indicates that an IPv6 address will be used for a host that will receive the syslog messages.
ipv6-address	IPv6 address of the host that will receive the syslog messages.
discriminator *discr-name*	(Optional) Specifies a message discriminator for the session. Name of the message discriminator.
filtered	(Optional) Specifies that logging messages sent to this host should first be filtered by the Embedded Syslog Manager (ESM) syslog filter modules specified in the **logging filter** commands.
stream *stream-id*	(Optional) Specifies that only ESM filtered messages with the stream identification number specified in the *stream-id* argument should be sent to this host. Number from 10 to 65535 that identifies the message stream.
xml	(Optional) Specifies that the logging output should be tagged using the XML tags defined by Cisco.

transport	(Optional) Method of transport to be used. UDP is the default.
beep	(Optional) Specifies that the Blocks Extensible Exchange Protocol (BEEP) transport will be used.
audit	(Optional) Available only for BEEP and TCP. When the **audit** keyword is used, the specified host is identified for firewall audit logging.
channel *chnl-number*	(Optional) Specifies the BEEP channel number to use. Number of the BEEP channel. Valid values are 1, 3, 5, 7, 9, 11, 13, and 15. The default is 1.
sasl	(Optional) Applies the Simple Authentication and Security Layer (SASL) BEEP profile.
profile-name	(Optional) Name of the SASL profile.
tls cipher	(Optional) Specifies the cipher suites to be used for a connection. Cipher suites are referred to by mask values. Multiple cipher suites can be chosen by adding the mask values. The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.
cipher-num	(Optional) Integer from 32 to 224 that is the mask value of a cipher suite (sum of up to three numbers: 32, 64, and 128) and refers to the following: • ENC_FLAG_TLS_RSA_WITH_NULL_SHA - 32 • ENC_FLAG_TLS_RSA_WITH_RC4_128_MD5 - 64 • ENC_FLAG_TLS_RSA_WITH_AES_128_CBC_SHA - 128 The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images.
trustpoint *trustpt-name*	(Optional) Specifies a trustpoint for identity information and certificates. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images. Name of the trustpoint. If you previously declared the trustpoint and want only to update its characteristics, specify the name you previously created. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.

tcp	(Optional) Specifies that the TCP transport will be used.
udp	(Optional) Specifies that the UDP transport will be used.
port *port-number*	(Optional) Specifies that a port will be used. Integer from 1 through 65535 that defines the port. If a port number is not specified, the standard Cisco default port number for TCP is 601, for BEEP is 601, and for UDP is 514.
sequence-num-session	(Optional) Includes a session sequence number tag in the syslog message.
session-id	(Optional) Specifies syslog message session ID tagging.
hostname	Includes the hostname in the session ID tag.
ipv4	Includes the logging source IP address in the session ID tag.
ipv6	Includes the logging source IPv6 address in the session ID tag.
string *custom-string*	Includes the custom string in the session ID tag. Custom string in the s_id="custom_string" tag.

Command Default

System logging messages are not sent to any remote host. When this command is entered without the **xml** or **filtered** keyword, messages are sent in the standard format.

Command Modes

Global configuration (config)

Command History

T Release	Modification
10.0	The **logging** command was introduced.
12.2(15)T	The **logging host** command replaced the **logging** command. The **xml** keyword was added.
12.3(2)T	The **filtered** [**stream**] *stream-id* syntax was added as part of the ESM feature.
12.3(14)T	The **transport** keyword was added.

T Release	Modification
12.4(4)T	The **ipv6** *ipv6-address* keyword-argument pair was added.
12.4(11)T	Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument was added.
S Release	**Modification**
12.0(14)S	The **logging host** command replaced the **logging** command.
12.0(14)ST	The **logging host** command replaced the **logging** command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S and the **vrf** *vrf-name* keyword-argument pair was added.
SR Release	**Modification**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **vrf** *vrf-name* and **xml** keywords were supported.
SX Release	**Modification**
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. Support was added for **vrf** *vrf-name* and **xml** keywords and argument.
12.2(33)SXI	Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument were added.
XE Release	**Modification**
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
SB Release	**Modification**
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. Support was added for the **vrf** *vrf-name* and **xml** keywords and argument.
12.2(31)SB2	This command was implemented on the Cisco 10000 series routers. Support was added for the **vrf** *vrf-name* and **xml** keywords and argument.

Usage Guidelines

Standard system logging is enabled by default. If logging is disabled on your system (using the **no logging on** command), you must enter the **logging on** command to reenable logging before you can use the **logging host** command.

The **logging host** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

Use the **vrf** *vrf-name* keyword and argument to enable a syslog client (a provider edge [PE] router) to send syslog messages to a syslog server host connected through a VRF interface. To delete the configuration of the syslog server host from the VRF, use the **no logging host** command with the **vrf** *vrf-name* keyword and argument.

When XML-formatted syslog is enabled using the **logging host** command with the **xml** keyword, messages are sent to the specified host with the system-defined XML tags. These tags are predefined and cannot be configured by a user. XML formatting is not applied to debug output.

If you are using the ESM feature, you can enable ESM-filtered syslog messages to be sent to one or more hosts using the **logging host filtered** command. To use the ESM feature, you must first specify the syslog filter modules that should be applied to the messages using the **logging filter** command. See the description of the **logging filter** command for more information about the ESM feature.

Note ESM and message discriminator usage is mutually exclusive in a given syslog session.

Using the BEEP transport protocol, you can have reliable and secure delivery for syslog messages and configure multiple sessions over eight BEEP channels. The **sasl** *profile-name*, **tls cipher** *cipher-num*, **trustpoint** *trustpt-name* keywords and arguments are available only in crypto images.

To configure standard logging to a specific host after configuring XML-formatted or ESM-filtered logging to that host, use the **logging host** command without the **xml** or **filtered** keyword. Issuing the standard **logging host** command replaces an XML- or ESM-filtered **logging host** command, and vice versa, if the same host is specified.

You can configure the system to send standard messages to one or more hosts, XML-formatted messages to one or more hosts, and ESM-filtered messages to one or more hosts by repeating this command as many times as desired with the appropriate syntax. (See the “Examples” section.)

When the **no logging host** command is issued with or without the optional keywords, all logging to the specified host is disabled.

Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) (**logging trap** command severity levels) are logged to a host at 192.168.202.169:

```
Router(config)# logging host 192.168.202.169

Router(config)# logging trap 5
```

In the following example, standard system logging messages are sent to the host at 192.168.200.225, XML-formatted system logging messages are sent to the host at 192.168.200.226, ESM-filtered logging messages with the stream 10 value are sent to the host at 192.168.200.227, and ESM-filtered logging messages with the stream 20 value are sent to host at 192.168.202.129:

```
Router(config)# logging host 192.168.200.225

Router(config)# logging host 192.168.200.226 xml

Router(config)# logging host 192.168.200.227 filtered stream 10

Router(config)# logging host 192.168.202.129 filtered stream 20
```

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF named vpn1:

```
Router(config)# logging host 172.16.150.63 vrf vpn1
```

In the following example, the default UDP on an IPv6 server is set because no port number is specified. The default port number of 514 is used:

```
Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF
```

In the following example, TCP port 1774 on an IPv6 server is set:

```
Router(config)# logging host ipv6 BBBB:CCCC:DDDD:FFFF::1234 transport tcp port 1774
```

In the following example, the UDP port default is used on an IPv6 server with a hostname of v6-hostname:

```
Router(config)# logging host ipv6 v6-hostname transport udp port 514
```

In the following example, a message discriminator named fltr1 is specified along with the BEEP protocol for port 600 and channel 3.

```
Router(config)# logging host host2 dicriminator fltr1 transport beep channel 3 port 600
```

Related Commands

Command	Description
logging filter	Specifies a syslog filter module to be used by the ESM.
logging on	Globally controls (enables or disables) system message logging.
logging trap	Limits messages sent to the syslog servers based on severity level.
show logging	Displays the state of system message logging, followed by the contents of the standard syslog buffer.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging linecard

To log messages to an internal buffer on a line card, use the **logging linecard** command in global configuration mode. To cancel the use of the internal buffer on the line cards, use the **no** form of this command.

logging linecard [*size*| *level*]

no logging linecard

Syntax Description

size	(Optional) Size of the buffer used for each line card. The range is from 4096 to 65,536 bytes. The default is 8 KB.
level	(Optional) Limits the logging of messages displayed on the console terminal to a specified level. The message level can be one of the following: • **alerts —**Immediate action needed • **critical —**Critical conditions • **debugging —**Debugging messages • **emergencies —**System is unusable • **errors —**Error conditions • **informational —**Informational messages • **notifications —**Normal but significant conditions • **warnings —**Warning conditions

Command Default

The Cisco IOS software logs messages to the internal buffer on the GRP card.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 series Gigabit Switch Routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specifying a message level causes messages at that level and numerically lower levels to be stored in the internal buffer on the line cards.

The table below lists the message levels and associated numerical level. For example, if you specify a message level of critical, all critical, alert, and emergency messages will be logged.

Table 5: Message Levels

Level Keyword	Level
emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

To display the messages that are logged in the buffer, use the **show logging slot** EXEC command. The first message displayed is the oldest message in the buffer.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** EXEC command to view the free processor memory on the router; however, this is the maximum available and should not be approached.

Examples

The following example enables logging to an internal buffer on the line cards using the default buffer size and logging warning, error, critical, alert, and emergency messages:

```
Router(config)# logging linecard warnings
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
show logging	Displays the state of logging (syslog).

logging message-counter

To enable logging of debug, log, or syslog messages, use the **logging message-counter** command in global configuration mode. To disable logging for these message types, use the **no** form of this command.

logging message-counter {**debug**| **log**| **syslog**}

no logging message-counter {**debug**| **log**| **syslog**}

Syntax Description

debug	Enables the debug information message counter, which is a counter of accumulated debug information messages received by the logger.
log	Enables all message counters of accumulated logging messages received by the logger.
syslog	Enables the syslog message counter, which is a counter of current lines of syslog messages sent. This counter is enabled by default.

Command Default

The logging message counter function is disable d.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to help identify where event messages are being dropped because of rate limiting or to exclude the syslog counter from a syslog message.

Examples

The following example shows how to enable the syslog message counter:

```
Router(config)# logging message-counter syslog
```

logging monitor

To enable system message logging to the terminal lines (monitor connections), use the **logging monitor**command in global configuration mode. To disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor [**discriminator** *discr-name*] [*severity-level*]

no logging monitor

Syntax Description

discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages Level 7 is the default.

Command Default

The logging monitor function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Specifying a severity-level causes messages both at that level and at numerically lower levels to be displayed to the monitor. The table below shows a list of levels and corresponding syslog definitions.

Table 6: Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Examples

The following example shows how to specify that messages at levels 3 (errors), 2 (critical), 1 (alerts), and 0 (emergencies) be logged to monitor connections:

```
Router(config)# logging monitor 3
```

The following example shows how to use a discriminator named monitor1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging monitor discriminator monitor1 critical
```

Related Commands

Command	Description
logging monitor filtered	Enables ESM filtered system message logging to monitor connections.
logging monitor xml	Applies XML formatting to messages logged to the monitor connections.
terminal monitor	Displays **debug** command output and system error messages for the current terminal and session.

logging monitor filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to monitor connections, use the **logging monitor filtered** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor filtered [*severity-level*]

no logging monitor filtered

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged.

Command Default

Logging to monitor connections is enabled.

ESM filtering of system logging messages sent to the monitor connections is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **monitor** keyword specifies the TTY (TeleTYpe) line connections at all line ports. TTY lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a TTY connection is a PC with a terminal emulation program connected to the device using a dialup modem, or a Telnet connection.

Standard logging is enabled by default, but filtering by the ESM is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging monitor filtered** command.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the monitor have the configured syslog filter modules applied. To disable filtered logging to the monitor and return to standard logging, issue the standard **logging monitor** command (without the **filtered** keyword). To disable all logging to the monitor connections, use the **no logging monitor** command, with or without the **filtered** keyword.

Examples

The following example shows how to enable ESM filtered logging to the monitor connections:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging monitor filtered
```

Related Commands

Command	Description
logging monitor	Enables standard system message logging to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging monitor xml

To enable XML-formatted system message logging to monitor connections, use the **logging console xml** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor xml [*severity-level*]

no logging monitor xml

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages

Command Default

Logging to monitor connections is enabled.

XML-formatted logging to monitor connections is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **monitor** keyword specifies the tty line connections at all line ports. The tty lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a tty connection is a PC with a terminal emulation program connected to the device using a dial-up modem, or a Telnet connection.

To return system logging messages to standard text (without XML formatting), issue the standard **logging monitor** command (without the **xml** keyword extension).

Examples

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4 and XML-formatted system message logging to tty line connections at the default severity level:

```
Router(config)# logging console xml 4
Router(config)# logging monitor xml
```

Related Commands

Command	Description
logging monitor	Enables system message logging in standard (plain text) format to all monitor (TTY) connections.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

logging on

To enable logging of system messages, use the **logging on** command in global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

logging on

no logging on

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco IOS software sends messages to the asynchronous logging process.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or syslog server. System logging messages are also known as system error messages. You can turn logging on and off for these destinations individually using the **logging buffered**, **logging monitor**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. Only the console will receive messages.

Additionally, the logging process logs messages to the console and the various destinations after the processes that generated them have completed. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

Caution Disabling the logging on command may substantially slow down the router. Any process generating debug or error messages will wait until the messages have been displayed on the console before continuing.

The **logging synchronous** line configuration command also affects the displaying of messages to the console. When the **logging synchronous** command is enabled, messages will appear only after the user types a carriage return.

Examples

The following example shows command output and message output when logging is enabled. The ping process finishes before any of the logging information is printed to the console (or any other destination).

```
Router(config)# logging on
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# ping dirt

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
Router#
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
```

In the following example, logging is disabled. The message output is displayed as messages are generated, causing the debug messages to be interspersed with the message “Type escape sequence to abort.”

```
Router(config)# no logging on
Router(config)# end
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router# ping dirt

IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingTyp
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1e
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sending esc
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingape
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingse
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1
IP: s=172.21.96.41 (local), d=172.16.1.129 (Ethernet1/0), len 100, sendingquen
IP: s=171.69.1.129 (Ethernet1/0), d=172.21.96.41, len 114, rcvd 1ce to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/152/156 ms
Router#
```

Related Commands

Command	Description
logging host	Logs messages to a syslog server host.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

logging origin-id

To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

logging origin-id {**hostname| ip| ipv6| string** *user-defined-id*}

no logging origin-id

Syntax Description

hostname	Specifies that the hostname will be used as the message origin identifier.
ip	Specifies that the IP address of the sending interface will be used as the message origin identifier.
ipv6	Specifies that the IPv6 address of the sending interface will be used as the message origin identifier.
string *user-defined-id*	Allows you to enter your own identifying description. The *user-defined-id* argument is a string you specify. • You can enter a string with no spaces or use delimiting quotation marks to enclose a string with spaces.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(1)	The **string** *user-defined-id* keyword-argument pair was added.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	The **ipv6** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, the IPv6 address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

When you specify your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces. For example:

```
Router(config)# logging origin-id string Cisco_Systems
```

To use spaces (multiple words) or additional syntax, enclose the string with quotation marks (“ ”). For example:

```
Router(config)# logging origin-id string "Cisco Systems, Inc."
```

Examples

In the following example, the origin identifier “Domain 1, router B” will be added to the beginning of all system logging messages sent to remote hosts:

```
Router(config)# logging origin-id string Domain 1, router B
```

In the following example, all logging messages sent to remote hosts will have the IP address configured for serial interface 1 added to the beginning of the message:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap 5
Router(config)# logging source-interface serial 1
Router(config)# logging origin-id ip
```

Related Commands

Command	Description
logging host	Enables system message logging to a remote host.
logging source-interface	Forces logging messages to be sent from a specified interface, instead of any available interface.
logging trap	Configures the severity level at or numerically below which logging messages should be sent to a remote host.

logging persistent

To enable the storage of logging messages on the router's advanced technology attachment (ATA) disk, use the **logging persistent** command in global configuration mode. To disable logging message storage on the ATA disk, use the **no** form of this command.

logging persistent[**batch** *batch-size*]{**filesize** *logging-file-size*}[**immediate**]{**notify**}[**protected**]{**size** *filesystem-size*}[**threshold** *threshold-capacity*[**alert**]][**url**{**disk0:**/*directory*| **disk1:**/*directory*}]

no logging persistent

Syntax Description

batch *batch-size*	(Optional) Specifies the batch size in bytes. • Minimum value is 4096. • Maximum value is the total amount of available disk space. • Default value is 4096.
filesize *logging-file-size*	(Optional) Specifies the size of individual logging files in bytes. • Minimum value is 8192. • Maximum value is the total amount of available disk space. • Default value is 262144.
immediate	(Optional) Writes a new audit record to the log file immediately.
notify	(Optional) Issues a notification when the logging persistent display is activated.
protected	(Optional) Eliminates manipulation on logging-persistent files.
size *filesystem-size*	(Optional) Specifies the amount of disk space, in bytes, allocated to syslog messages. • Minimum value is 16384. • Maximum value is the total amount of available disk space. • Default value is 10 percent of the total disk space.

threshold *threshold-capacity*	(Optional) Sets threshold, in percentage, for logging persistence. The threshold capacity ranges from 1 to 99. Default threshold capacity is 95.
alert	(Optional) Issues an audible signal when the threshold is exceeded.
url	(Optional) Specifies any supported local Cisco IOS file system location. The default URL is disk0:/syslog.
disk0: */directory*	Indicates the directory on disk 0 where syslog messages are saved. The colon and slash are required.
disk1: */directory*	Indicates the directory on disk 1 where syslog messages are saved. The colon and slash are required.

Command Default

The logging messages are not stored in the router's ATA memory.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(24)T	The **batch** keyword and *batch-size* argument were added.
Cisco IOS XE Release 2.4	This command was modified. The **immediate**, **notify**, **protected**, **threshold**, and **alert** keywords, and the *threshold-capacity* argument, were added.

Usage Guidelines

The **logging persistent** command enables the storage of syslog data on the router's ATA flash disk. Because the syslog data must be copied from the router's internal memory buffer, you must enable the **logging buffered** command prior to enabling the **logging persistent** command.

The filename format of log files is *log_MM:DD:YYYY::hh:mm:ss*. For example, *log_06:10:2008::07:42:14*. For Release 12.4(20)T and later releases, the filename format is changed to: *log_YYYYMMDD-hhmmss*. For example, log_20080610-074214.

Note Any filtering of syslog messages written to the router's internal memory buffer results in filtering of syslog messages written to the router's ATA flash disk.

Note The common criteria condition is specific to ASR 1000 Series Aggregation Services Routers. The **protected** keyword is supported on the ASR 1000 Series Aggregation Services Routers only.

In the common criteria compliant environment, the **logging persistent** command is accessible only to the administrator and the audit administrator. The common criteria restrict access to audit information, such as syslog records, to the administrator. The audit administrator alone is allowed to create a persistent logging repository and remove the log files. Use the **logging persistent protected** command to enable the protected mode of Cisco IOS logging subsystem operation. Once this operation is enabled, access to the persistent audit information is denied to the users of **copy**, **delete**, **more**, and **rename** generic Cisco IOS commands. The commands **format**, **erase**, and **partition** have no effect if audit information is present on the target device of these commands.

If the **immediate** keyword is specified, the syslog issues an instruction to immediately write the new audit entry to the log file. If the **immediate** keyword is not specified, the Cisco IOS peristent logging behavior does not change. By default, the unbuffered mode of operation is turned off.

If a threshold capacity value is not set, the logging policy adheres to a default circular behavior. When the log capacity is reached, the oldest log records are overwritten. Setting a threshold capacity value enables a lossless logging policy.

When the set threshold capacity is reached, the logger issues an alarm for the severity level set in the current logging policy and executes that current logging policy.

Use the **logging persistent notify** command to create audit trails for administrators who review the audit records. In the common criteria environment, only the administrator can use this command.

Examples

The following example shows how to write up to 134,217,728 bytes (128 MB) of logging messages to the syslog directory of disk 0, with a file size of 16,384 bytes and a batch size of 5098 bytes:

```
Router(config)# logging buffered
Router(config)# logging persistent url disk0:/syslog batch filesize 16384 5098 size 134217728
```

The following example shows how to enable protected mode of logging subsystem operation with a threshold capacity of 25 percent.

```
Router> enable
Router# configure terminal
Router(config)# logging persistent protected threshold 25
Router(config)# exit
```

The following example shows the error message being displayed if the user tries to copy files from and to the log directory when the protected mode is enabled on the logging subsystem:

```
Router# copy log__persistent_12_22_2007__06_44_05 xxx
%Error parsing filename (Unknown error 0)
```

Related Commands

Command	Description
logging buffered	Saves syslog messages in router memory.

logging persistent move

To move logging persistent files from one directory to another, use the **logging persistent move** command in privileged EXEC mode.

logging persistent move[**src-url** *filesystem***:**/*directory*]**dst-url** *filesystem***:**/*directory***verbose**

Syntax Description

src-url	(Optional) Specifies the source URL from where the files are moved.
filesystem **:**	Indicates the filesystem, followed by a colon.
/ *directory*	The directory on the filesystem. The slash is required.
dst-url	Specifies the destination URL to where the files are moved.
verbose	(Optional) Issues a notification every time the file is moved from source to destination.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

When an audit log is configured on a fixed memory device such as a hard disk or when physical access to the system is not available, the audit administrator can use the **logging persistent move** command to move files from the audit directory to a designated location. The **logging persistent move** command organizes the existing log files based on the time of creation and copies one log file at a time to the destination location. If no source location is specified, the log files are moved from the default source location. The default source destination can be specified by using the **logging persistent** command. The log file at the source destination is deleted after the copy is complete.

This command displays a syslog message when the archiving operation begins.

Examples

The following example shows how to move files from the default logging peristent directory to another directory:

```
Router# logging persistent move dst-url usb0:audit_log_1

 Move persistent logging files from usb0:/audit_log to usb0:/audit_log_1 ? [confirm]
000060: *Jul 26 06:18:17.428: %SYS-6-LOGGING_MOVE: User lab has activated the logging
```

```
persistent move command.
39 files out of 39 moved from usb0:/audit_log to usb0:/audit_log_1
```

The following example shows how to move files from the specified logging persistent directory to another directory:

```
Router# logging persistent move src-url usb0:audit_log_1 dst-url obfl:audit_log

 Move persistent logging files from usb0:/audit_log_1 to obfl:/audit_log ? [confirm]
000061: *Jul 26 06:45:40.691: %SYS-6-LOGGING_MOVE: User lab has activated the logging
persistent move command.
39 files out of 39 moved from usb0:/audit_log_1 to obfl:/audit_log
```

The following example shows how to move files from the source directory to the destination directory with the verbose option enabled:

```
Router# logging persistent move src-url obfl:audit_log dst-url obfl:audit_log_1 verbose

 Move persistent logging files from obfl:/audit_log to obfl:/audit_log_1 ? [confirm]
000062: *Jul 26 06:50:15.795: %SYS-6-LOGGING_MOVE: User lab has activated the logging
persistent move command.
File log_20090723-063200 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-065111 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-071610 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-102105 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-103316 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-110747 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-110928 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-111044 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
File log_20090723-111157 moved from obfl:/audit_log URL to obfl:/audit_log_1 URL.
9 files out of 9 moved from obfl:/audit_log to obfl:/audit_log_1
```

Related Commands

Command	Description
logging persistent	Enables the storage of logging messages on the router's ATA disk.

logging queue-limit

To control how much system memory may be used for queued log messages, use the **logging queue-limit** command in global configuration mode. To permit unlimited use of memory for queued log messages, use the **no** form of this command.

logging queue-limit [*queuesize*| **trap** *queuesize*| **esm** *queuesize*]

no logging queue-limit

Syntax Description

queuesize	(Optional) The number of messages in the logger queue. The valid range is 100 to 2147483647. The default is 100.
trap	(Optional) Specifies the limit for the number of log messages that may be queued for a remote system logging (syslog) server and sends the messages to a trap.
esm	(Optional) Specifies the limit for the number of log messages that may be queued for the Embedded Syslog Manager (ESM) subsystem. The size change to the ESM queue will take effect only if the ESM feature is supported in the image and an ESM filter has been configured.

Command Default

100 messages

The default logger queue size varies depending on the hardware platform and is set up by an internal function at run time. The default queue sizes in Cisco IOS Release 12.4(8) are listed as follows. These sizes are subject to change.

- Cisco Catalyst 6500 series switches—256 messages
- Cisco 7200 platform—250 messages
- Cisco AS5400 platform—200 messages
- All other Cisco platforms—100 messages

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(8)	This command was introduced.

Release	Modification
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The size of the logging queue affects system memory. In the logging queue, each message has its own memory object. The more messages being queued, the less memory is available for other components of the system to share.

Tuning the queue size is sometimes required when Cisco technical support staff needs to reduce the possibility that logging messages are dropped because the event messages are bursty. The **logging queue-limit** command is meant for use by Cisco technical support staff assisting on a field-critical case to ensure critical messages are not dropped because of a smaller default queue size.

Customers are discouraged from tuning the message queue size if they have not first contacted the Cisco Technical Support Center (TAC).

Caution When you are tuning the queue size to a larger value, no messages will be dropped. When you relax or remove limits on logger queueing, it is possible to adversely impact the system due to memory, CPU, or network exhaustion.

When the **logging queue-limit** command is used to reset the logging queue to the default size, it also resets the trap and ESM queues to their default sizes.

Examples

The following example sets the logging queue to the system default size:

```
Router(config)# logging queue-limit
```

The following example sets the logging queue to 1000 queue entries:

```
Router(config)# logging queue-limit 1000
```

The following example removes all logging queue limits:

```
Router(config)# no
 logging queue-limit
```

The following example sets the logging queue size at 1000 for messages sent to the ESM:

```
Router(config)# logging queue-limit esm 1000
```

The following example sets the logging queue size to 1000 for messages sent to an external syslog:

```
Router(config)# logging queue-limit trap 1000
```

Related Commands

Command	Description
logging rate-limit	Limits the rate of messages logged per second.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

Command	Description
logging trap	Limits messages logged to the syslog servers based on severity.
show logging	Displays the state of the syslog and the contents of the standard system logging buffer.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

logging rate-limit {**number**| **all number**| **console** {**number**| **all number**}} [**except severity**]

no logging rate-limit

Syntax Description

number	Number of messages to be logged per second. Valid values are 1 to 10000. The default is 10.
all	Sets the rate limit for all error and debug messages displayed at the console and printer.
console	Sets the rate limit for error and debug messages displayed at the console.
except *severity*	(Optional) Excludes messages of this severity level and lower. Valid levels are 0 to 7. Severity decreases as the number increases; therefore, severity level 1 indicates a problem more serious than a severity level 3.

Command Default

The default is 10 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging rate-limit** command controls the output of messages from the system. Use this command to avoid a flood of output messages. You can select the severity of the output messages and the output rate by using the **logging rate-limit** command. You can issue the **logging rate-limit** command at any time. System performance is not negatively affected and may improve when severities and rates of output messages are specified.

You can use **logging rate-limit** command with or without the **logging synchronous** line configuration command. For example, if you want to see all severity 0, 1, and 2 messages, use the **no logging synchronous** command and specify **logging rate-limit 10 except 2**. By using the two commands together, you cause all messages of 0, 1, and 2 severity to print and limit the less severe ones (higher number than 2) to only 10 per second.

The table below shows the numeric severity level, equivalent meaning in text, and a description for error messages.

Table 7: Error Message Severity Levels, Equivalent Text, and Descriptions

Numeric Severity Level	Equivalent Word	Description
0	**emergencies**	System unusable
1	**alerts**	Immediate action needed
2	**critical**	Critical conditions
3	**errors**	Error conditions
4	**warnings**	Warning conditions
5	**notifications**	Normal but significant condition
6	**informational**	Informational messages only
7	**debugging**	Debugging messages

Cisco 10000 Series Router

To avoid CPU overload and router instability, use the **logging rate-limit** command to limit the rate at which the Cisco 10000 series router logs system messages. To increase the Point-to-Point Protocol call rate, you can turn off console logging completely using the no logging console command.

Examples

The following example shows how to limit message output to 200 per second:

```
Router(config)# logging rate-limit 200
```

Related Commands

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.
no logging console	Disables syslog message logging to the console terminal.

logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface {**interface-name** *number* **vrf** *vrf-name*}

no logging source-interface{**interface-name** *number* **vrf** *vrf-name*}

Syntax Description

Interface-name *number*	Interface type and number.
vrf*vrf -name*	Provides logging source-interface setting capability to Virtual Routing and Forwarding (VRF) syslog destinations. Name assigned to the VRF.

Command Default

The wildcard interface address is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was modified. IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY. The **vrf** keyword and *vrf-name* argument were added

Usage Guidelines

This command can be configured on the VRF and non-VRF interfaces. Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets that contain the IPv4 or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

When no specific interface is configured, a wildcard interface address of 0.0.0.0 (for IPv4) or :: (for IPv6) is used, and the IP socket selects the best outbound interface.

Examples

The following example shows how to specify that the IP address of Ethernet interface 0 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0 vrf1
```

The following example shows how to specify the IP address for Ethernet interface 2/1 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1 vrf1
```

The following sample output displays that the **logging source-interface** command is configured on a VRF source interface:

```
Router# show running interface loopback49

             Building configuration...
             Current configuration : 84 bytes
             !
             interface Loopback49
              ip vrf forwarding vrf1
              ip address 10.4.2.39 255.0.0.0
             end
Router# show running | includes logging
      logging source-interface Loopback49 vrf1
      logging host 192.0.2.1 vrf1
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the **logging synchronous** command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the **no** form of this command.

logging synchronous [**level** *severity-level*| **all**] [**limit** *number-of-lines*]

no logging synchronous [**level** *severity-level*| **all**] [**limit** *number-of-lines*]

Syntax Description

level *severity-level*	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
all	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
limit *number-of-lines*	(Optional) Specifies the number of buffer lines to be queued for the terminal, after which new messages are dropped. The default value is 20.

Command Default

This command is disabled.

If you do not specify a severity level, the default value of 2 is assumed.

If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When synchronous logging of unsolicited messages and debug output is turned on, unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. This keeps unsolicited messages and debug output from being interspersed with solicited software output and prompts.

Tip This command is useful for keeping system messages from interrupting your typing. By default, messages will appear immediately when they are processed by the system, and the CLI cursor will appear at the end of the displayed message. For example, the line "Configured by console from console" may be printed to the screen, interrupting whatever command you are currently typing. The **logging synchronous** command allows you to avoid these potentially annoying interruptions without have to turn off logging to the console entirely.

When this command is enabled, unsolicited messages and debug output are displayed on a separate line than user input. After the unsolicited messages are displayed, the CLI returns to the user prompt.

Note This command is also useful for allowing you to continue typing when debugging is enabled.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.

When a message queue limit of a terminal line is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice "%SYS-3-MSGLOST *number-of-messages* due to overflow" follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.

Caution By configuring abnormally large message queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages could consume all available RAM. You should guard against this type of attack through proper configuration.

Examples

In the following example, a system message appears in the middle of typing the show running-config command:

```
Router(config-line)# end
Router# show ru
2w1d: %SYS-5-CONFIG_I: Configured from console by console
nning-config
 .
 .
 .
```

The user then enables synchronous logging for the current line (indicated by the * symbol in the **show line** command), after which the system displays the system message on a separate line, and returns the user to the prompt to allow the user to finish typing the command on a single line:

```
Router# show line
```

```
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      0       3     0/0       -
 .
 .
 .
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# line 0
Router(config-line)# logging syn
<tab>
Router(config-line)# logging synchronous

Router(config-line)# end

Router# show ru

2w1d: %SYS-5-CONFIG_I: Configured from console by console
Router# show running-config
```

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Router(config)# line 4
Router(config-line)# logging synchronous level 6
Router(config-line)# exit
Router(config)# line 2
Router(config-line)# logging synchronous level 7 limit 1000
Router(config-line)# end
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
logging on	Controls logging of error messages and sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode . To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap *level*

no logging trap

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0** | **emergencies**]—System is unusable [**1** | **alerts**]—Immediate action needed [**2** | **critical**]—Critical conditions [**3** | **errors**]—Error conditions [**4** | **warnings**]—Warning conditions [**5** | **notifications**]—Normal but significant conditions [**6** | **informational**]—Informational messages [**7** | **debugging**]—Debugging messages

Command Default

Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A trap is an unsolicited message sent to a remote network management host. Logging traps should not be confused with SNMP traps (SNMP logging traps require the use of the CISCO -SYSLOG-MIB, are enabled using the **snmp-server enable traps syslog** command, and are sent using the Simple Network Management Protocol.)

The **show logging** EXEC command displays the addresses and levels associated with the current logging setup. The status of logging to remote hosts appears in the command output as “trap logging”.

The table below lists the syslog definitions that correspond to the debugging message levels. Additionally, four categories of messages are generated by the software, as follows:

- Error messages about software or hardware malfunctions at the LOG_ERR level.
- Output for the debug commands at the LOG_WARNING level.
- Interface up/down transitions and system restarts at the LOG_NOTICE level.
- Reload requests and low process stacks at the LOG_INFO level.

Use the **logging host** and **logging trap** commands to send messages to a remote syslog server.

Table 8: logging trap Error Message Logging Priorities

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Examples

In the following example, system messages of levels 0 (emergencies) through 5 (notifications) are sent to the host at 209.165.200.225:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap notifications
Router(config)# end
Router# show logging
```

```
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level emergencies, 0 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 67 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: enabled
    Trap logging: level notifications
, 71 message lines logged
Log Buffer (4096 bytes):
00:00:20: %SYS-5-CONFIG_I: Configured from memory by console
 .
 .
 .
```

Related Commands

Command	Description
logging host	Enables remote logging of system logging messages and specifies the syslog server host that messages should be sent to.

logging userinfo

To enable the logging of user information, use the **logging userinfo** command in global configuration mode. To cancel the logging of user information, use the **no** form of this command.

logging userinfo

no logging userinfo

Syntax Description

This command has no arguments or keywords.

Command Default

User information logging is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SXH2	This command was integrated into Cisco IOS Release 12.2SXH2.

Usage Guidelines

The **logging userinfo** global configuration command allows the logging of user information when the user invokes the enable privilege mode or when the user changes the privilege level. The user can change the privilege level of a terminal session by using the **enable** and the **disable** command.

Information logged includes username, line (for example, Console and vty0), and privileged level (for example, 0 to 15).

Note When a username is not available, “unknown” is displayed as the username.

Examples

The following example shows how to enable user information logging:

```
Router# configure terminal

Router(config)# logging userinfo
Router(config)# exit
```

The following are two examples of user information logging using the **enable** and **disable** commands:

```
Router> enable 15
```

```
Password:
Router#
*Feb 26 17:11:15.398: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by cisco)
```

The **enable** command allows the user to enter a desired privilege level.

```
Router# disable 6
Router#
*Feb 26 17:12:28.922: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 6 by cisco)
```

The **disable** command allows the user to enter a desired privilege level.

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, exits to the specified privilege level.
enable	Enables higher privilege level access, such as privileged EXEC mode.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

show logging persistent

To display the contents of the logging persistent files, use the **show logging persistent** command in privileged EXEC mode.

show logging persistent [**url** *filesystem* **:** *location*] [**selector-url** *filesystem* **:** *filename*]

Syntax Description

url	(Optional) Specifies the URL to display logging messages.
filesystem **:**	The URL or alias of the file system followed by a colon.
location	The audit folder location.
selector-url	(Optional) Specifies the URL or location for the search parameters file.
filename	The URL or alias of the search parameters file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

To display the contents of the logging persistent files based on specific parameters in the syslog messages, you need to conduct a search on the syslog messages. In order to reduce the data input complexity, the **show logging persistent** command calls for a URL of a search parameters file, which contains a collection of search and sorting rules.

The search parameters file comprise three sections: search templates, search patterns, and sorting rules. These sections are described in the following text.

Search Templates

Search templates are constructed by using logical expressions and value rules. Value rules are methods of locating the beginning and ending of the object's value. The search templates along with value rules are used to locate objects in the syslog messages and to extract the objects' value.

The table below provides the definition of value rules for a list of search objects that can be used to construct search templates.

Table 9: Value Rules for Object Types

Object Type	Value Rules
AUDIT_RECORD_DATE	Fixed format field.
AUDIT_RECORD_TIME	Fixed format field.
FW_DROP_PKT_CAUSE	Finds the first alphanumeric value; stops at the first nonalphanumeric value or underscore (“_”) symbol.
INTERFACE_NAME	Finds the first alphanumeric value; stops at the first nonalphanumeric value or a symbol that is not a slash (“/”) or a period (“.”).
L4_PROTO_ID	Finds the first alphanumeric value; stops at the first nonalphanumeric value.
L4_PROTO_ID_RANGE	Finds the first numeric value; stops at the first nonnumeric value.
RULE_IDENTITY	Finds the first alphanumeric value; stops at the colon symbol (“:”).
RULE_IDENTITY_PLATFORM	Finds the first alphanumeric value; stops at the colon symbol (“:”).
SOURCE_SUBJECT DESTINATION_SUBJECT	IPv4: Finds the first numeric value; includes the substring containing number or period (“.") ; stops at the first nonnumeric value or nonperiod (“.”); trims the trailing period (“.”), if any. IPv6: Finds the first numeric value; includes the substring containing numbers or periods (“.") ; stops at first nonnumeric value or non-period (“.”); trims the trailing period (“.”), if any.
SUBJECT_SERVICE_ID	Finds the first alphanumeric value; stops at the first nonalphanumeric value.
SUBJECT_SERVICE_ID_RANGE	Finds the first numeric value; stops at the first nonnumeric value.
USER_ID	Finds the first alpha symbol; stops at the first nonalphanumeric symbol

Syntax for Search Templates

Search templates for all types of objects are strings enclosed in quotes (“...”). If you provide multiple search templates on the same line, a search is performed for each of the search template in the left-to-right order (by using the logical operation OR).

You can provide arbitrary search templates for all object types except the following: AUDIT_RECORD_DATE, AUDIT_RECORD_TIME, RULE_IDENTITY, and RULE_IDENTITY_PLATFORM.

Search templates of the AUDIT_RECORD_DATE, AUDIT_RECORD_TIME, RULE_IDENTITY, and RULE_IDENTITY_PLATFORM, objects are hard coded because the location and the format of these objects in the Cisco IOS syslog messages are fixed.

The general syntax for the search template is:

```
<object_id>:
<logical-expression>
```

For example, the following syntax searches for user:, username, or user in the sylog messages and equates it to USER_ID.

```
USER_ID: “user:” “username” “user”
```

Search Patterns

A search pattern is a regular expression (regexp) for selecting a subset of objects of a given type or a range of values.

Syntax for Search Patterns

The table below lists the syntax for search patterns of various types of objects:

Table 10: Syntax for Search Patterns

Object Type	Syntax	Example
AUDIT_RECORD_DATE	YYYY-MM-DD[:YYYY-MM-DD]	`AUDIT_RECORD_DATE:2009-01-03` `AUDIT_RECORD_DATE:2009-01-03:2009-02-04`
AUDIT_RECORD_TIME	HH:MM:SS[-HH:MM:SS]	`AUDIT_RECORD_TIME:22:30:33` `AUDIT_RECORD_TIME:22:30:33-23:30:00`
FW_DROP_PKT_CAUSE	Regular expression with double quotes (“...”)	`FW-DROP-PKT_CAUSE: "POLICY"`
INTERFACE_NAME	Regular expression with double quotes (“...”)	`INTERFACE_NAME: “FastEthernet0/1/2\.1|Gig*”`
L4_PROTO_ID	Regular expression with double quotes (“...”)	`L4_PROTO_ID: "tcp"`
L4_PROTO_ID_RANGE	Numeric value or numeric range without double quotes (“...”)	`L4_PROTO_ID_RANGE:6` `L4_PROTO_ID_RANGE:8 - 9`
RULE_IDENTITY	Regular expression with double quotes (“...”)	`RULE_IDENTITY: “SEC_LOGIN\-4\-LOGIN_FAILED|SEC_LOGIN\-5\-LOGIN_SUCCESS”`
RULE_IDENTITY_PLATFORM	Regular expression with double quotes (“...”)	`RULE_IDENTITY_PLATFORM: "FW\-6\-DROP_PKT"`
SOURCE_SUBJECT, DESTINATION_SUBJECT	Regular expression without double quotes (“...”)	`SOURCE_SUBJECT: “192\.168\.1\.*|192\.168\.2.\2?”`
SUBJECT_SERVICE_ID	Regular expression with double quotes (“...”)	`SUBJECT_SERVICE_ID: "telnet|ssh|22"`
SUBJECT_SERVICE_ID_RANGE	Numeric value or numeric range without double quotes (“...”)	`SUBJECT_SERVICE_ID_RANGE:5` `SUBJECT_SERVICE_ID_RANGE:5-122`
USER_ID	Case insensitive regular expression with double quotes (“...”)	`USER_ID: "alice|Bob"`

Sorting Rules

The sorting rules instruct how to sort the selected subset. The sorting rule is specified as a search object ID followed by a sort-order specifier, which is either ASCENDING or DESCENDING.

Syntax for Sorting Rules

The general syntax for the sorting rules is:

```
<object_id>: ASCENDING | DESCENDING
```

For example, the following syntax sorts the user IDs in an ascending order:

```
USER_ID: ASCENDING
```

Search Parameters File

The search parameters file contains a search template, search patterns, and sorting rules. Each section of a search parameters file begins with a header and ends with footer. The general syntax for the search parameters file is as follows:

```
<SEARCH TEMPLATES>
... search-templates here...
</SEARCH TEMPLATES>
<SEARCH PATTERNS>
...search-patterns here...
</SEARCH PATTERNS>
<SORT RULES>
... sort-rules here...
</END SORT RULES>
```

Search Parameters File: Example

The following example shows how to construct search parameters for finding all audit records sorted by the user, between 9/17/2009 and 9/21/2009, captured between 1:00 a.m. and 4:00 a.m. on those dates, which belong to usernames testuser1 or testuser2, and are attempts to initiate a telnet or console connection.

The following syslog messages appear in the output:

*Sep 19 02:46:02.173: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testuser1] [Source: 172.27.53.101] [localport: 22] at 02:46:02 UTC Wed Sep 19 2001

*Sep 19 02:46:51.359: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: testuser1] [Source: 172.27.53.101] [localport: 22] [Reason: Login Authentication Failed] at 02:46:51 UTC Wed Sep 19 2001

*Sep 19 03:26:28.721: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testuser2] [Source: 0.0.0.0] [localport: 0] at 03:26:28 UTC Wed Sep 19 2001

The search parameters file for this example is constructed as follows:

```
<SEARCH TEMPLATES>
USER_ID: “user:”
SUBJECT_SERVICE_ID: “localport:”
</SEARCH TEMPLATES>
<SEARCH PATTERNS>
RULE_IDENTITY: “SEC_LOGIN\-5\-LOGIN_SUCCESS” “SEC_LOGIN\-4\-LOGIN_FAILED”
USER_ID: “Alice|Bob”
SUBJECT_SERVICE_ID: “0|22”
AUDIT_RECORD_DATE: 2009-09-17:2009-09-21
AUDIT_RECORD_TIME: 01:00:00 - 03:59:59
</SEARCH PATTERNS>
<SORT RULES>
USER_ID: ASCENDING
</SORT RULES>
```

The **url** *filesystem* **:** *location* keyword and argument combination specifies the audit folder location. If you do not specify these attributes, a default audit folder location is used. The default audit folder location is defined using the **logging persistent** command.

If you do not specify the **selector-url** *filesystem* **:** *filename* keyword and argument combination, the viewer displays log files in a chronological order.

Examples

The following is sample output from the **show logging persistent** command:

```
Router# show logging persistent
```

```
000070: *Feb 17 01:22:24.147: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
000071: *Feb 17 01:22:24.979: %SYS-5-CONFIG_I: Configured from console by ena on console
000072: *Feb 17 01:22:24.979: %PARSER-6-EXPOSEDLOCKRELEASED: Exclusive configuration lock
released from terminal '0' -Process= "Exec", ipl= 0, pid= 3
000073: *Feb 17 02:45:17.201: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
Router#
000074: *Feb 18 05:49:19.443: %SYS-6-SHOW_LOGGING_PERSISTENT: User test has activated the
show logging persistent command.
```

The following example shows how to specify the location of the search parameters file “filter_rule_id” from bootflash. The syslog messages are sorted using the search parameters specified in the “filter_rule_id” file and the contents are displayed in the output. In this case, the search parameters specify the system to search for audit records sorted by the “testu1” user for the date 08/31/09.

```
Router# show logging persistent selector-url bootflash:filter_rule_id_pl

*Aug 31 19:35:37.540: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testu1] [Source:
0.0.0.0] [localport: 0] at 19:35:37 UTC Fri Aug 31 2009
*Aug 31 19:35:54.385: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock acquired
 by user 'testu1' from terminal '0'  -Process= "Exec", ipl= 0, pid= 96 (note: includes space
 and apostrophe)
```

The following example shows how to display syslog messages from an audit folder location:

```
Router# show logging persistent url bootflash:test_location

000070: *Feb 17 01:22:24.147: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
000071: *Feb 17 01:22:24.979: %SYS-5-CONFIG_I: Configured from console by test onconsole
Router#
000074: *Feb 18 05:49:19.443: %SYS-6-SHOW_LOGGING_PERSISTENT: User test has activated the
show logging persistent command.
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging persistent	Enables the storage of logging messages on the router’s ATA disk.