Reliable Delivery and Filtering for Syslog

First Published: November 17, 2006
Last Updated: September 10, 2007

The Reliable Delivery and Filtering for Syslog feature allows a device to be customized for receipt of syslog messages. This feature provides reliable and secure delivery for syslog messages using Blocks Extensible Exchange Protocol (BEEP). Additionally, it allows multiple sessions to a single logging host, independent of the underlying transport method, and provides a filtering mechanism called a message discriminator.

This module describes the functions of the Reliable Delivery and Filtering for Syslog feature and how to configure them in a network.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Reliable Delivery and Filtering for Syslog" section on page 38.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Reliable Delivery and Filtering for Syslog

- Router level rate limit is set to meet business needs, network traffic requirements, or performance requirements.
- Each BEEP session must have an RFC-3195 compliant syslog-RAW exchange profile.
- A Simple Authentication and Security Layer (SASL) profile specifying “DIGEST-MD5” for provisioning services must be established when a crypto image is used.
- Syslog servers must be compatible with BEEP.
- Syslog server applications must be capable of handling multiple sessions to use the multiple session capability of the Reliable Delivery and Filtering for Syslog feature.

Restrictions for Reliable Delivery and Filtering for Syslog

- Only the syslog-RAW, SASL, and Transport Layer Security (TLS) profiles are supported.
- Both ends of a syslog session must use the same transport method.
- A message discriminator must be defined before it can be associated with a specific syslog session.
- A syslog session can be associated with only one message discriminator.
- Message delivery with User Datagram Protocol (UDP) will be faster than with either TCP or BEEP.

Information About Reliable Delivery and Filtering for Syslog

To use the Reliable Delivery and Filtering for Syslog feature, you should understand the following concepts:

BEEP Transport Support

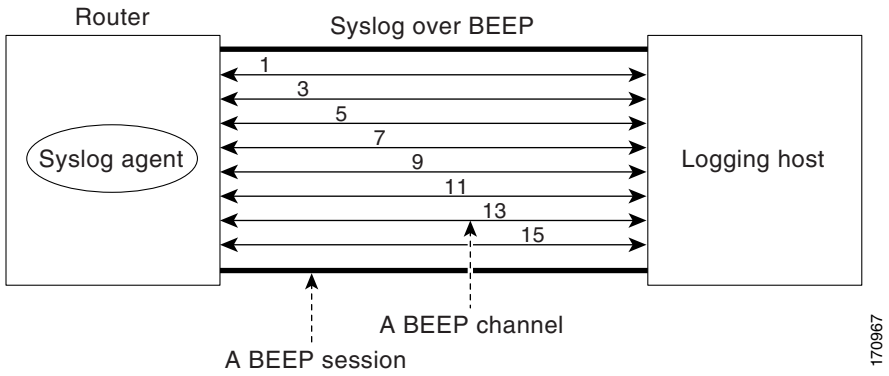
BEEP is a generic application protocol framework for connection-oriented, asynchronous interactions. It is intended to provide the features that traditionally have been duplicated in various protocol implementations. BEEP typically runs on top of TCP and allows the exchange of messages. Unlike HTTP and similar protocols, either end of the connection can send a message at any time. BEEP also includes facilities for encryption and authentication and is highly extensible.

BEEP as a transport protocol for syslog messages provides multiple channels. Each channel can be configured for a separate session to the same host. BEEP provides reliable transport. Syslog messages sent over a BEEP connection are guaranteed to be delivered in sequence.

With command-line interface (CLI) commands introduced in the Reliable Delivery and Filtering for Syslog, you can configure a new BEEP session to have a maximum of eight channels.

Figure 1 shows a BEEP session with eight channels, allowing eight separate syslog sessions.

Figure 1 BEEP Session with Eight Channels



Channels are identified as 1, 3, 5, 7, 9, 11, 13, and 15. The number (eight) of available channels was designed to correspond to the number of severity levels of classic RFC-3164 syslog messages (0 to 7). Message discriminators can be used such that severity levels are mapped to BEEP channels. An intelligent BEEP syslog server (depending upon the BEEP stack used) could use this mapping to prioritize messages with higher severity (see RFC-3081, section 3.1.4). Unless associated with a message discriminator, all syslog sessions (channels) receive all syslog messages.

Syslog Message

A syslog message has a sequence number that allows the host to use the number as an identifier for the message as well as to detect whether there were any gaps in the messages that were received. Consecutive syslog messages are numbered consecutively. The reliability of BEEP does not replace the need for sequence numbers, which are required for the following reasons:

- A sequence number provides an easy way to identify a syslog message. Independent of reliability considerations, the sequence number serves as a message identifier.
- A BEEP session may not be in place for the entire time that a device sending syslog messages is up. Sequence numbers provide a way for management applications to assess whether messages were missed between BEEP sessions.
- BEEP is only one of several transports. Unreliable transports are also used and the syslog protocol should not rely on a reliable transport always being provided.

The existing numbering scheme for syslog messages is limited with the extension of syslog to accommodate advanced message discrimination features and multiple hosts. Message discrimination leads to gaps in the sequence numbers, meaning that hosts lose the ability to detect whether they have missed a message. If syslog messages are numbered consecutively on each session to avoid the gaps in sequence numbers, it will not be possible to easily correlate which messages are the same and which ones are different because the sequence number would no longer uniquely identify a message.

To separate identification from sequencing and reliability, the following changes to syslog messages were made:

- The sequence number is retained as an identifier for the message. Messages with a lower number precede messages with a higher number, but they are not be guaranteed to be consecutive.
- An additional field is added in the body portion of a syslog message to help ensure sequencing. The contents of this field contain a sequence number for a particular session. The same message transmitted over different sessions may have a different sequence number.

Syslog Session

A syslog session is a logical link from the syslog agent on a router to the recipient of a syslog message. For example, a syslog session can be established between a syslog agent and any of the following:

- Router console
- Router logging buffer
- Router monitor
- External syslog server

A syslog session runs over a transport connection between the syslog source and the syslog destination. A transport connection can use any of the following protocols:

- TCP
- UDP (association to one remote address and port)
- BEEP (channel within a BEEP session)

Figure 2 shows a mapping of syslog sessions and transport protocols between a router and a syslog server using an Open Systems Interconnection (OSI) model.

Note Figure 2 appears differently in different web browsers. It is best viewed using Internet Explorer.

Figure 2 Router to Syslog Server Mapping of Syslog Sessions and Transport Protocols

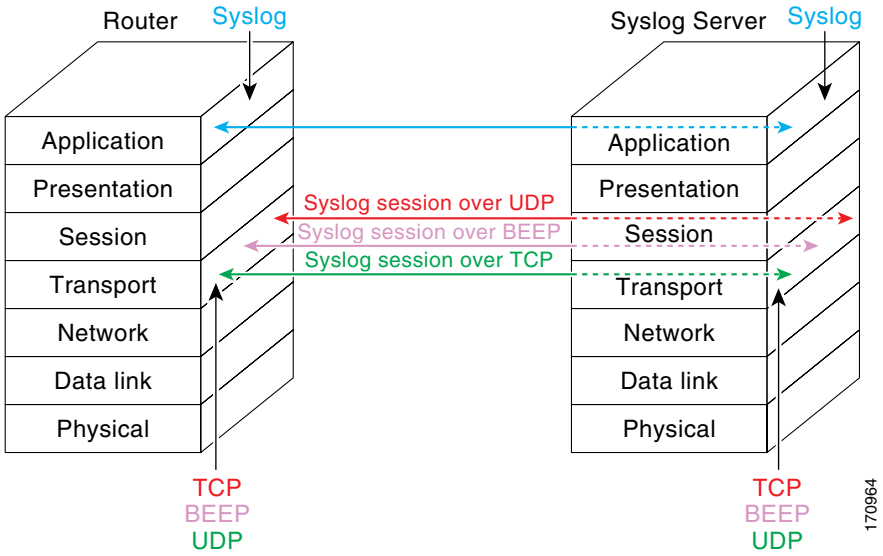
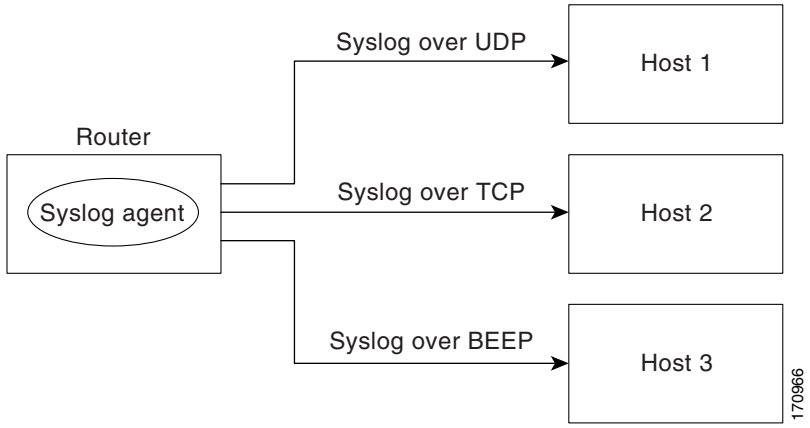


Figure 3 shows multiple syslog sessions from a single syslog agent to different hosts using UDP, TCP and BEEP.

Figure 3 Multiple Syslog Sessions from One Syslog Agent to Multiple Hosts

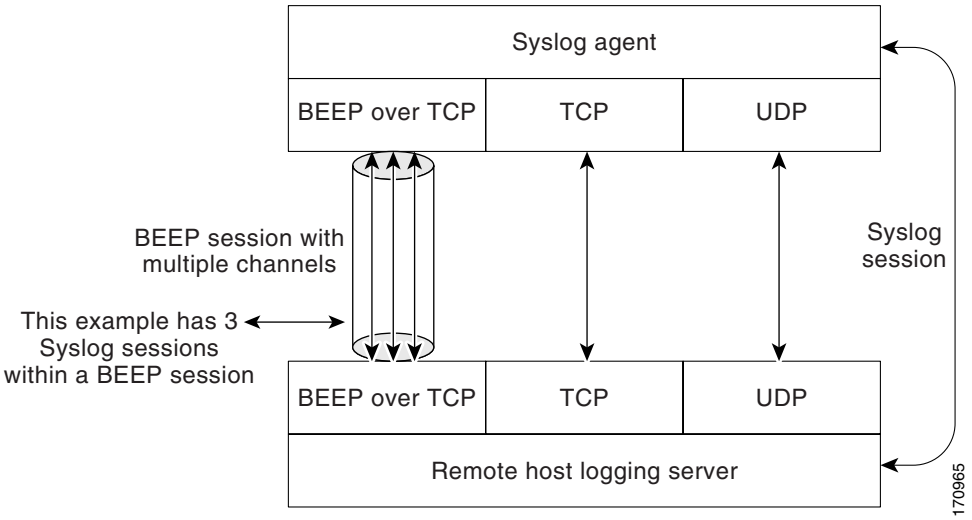


Multiple Syslog Sessions

A syslog session is independent of a transport connection. A Cisco router can support multiple syslog sessions, each running over its own transport connection. Multiple syslog sessions cannot share the same transport connection, but multiple syslog sessions may terminate at the same remote host, each running over its own transport connection. An example is a BEEP session in which multiple channels are used.

Figure 4 shows an end-to-end view of a syslog session. Note the three syslog sessions within a single BEEP session.

Figure 4 End-to-End View of a Syslog Session



The TCP and UDP protocols do not have multiplexed channels but the protocols do allow for using multiple ports to establish multiple syslog sessions to the same syslog host. To enable the UDP and TCP transport methods to have capability similar to BEEP's multiple channel capability, the Reliable Delivery and Filtering for Syslog feature allows multiple syslog sessions to be established via the UDP and TCP transport methods to the same logging host. Multiple syslog sessions going over BEEP sessions is also supported.

Message Discriminator

A message discriminator is a syslog processor. A message discriminator is associated with a syslog session and binds that session to a transport connection. A message discriminator offers the following capabilities:

Prior to message delivery, the message is subject to the message discriminator with a user-specified list of criteria. After the first filtering criterion results in a message being blocked, the filtering check stops.

Note The sequence of criteria in the CLI does not affect the sequence in which criteria is checked.

- Following are filtering criteria. These criteria are checked in the order listed here:
  - Severity level or levels specified
  - Facility within the message body that matches a regular expression
  - Mnemonic that matches a regular expression
  - Part of the body of a message that matches a regular expression
- Optional rate limiting—Specifying a transmission rate of messages per time interval that is not to be exceeded. If the rate limit is exceeded, messages are either delayed or dropped, at the discretion of the device. The application of a rate limiter means that reliable delivery of syslog messages over that syslog session is no longer guaranteed. The purpose of a rate limiter is to avoid potential "flooding" at recipient syslog servers for applications that do not require guaranteed syslog delivery.

- Correlating—Inspecting candidate event messages and possibly aggregating information across events, creating a new event that contains the aggregated information. Correlating functions include:
  - Elimination of duplicate messages by maintaining a message count and waiting a specific time period between sending the first message of a certain type and sending the next message of that type
  - Elimination of oscillating messages
  - Simple message correlation; for example, if one message is a symptom of a cause reported by another message, one consolidated message is reported

A message discriminator can be associated with a specific destination and transport; that is, the filter can be host dependent. For this reason, a message discriminator is attached to a syslog session, transport, or channel, with possible device support for multiple sessions, transports, or channels, each of which can be attached to a different discriminator.

The establishment of a message discriminator should be separate from the establishment of a syslog session. A message discriminator should refer to the syslog session, transport, or channel to which it should be attached. The reasons for the separation are the following:

- Message discriminators can be managed separately from the connections, and refinements in the capabilities available to set up message discriminators need not affect how syslog sessions are set up and vice versa.
- Multiple connections can be attached to the same message discriminator, allowing for various syslog redundancy topologies.

When an explicit message discriminator is not associated with a syslog session, the generic message discriminator from the router-wide global settings is used. If you want to create an “empty” message discriminator without specifying attribute values (no rate limit and no filter configured), you can do that.

Rate Limiting

The router-wide rate limiting capability in Cisco IOS Syslog is preserved in the Reliable Delivery and Filtering for Syslog feature and is referred to as “global rate limiting.” If you do not use global rate limiting, all event messages are sent to remote syslog hosts if system resources can support the volume. When global rate limiting is set, it applies to all destinations. The value is set to the rate-limit attribute of the “generic message discriminator” if one has been set. The disadvantage of global rate limiting is that the rate limit of the least performing remote syslog host sets the rate for how fast a router can send out syslog messages.

The Reliable Delivery and Filtering for Syslog feature provides syslog session-based rate limiting to bypass the effects of global rate limiting. This session-based rate limiting is associated with a specific message discriminator and allows you to set the rate acceptance level independently for each syslog session.

Use of global rate limiting is not recommended when session rate limiting is in effect. A rate limit in a message discriminator specifies a not-to-exceed rate of syslog messages but does not guarantee that this rate will be reached. A configured global rate limit may cause messages on a session to be dropped even if the rate limit for that session has not been reached. These actions are important to understand if global rate limiting and session rate limiting are used concurrently.

Benefits of Reliable Delivery and Filtering for Syslog

- Authentication and encryption capabilities in BEEP provide reliable and secure delivery for syslog messages
- Multiple sessions to a single logging host independent of the underlying transport method
- Session-based message filtering and rate limiting
- Multiple connections can be attached to the same message discriminator, allowing various syslog redundancy topologies
- New CLI command to disable the default syslog count
- New CLI command to help identify relative positions of syslog messages that are dropped due to rate limiting

How to Configure Reliable Delivery and Filtering for Syslog

To configure Reliable Delivery and Filtering for Syslog, perform the following tasks:

Creating a Message Discriminator

Perform this task to create a message discriminator for syslog messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*] **Example:** `Router(config)# logging discriminator pacfltr1 facility includes facl357`	Creates a message discriminator with a facility subfilter. In this example, all messages with "facl357" in the facility field will be delivered.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Associating a Message Discriminator with a Logging Buffer

Perform this task to associate a message discriminator with a specific buffer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*]
4. **logging buffered** [*buffer-size* | *severity-level* | **discriminator** *discr-name* [*severity-level*]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*] **Example:** `Router(config)# logging discriminator pacfltr2`	Creates a message discriminator.
Step 4	**logging buffered** [*buffer-size* | *severity-level* | **discriminator** *discr-name* [*severity-level*]] **Example:** `Router(config)# logging buffered discriminator pacfltr2 5`	Enables logging to a local buffer and specifies a message discriminator.
Step 5	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Associating a Message Discriminator with a Console Terminal

Perform this task to associate a message discriminator with a console terminal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*]
4. **logging console** [*severity-level* | **discriminator** *discr-name* [*severity-level*]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*] **Example:** `Router(config)# logging discriminator pacfltr3`	Creates a message discriminator.
Step 4	**logging console** [*severity-level* | **discriminator** *discr-name* [*severity-level*]] **Example:** `Router(config)# logging console discriminator pacfltr3 1`	Enables logging to the console and specifies a message discriminator filtering messages at a specific severity level.
Step 5	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Associating a Message Discriminator with Terminal Lines

Perform this task to associate a message discriminator with terminal lines and have messages display at a monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*]
4. **logging monitor** [*severity-level* | **discriminator** *discr-name* [*severity-level*]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging discriminator** *discr-name* [[**facility** | **mnemonics** | **msg-body** {**drops** | **includes**} *string*] | **severity** {**drops** | **includes**} *sev-num* | **rate-limit** *msglimit*] **Example:** `Router(config)# logging discriminator pacfltr4`	Creates a message discriminator.
Step 4	**logging monitor** [*severity-level* | **discriminator** *discr-name* [*severity-level*]] **Example:** `Router(config)# logging monitor discriminator pacfltr4 2`	Specifies a message discriminator named pacfltr4 and enables logging to the terminal lines of messages at severity level 2 and lower.
Step 5	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Enabling Message Counters

Perform this task to enable logging of debug, log, or syslog messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging message-counter** {**debug** | **log** | **syslog**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging message-counter** {**debug** | **log** | **syslog**} **Example:** `Router(config)# logging message-counter syslog`	Enables logging of syslog messages.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Adding and Removing a BEEP Session

Perform this task to add and remove a BEEP session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **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**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**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**] **Example:** `Router(config)# logging host host3 transport beep port 600 channel 3`	Identifies a logging host and specifies the transport protocol, port, and channel for logging messages.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Configuration Examples for Reliable Delivery and Filtering for Syslog

This section provides the following configuration example:

- Configuring Transport and Logging: Example, page 14

Configuring Transport and Logging: Example

```
Router(config)# show running-config | include logging

logging buffered xml
 logging
 logging
logging host 209.165.201.1 transport udp port 601
 logging synchronous

Router(config)# logging host 209.165.201.1 transport beep port 600 channel 3
Router(config)# logging host 209.165.201.1 transport tcp port 602
Router(config)# show running-config | include logging
```

```
logging buffered xml
 logging
 logging
logging host 209.165.201.1 transport udp port 601
logging host 209.165.201.1 transport beep port 600 channel 3
logging host 209.165.201.1 transport tcp port 602
 logging synchronous
Router(config)#
```

Additional References

The following sections provide references related to the Reliable Delivery and Filtering for Syslog feature.

Related Documents

Related Topic	Document Title
Syslog protocol	*The BSD Syslog Protocol*, RFC 3164
Syslog logging	"Troubleshooting, Logging, and Fault Management" section of the *Cisco IOS Network Management Configuration Guide*, Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC-3195	*Reliable Delivery for Syslog*
RFC-3081, section 3.1.4	*Mapping the BEEP Core onto TCP,* "Use of Flow Control"
RFC-3164	*The BSD Syslog Protocol*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **logging buffered**
- **logging console**
- **logging discriminator**
- **logging host**
- **logging message-counter**
- **logging monitor**
- **show logging**

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 [*buffer-size* | *severity-level* | **discriminator** *discr-name* [*severity-level*]]

no logging buffered

default logging buffered

Syntax Description

buffer-size	(Optional) Size of the buffer, in bytes. The range is 4096 to 4294967295. 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.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1(17)T	The *severity-level* argument was added in Cisco IOS Release 11.1(17)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

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 *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.

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.

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.

Table 1 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 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 [*severity-level* | **discriminator** *discr-name* [*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 Level 7 is the default.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

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

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.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

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.

Table 2 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
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 discriminator

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

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

no logging discriminator *discr-name*

Syntax Description

discr-name	String of a maximum of 8 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 do not 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 1000 that identifies the number of messages not to be exceeded.

Command Default

The logging discriminator function is disabled.

Command Modes

Global configuration

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.

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
```

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**]

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	(Optional) Specifies a virtual private network (VPN) routing and forwarding instance (VRF) that connects to the syslog server host.
vrf-name	(Optional) 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	(Optional) Specifies a message discriminator for the session.
discr-name	(Optional) 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	(Optional) Specifies that only ESM filtered messages with the stream identification number specified in the *stream-id* argument should be sent to this host.
stream-id	(Optional) Number from 10 to 65535 that identifies the message stream.
xml	(Optional) Specifies that the logging output should be tagged using the Extensible Markup Language (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	(Optional) Specifies the BEEP channel number to use.
chnl-number	(Optional) 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 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	(Optional) Specifies a trustpoint for identity information and certificates. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images.
trustpt-name	(Optional) 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 TCP transport will be used.
udp	(Optional) Specifies that the User Datagram Protocol (UDP) transport will be used.
port	(Optional) Specifies a port will be used.
port-number	(Optional) 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

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

Command History

Release	Modification
10.0	The **logging** command was introduced.
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(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(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 and the **vrf** *vrf-name* keyword-argument pair was added.
12.4(4)T	The **ipv6** *ipv6-address* and **vrf** *vrf-name* keyword-argument pairs were added.
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.
12.4(11)T	Support for BEEP and the **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was implemented on the Cisco 10000 series routers.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
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 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 are mutually exclusive on a given syslog session.

Using the BEEP transport protocol, you can have reliable and secure delivery for syslog messages and configure multiple sessions over 8 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 as well as the BEEP protocol for port 600 and channel 3.

```
Router(config)# logging host host2 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 message-counter

To enable logging of debug, log, or syslog messages, use the **logging message-counter** command in global configuration mode. To turn off 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 disabled.

Command Modes

Global configuration

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.

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 [*severity-level* | **discriminator** *discr-name* [*severity-level*]]

no logging monitor

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 Level 7 is the default.
discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of 8 alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.

Command Default

The logging monitor function is disabled.

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.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Specifying a severity-level causes messages both at that level and at numerically lower levels to be displayed to the monitor. Table 3 shows a list of levels and corresponding syslog definitions.

Table 3 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.

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in privileged EXEC mode.

show logging [**slot** *slot-number* | **summary**]

Syntax Description

slot *slot-number*	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and 0 to 7 for the Cisco 12008 Internet router.
summary	(Optional) Displays counts of messages by type for each line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2 GS	The **slot** and **summary** keywords were added for the Cisco 12000.
12.2(8)T	Command output was expanded to show the status of the logging count facility (“Count and timestamp logging messages”).
12.2(15)T	Command output was expanded to show the status of XML syslog formatting.
12.3(2)T	Command output was expanded (on supported software images) to show details about the status of system logging processed through the Embedded Syslog Manager (ESM). These lines appear as references to “filtering” or “filter modules”.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	Command-line interface (CLI) output was modified to show message discriminators defined at the router and syslog sessions associated with those message discriminators.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will also display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the [**no**] **logging buffered** command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the **logging buffered** command.

To enable and set the format for syslog message timestamping, use the **service timestamps log** command.

If debugging is enabled (using any **debug** command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system error messages and will not be preceded by the percent symbol (%).

Examples

The following is sample output from the **show logging** command on a software image that supports the Embedded Syslog Manager (ESM) feature:

```
Router# show logging

Syslog logging: enabled (10 messages dropped, 5 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 31 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: disabled
    Buffer logging: level errors, 36 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.


    Trap logging: level informational, 45 message lines logged

Log Buffer (8192 bytes):
```

The following example shows output from the **show logging** command after a message discriminator has been configured. Included in this example is the command to configure the message discriminator.

```
c7200-3(config)# logging discriminator ATTFLTR1 severity includes 1,2,5 rate-limit 100

Specified MD by the name ATTFLTR1 is not found.
Adding new MD instance with specified MD attribute values.

Router(config)# end
Router#

000036: *Oct 20 16:26:04.570: %SYS-5-CONFIG_I: Configured from console by console

Router# show logging

Syslog logging: enabled (11 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

Inactive Message Discriminator:
ATTFLTR1  severity group includes 1,2,5
    rate-limit not to exceed 100 messages per second

Console logging: level debugging, 25 messages logged, xml disabled, filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 25 messages logged, xml disabled, filtering disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled

No active filter modules.
```

```
Trap logging: level debugging, 28 message lines logged
Logging to 172.25.126.15  (udp port 1300,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
Logging to 172.25.126.15  (tcp port 1307,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled, filtering disabled
Logging to 172.20.1.1  (udp port 514,  audit disabled,
    authentication disabled, encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled

Log Buffer (1000000 bytes):
```

Table 4 describes the significant fields shown in the output for the two preceding examples.

Table 4 show logging Field Descriptions

Field	Description
Syslog logging:	Shows general state of system logging (enabled or disabled), the status of logged messages (number of messages dropped, rate-limited, or flushed), and whether XML formatting or ESM filtering is enabled.
No Active Message Discriminator	Indicates that a message discriminator is not being used.
Inactive Message Discriminator:	Identifies a configured message discriminator that has not been invoked.
Console logging:	Logging to the console port. Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging console**, **logging console xml**, or **logging console filtered** command.
Monitor logging:	Logging to the monitor (all TTY lines). Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging monitor**, **logging monitor xml**, or **logging monitor filtered** command.
Buffer logging:	Logging to the standard syslog buffer. Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging buffered**, **logging buffered xml**, or **logging buffered filtered** command.

Table 4 show logging Field Descriptions (continued)

Field	Description
Trap logging:	Logging to a remote host (syslog collector). Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. (The word "trap" means a trigger in the system software for sending error messages to a remote host.) Corresponds to the configuration of the **logging host** command. The severity level limit is set using the **logging trap** command.
SNMP logging	Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the **show logging history** command.
Logging Exception size (8192 bytes)	Corresponds to the configuration of the **logging exception** command.
Count and timestamp logging messages:	Corresponds to the configuration of the **logging count** command.
No active filter modules.	Appears if no syslog filter modules are configured with the **logging filter** command. Syslog filter modules are Tcl script files used when the Embedded Syslog Manager (ESM) is enabled. ESM is enabled when any of the **filtered** keywords are used in the logging commands. If configured, the URL and filename of configured syslog filter modules will appear at this position in the output. Syslog filter modules are executed in the order in which they appear here.
Log Buffer (8192 bytes):	The value in parentheses corresponds to the configuration of the **logging buffered** *buffer-size* command. If no messages are currently in the buffer, the output ends with this line. If messages are stored in the syslog buffer, they appear after this line.

The following example shows that syslog messages from the system buffer are included, with time stamps. In this example, the software image does not support XML formatting or ESM filtering of syslog messages.

```
Router# show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
    Console logging:disabled
    Monitor logging:level debugging, 0 messages logged
    Buffer logging:level debugging, 4104 messages logged
    Trap logging:level debugging, 4119 message lines logged
        Logging to 192.168.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225
(afi 0) reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from
tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
```

```
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down BGP
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1
(update malformed) 0 bytes
 .
 .
 .
```

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

Table 5 describes the symbols that precede the timestamp.

Table 5 Timestamping Symbols for syslog Messages

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually.	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

The following is sample output from the **show logging summary** command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, the line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.

Note For similar log counting on other platforms, use the **show logging count** command.

```
Router# show logging summary

+-----+-------+-------+-------+-------+-------+-------+-------+-------+
 SLOT | EMERG | ALERT | CRIT  | ERROR |WARNING| NOTICE| INFO  | DEBUG |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
|* 0* |     . |     . |     . |     . |     . |     . |     . |     . |
|  1  |       |       |       |       |       |       |       |       |
|  2  |       |       |       |     1 |     4 |    45 |       |       |
|  3  |       |       |       |       |       |       |       |       |
|  4  |       |       |       |     5 |     4 |    54 |       |       |
|  5  |       |       |       |       |       |       |       |       |
|  6  |       |       |       |       |       |       |       |       |
|  7  |       |       |       |    17 |     4 |    48 |       |       |
|  8  |       |       |       |       |       |       |       |       |
|  9  |       |       |       |     1 |     4 |    47 |       |       |
| 10  |       |       |       |       |       |       |       |       |
| 11  |       |       |       |    12 |     4 |    65 |       |       |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
Router#
```

Table 6 describes the logging level fields shown in the display.

Table 6 show logging summary Field Descriptions

Field	Description
SLOT	Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the **show logging** command.
EMERG	Indicates that the system is unusable.
ALERT	Indicates that immediate action is needed.
CRIT	Indicates a critical condition.
ERROR	Indicates an error condition.
WARNING	Indicates a warning condition.
NOTICE	Indicates a normal but significant condition.
INFO	Indicates an informational message only.
DEBUG	Indicates a debugging message.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the error log count capability.
logging history size	Changes the number of syslog messages stored in the history table of the router.
logging linecard	Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
service timestamps	Configures the system to timestamp debugging or logging messages.
show logging count	Displays a summary of system error messages (syslog messages) by facility and severity.
show logging xml	Displays the state of system logging and the contents of the XML-specific logging buffer.

Feature Information for Reliable Delivery and Filtering for Syslog

Table 7 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 7 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 7 Feature Information for Reliable Delivery and Filtering for Syslog

Feature Name	Releases	Feature Information
Reliable Delivery and Filtering for Syslog	12.4(11)T 12.2(33)SRB	The Reliable Delivery and Filtering for Syslog feature allows a device to be customized for receipt of syslog messages. This feature provides for reliable and secure delivery for syslog messages using BEEP. Additionally it allows multiple sessions to a single logging host, independent of the underlying transport method, and provides a filtering mechanism called a message discriminator.