Reliable Delivery and Filtering for Syslog

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.

Prerequisites for Reliable Delivery and Filtering for Syslog

- The device 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

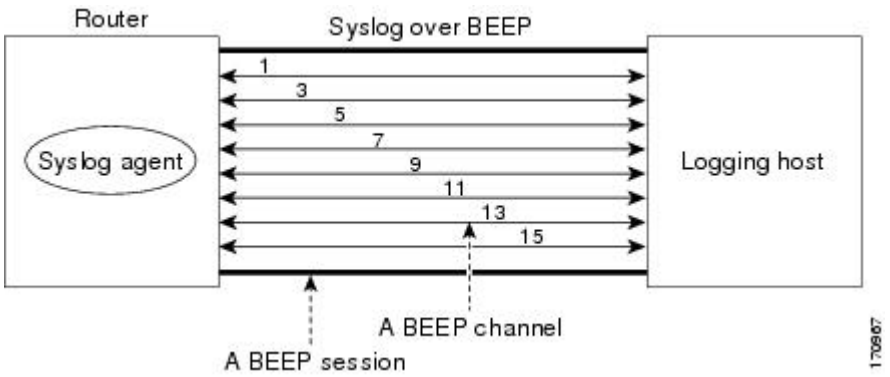
BEEP Transport Support

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 feature, you can configure a new BEEP session to have a maximum of eight channels.

The figure below shows a BEEP session with eight channels, allowing eight separate syslog sessions.



Channels are identified as 1, 3, 5, 7, 9, 11, 13, and 15. The number of available channels (eight) 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. 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 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 device to the recipient of a syslog message. For example, a syslog session can be established between a syslog agent and any of the following:

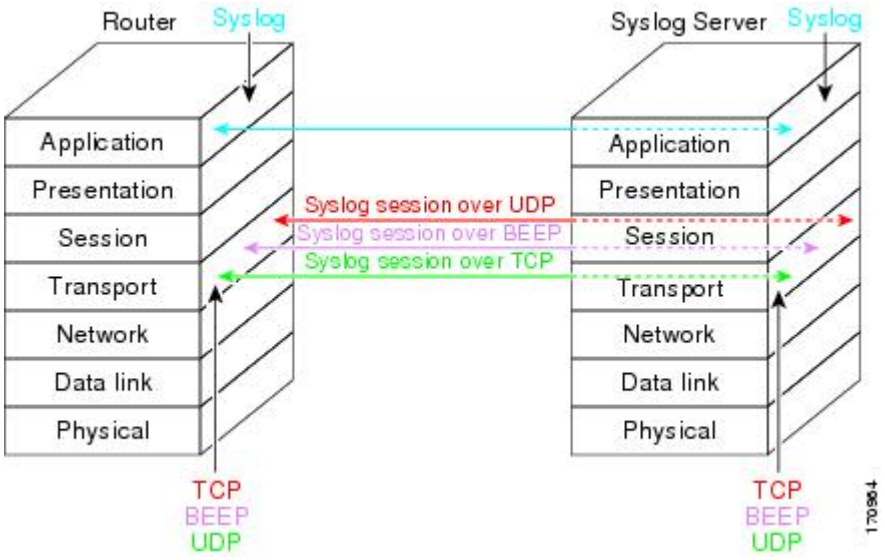
- Device console
- Device logging buffer
- Device monitor
- External syslog server

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:

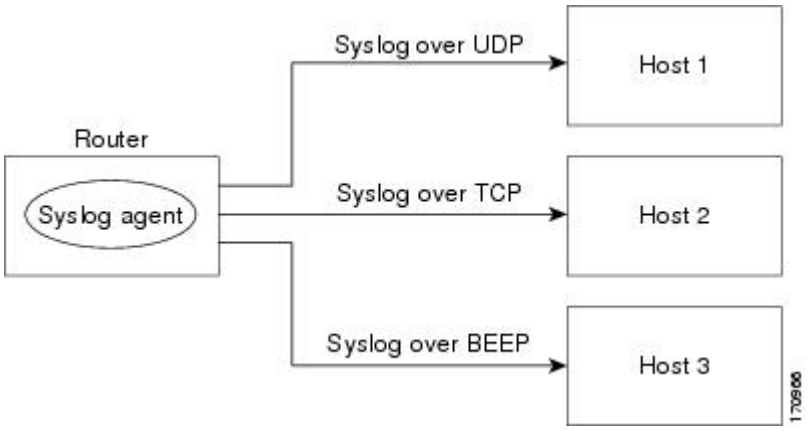
- TCP
- UDP (association to one remote address and port)
- BEEP (channel within a BEEP session)

The figure below shows a mapping of syslog sessions and transport protocols between a device and a syslog server using an Open Systems Interconnection (OSI) model.

Note The figure below is best viewed using Internet Explorer.



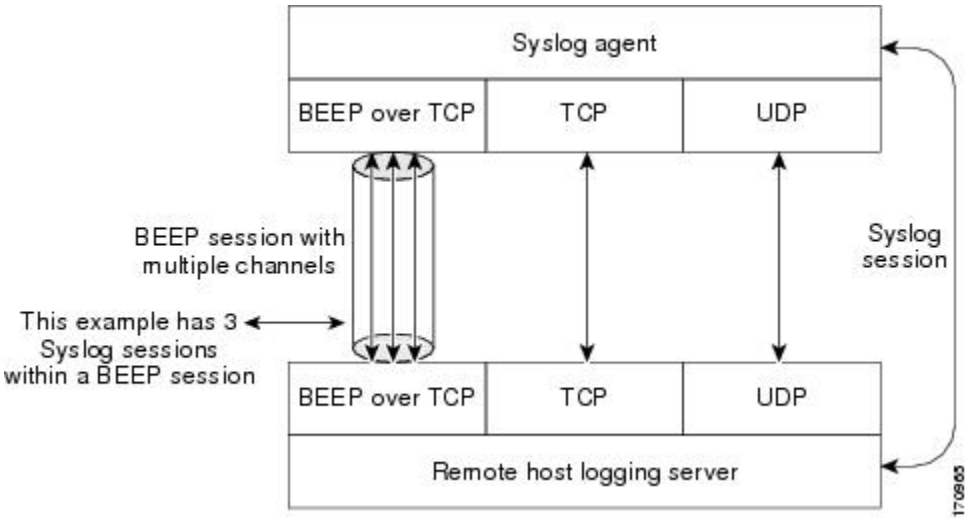
The figure below shows multiple syslog sessions from a single syslog agent to different hosts using UDP, TCP and BEEP.



Multiple Syslog Sessions

A syslog session is independent of a transport connection. A Cisco device 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.

The figure below shows an end-to-end view of a syslog session. Note the three syslog sessions within a single BEEP 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.

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

A message discriminator offers the following capabilities:

- 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 device-wide global settings is used. You can create an "empty" message discriminator without specifying attribute values (no rate limit and no filter configured).

Rate Limiting

The device-wide rate limiting capability in Cisco IOS XE 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 device 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-based 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-based 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

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** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging discriminator** *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] {**drops** *string*| **includes** *string*}] [**severity** {**drops** *sev-num*	**includes** *sev-num*}] [**rate-limit** *msglimit*] **Example:** `Device(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:**	Returns the CLI to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

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** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging buffered** [**discriminator** *discr-name* | **xml**] [*buffer-size*] [*severity-level*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device(config)# end`	

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** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging console** [**discriminator** *discr-name* | **xml**] [*severity-level*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device(config)# end`	

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** *string*| **includes** *string*}] [**severity** {**drops** *sev-num* | **includes** *sev-num*}] [**rate-limit** *msglimit*]
4. **logging monitor** [**discriminator** *discr-name*| **xml**] [*severity-level*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device(config)# end`	

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**logging message-counter** {**debug**	**log**	**syslog**} **Example:** `Device(config)# logging message-counter syslog`	Enables logging of syslog messages.
Step 4	**end** **Example:** `Device(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**{**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# 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**{**hostname** | **ipv4** | **ipv6** | **string** *custom-string*}] **Example:** `Device(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:** `Device(config)# end`	Returns the CLI to privileged EXEC mode.

Configuration Examples for Reliable Delivery and Filtering for Syslog

Configuring Transport and Logging Example

```
Device(config)# do show running-config
 | include logging
logging buffered xml
logging host 209.165.201.1 transport udp port 601
```

```
Device(config)# logging host 209.165.201.1 transport beep port 600 channel 3
Device(config)# logging host 209.165.201.1 transport tcp port 602

Device(config)# show running-config | include logging
logging buffered xml
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
Device(config)#
```

Additional References for VRF-Aware Source Interfaces for Syslog Transactions

Related Documents

Related Topic	Document Title
Network Management commands (including logging commands): complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Syslog logging	*Troubleshooting and Fault Management module*

Standards and RFCs

Standard/RFC	Title
No new or modified standards/RFCs are supported by this feature, and support for existing standards/RFCs 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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Reliable Delivery and Filtering for Syslog

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Reliable Delivery and Filtering for Syslog

Feature Name	Releases	Feature Information
Reliable Delivery and Filtering for Syslog	Cisco IOS XE Release 2.1	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. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **logging buffered**, **logging console**, **logging discriminator**, **logging host**, **logging message-counter**, **logging monitor**, **show logging**.