VRF Aware System Message Logging (Syslog)

First Published: June 12, 2006
Last Updated: August 6, 2007

The VRF Aware System Message Logging (Syslog) feature allows a router to send system logging (syslog) messages to a syslog server host connected through a Virtual Private Network (VPN) routing and forwarding (VRF) interface.

You can use logging information for network monitoring and troubleshooting. This feature extends this capability to network traffic connected through VRFs.

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 VRF Aware System Message Logging" section on page 19.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

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

Prerequisites for VRF Aware System Message Logging

A VRF must be configured on the router.

Restrictions for VRF Aware System Message Logging

You cannot specify a source address for VRF system logging messages. The VRF Aware System Message Logging feature uses the VRF interface address as the source address for all VRF-aware system logging messages.

Information About VRF Aware System Message Logging

You should understand the following concepts before configuring the VRF Aware System Message Logging feature:

VRF Aware System Message Logging Benefit—Monitoring and Troubleshooting Network Traffic Connected Through a VRF

A Virtual Private Network (VPN) routing and forwarding (VRF) instance is an extension of IP routing that provides multiple routing instances. A VRF provides a separate IP routing and forwarding table to each VPN. You must configure a VRF on a routing device before you configure the VRF Aware System Message Logging feature.

After you configure the VRF Aware System Message Logging feature on a routing device, the device can send syslog messages to a syslog host through a VRF interface. Then you can use logging messages to monitor and troubleshoot network traffic connected through a VRF. Without the VRF Aware System Message Logging feature on a routing device, you do not have this benefit; The routing device can send syslog messages to the syslog host only through the global routing table.

You can receive system logging messages through a VRF interface on any router where you can configure a VRF, that is:

- On a provider edge (PE) router that is used in concert with Multiprotocol Label Switching (MPLS) and multiprotocol Border Gateway Protocol (BGP) to provide a Layer 3 MPLS VPN network service.

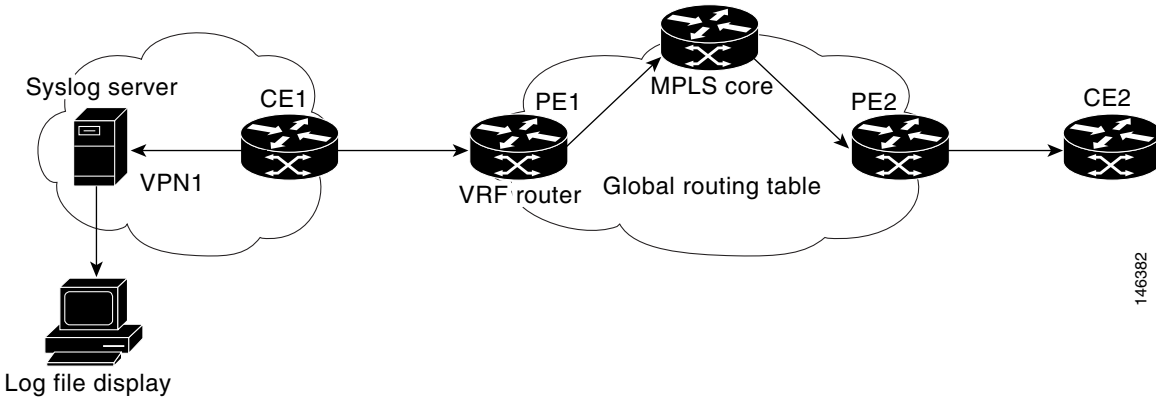
- On a customer edge (CE) device (switch or router) that is configured for VRF-Lite, which is a VRF implementation without multiprotocol BGP.

VRF Aware System Message Logging on Provider Edge Router in an MPLS VPN Network

You can configure the VRF Aware System Message Logging feature on a PE router in a Layer 3 MPLS VPN network. The PE router can then send syslog messages through a VRF interface to a syslog server located in the VPN.

Figure 1 shows an MPLS VPN network and the VRF Aware System Message Logging feature configured on a PE router associated with VRF VPN1. The PE router sends log messages through a VRF interface to a syslog server located in VPN1. You can display the messages from the syslog server on a terminal.

Figure 1 MPLS VPN and VRF Aware System Message Logging Configured on a Customer Edge Router

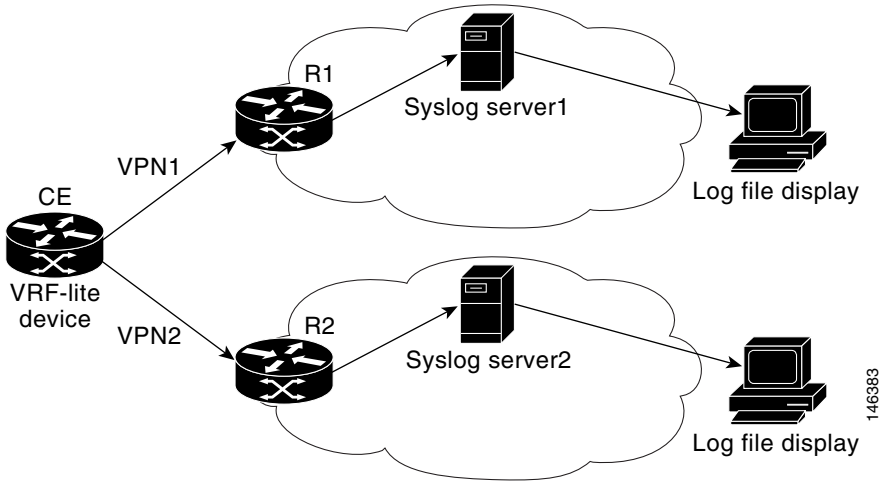


VRF Aware System Message Logging on a Customer Edge Device with VRF-Lite Configured

You can configure the VRF Aware System Message Logging feature on a CE device where you have configured the VRF-Lite feature. The CE device can then send syslog messages through a VRF interface to syslog servers in multiple VPNs. The CE device can be either a router or a switch.

Figure 2 shows the VRF Aware System Message Logging feature configured on a VRF-Lite CE device. The CE device can send VRF syslog messages to syslog servers in VPN1 or VPN2 or to servers in both VPN1 and VPN2. You can configure multiple VRFs on a VRF-Lite CE device, and the device can serve many customers.

Figure 2 VRF Aware System Message Logging Configured on a VRF-Lite Customer Edge Device



Message Levels for Logging Commands

Table 1 lists message levels for **logging** commands that you can use when you configure the VRF Aware System Message Logging feature. Information provided by Table 1 includes keyword level names and numbers, their description, and the associated syslog definitions. You can use either the level keyword name or number with the **logging trap** *level* and **logging buffered** *severity-level* commands.

Table 1 Message Levels for logging Commands

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

How to Configure and Verify VRF Aware System Message Logging

This section contains instructions on how to configure and verify the VRF Aware System Message Logging feature. The VRF Aware System Message Logging feature allows a router to send syslog messages to a syslog server host connected through the configured VRF interface.

You need to configure a VRF on the networking device and associate the VRF with an interface before you configure the VRF Aware System Message Logging feature on the device.

This section contains the following procedures:

Configuring a VRF on a Routing Device

Perform this task to configure a VRF instance on a routing device. Configuring a VRF on a routing device helps provides customer connectivity to a VPN. The routing device can be a PE router connected to an MPLS VPN network or a CE (switch or router) that is configured for VRF-Lite.

You must configure a VRF on a routing device and associate the VRF with an interface (see "Associating a VRF with an Interface" section on page 7) before you can configure the VRF Aware System Message Logging feature. The VRF Aware System Message Logging feature allows you to receive syslog messages through a VRF, in addition to receiving them through the global routing table.

For a link to more information about configuring VPNs, see the "Related Documents" section on page 13.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **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	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpn1`	Defines a VRF and enters VRF configuration mode. • The *vrf-name* argument is a name assigned to the VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF. • The *route-distinguisher* argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. • The route distinquisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. • You can enter an RD in either of these formats: – 16-bit autonomous system number: your 32-bit number For example, 101:3. – 32-bit IP address: your 16-bit number For example, 192.168.122.15:1.

	Command or Action	Purpose
Step 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target both 100:1`	Creates a route-target extended community for a VRF. • The **import** keyword imports routing information from the target VPN extended community. • The **export** keyword exports routing information to the target VPN extended community. • The **both** keyword imports routing information from and exports routing information to the target VPN extended community. • The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities. The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats: • 16-bit autonomous system 1 32-bit number For example, 101:3. • 32-bit IP address:your 16-bit number For example, 192.168.122.15: 1.
Step 6	**end** **Example:** `Router(config-vrf)# end`	Exits to privileged EXEC mode.

Associating a VRF with an Interface

Perform this task to associate a VRF instance with an interface. A VRF must be associated with an interface before you can forward VPN traffic.

Note You cannot configure a source address for VRF system logging messages. The VRF Aware System Message Logging feature uses the VRF interface address as the source address for all VRF-aware system logging messages.

After configuring the VRF and associating it with an interface, you can configure the VRF Aware System Message Logging feature on the routing device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **ip vrf forwarding** *vrf-name*
5. **end**
6. **copy running-config startup-config**

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	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. On Cisco 4700 series routers, it specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when the port, connector, or interface card is added to a system, and can be displayed with the **show interfaces** command.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding vpn1`	Associates a VRF with an interface or subinterface. • The *vrf-name* argument associates the interface with the specified VRF.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves configuration changes to NVRAM.

Configuring VRF Aware System Message Logging on a Routing Device

Perform this task to configure the VRF Aware System Message Logging feature on a routing device. This allows the sending of logging messages that can be used to monitor and troubleshoot network traffic connected through VRF instances.

Prerequisites

You must perform the following tasks before you perform this task:

- Configuring a VRF on a Routing Device, page 5
- Associating a VRF with an Interface, page 7

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging host** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
4. **logging trap** *level*
5. **logging facility** *facility-type*
6. **logging buffered** [*buffer-size* | *severity-level*]
7. **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*] **Example:** `Router(config)# logging host 10.0.150.63 vrf vpn1`	Specifies a host to receive syslog messages. • The *ip-address* argument is the IP address of the syslog server host. • The *hostname* argument is the name of the IP or IPv6 host that receives the syslog messages. • The **vrf** *vrf-name* keyword argument pair specifies a VRF that connects to the syslog server host.
Step 4	**logging trap** *level* **Example:** `Router(config)# logging trap debugging`	Limits messages logged to the syslog servers based on severity. • The *level* argument limits the logging of messages to the syslog servers to a specified level. You can enter the level number or level name. See Table 1 for a description of acceptable keywords.

	Command or Action	Purpose
Step 5	**logging facility** *facility-type* **Example:** `Router(config)# logging facility local6`	(Optional) Configures the syslog facility in which error messages are sent. • The *facility-type* argument names the syslog facility type keyword. For locally defined messages, the range of acceptable keywords is **local0** to **local7**. The default is **local7**.
Step 6	**logging buffered** [*buffer-size* | *severity-level*] **Example:** `Router(config)# logging buffered debugging`	(Optional) Limits messages logged to an internal buffer on the router based on severity. • The *buffer-size* argument is the size of the buffer from 4096 to 4,294,967,295 bytes. The default size varies by platform. • The *severity-level* argument limits the logging of messages to the buffer to a specified level. You can enter the level name or level number. See Table 1 for a list of the acceptable level name or level number keywords. The default logging level varies by platform, but is generally 7, meaning that messages at all levels (0–7) are logged to the buffer.
Step 7	**end** **Example:** `Router(config)# end`	(Optional) Exits to privileged EXEC mode.

Verifying VRF Aware System Message Logging Operation

Perform this task to verify VRF Aware System Message Logging operation.

SUMMARY STEPS

1. **enable**
2. **show running-config | include logging**
3. **show ip vrf interfaces**
4. **show running-config** [**interface** *type number*]
5. **ping vrf** *vrf-name target-ip-address*
6. **exit**

DETAILED STEPS

Step 1 enable

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

Step 2 **show running-config | include logging**

Use this command to display the logging configuration for the router and the logging host for a VRF. For example:

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

logging queue-limit 100
logging buffered 100000 debugging
mpls ldp logging neighbor-changes
logging trap debugging
logging facility local6
logging host vrf vpn1 10.0.150.63
Router#
```

This example shows the configuration of a syslog server in VRF vpn1 with a server host address of 10.0.150.63.

Step 3 **show ip vrf interfaces**

Use this command to display the interfaces associated with the VRF that links to a syslog server host. The following example displays a list of VRF interfaces and their associated IP addresses that are configured on the router:

```
Router# show ip vrf interfaces

Interface              IP-Address      VRF                              Protocol
FastEthernet0/0        10.0.0.98       vpn1                              up
Ethernet1/4            172.16.0.1      vpn1                              up
Loopback1              10.66.66.66     vpn1                              up
```

Step 4 **show running-config** [**interface** *type number*]

Use this command to display interface specific configuration information for an interface associated with a VRF. For example:

```
Router# show running-config interface FastEthernet 0/0

Building configuration...
Router#
.
.
.
!
Current configuration : 116 bytes
!

interface FastEthernet0/0
 ip vrf forwarding vpn1
 ip address 10.0.0.98 255.0.0.0
 duplex half
 no cdp enable
end
```

This example displays configuration information for Fast Ethernet interface 0/0 in VRF vpn1.

Step 5 **ping vrf** *vrf-name target-ip-address*

Use this command to verify that you can reach the syslog server host, the *target-ip-address*, through the specified VRF. For example:

```
Router# ping vrf vpn1 10.3.199.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.199.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

In this example, the syslog server has an IP address of 10.3.199.1 and the VRF is named vpn1. The server is reached successfully four of five times.

Step 6 **exit**

Use this command to exit privileged EXEC mode. For example:

```
Router# exit
Router>
```

Configuration Examples for VRF Aware System Message Logging

This section contains the following configuration examples for the VRF Aware System Message Logging feature:

- Configuring a VRF on a Routing Device: Example, page 12
- Configuring VRF Aware System Message Logging on a Routing Device: Example, page 13

Configuring a VRF on a Routing Device: Example

The following example shows how to configure a VRF on a routing device:

```
enable
configure terminal
!
ip vrf vpn1
 rd 100:1
 route-target both 100:1
 end
```

Associating a VRF with an Interface: Example

The following example shows how to associate a VRF with an interface:

```
enable
configure terminal
!
interface FastEthernet 0/0
 ip vrf forwarding vpn1
 end
```

Configuring VRF Aware System Message Logging on a Routing Device: Example

The following example shows how to configure the VRF Aware System Message Logging feature on a routing device. The IP address of the syslog server host is 10.10.150.63 and the VRF is vpn1.

```
enable
configure terminal
!
 logging host 10.0.150.63 vrf vpn1
 logging trap debugging
 logging facility local6
 logging buffered 10000
 logging buffered debugging
 end
```

The following example shows how to turn off logging to the syslog server:

```
enable
configure terminal
!
 no logging 10.0.150.63
 end
```

Additional References

The following sections provide references related to configuring the VRF Aware System Message Logging feature.

Related Documents

Related Topic	Document Title
Concepts and tasks for configuring MPLS VPNs	"Configuring MPLS Layer 3 VPNs" module
Basic tasks for troubleshooting your system and the network	"Troubleshooting, Logging, and Fault Management" chapter of the *Cisco IOS Network Management Configuration Guide*, Release 12.4
Concepts and configuration tasks for MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4
Concepts and tasks for configuring VRF-lite on a Catalyst 4500 switch	"Configuring VRF-lite" chapter, *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*, 12.2(25)EWA
Concepts and tasks for configuring VRF Lite on ML-Series Ethernet cards	"Configuring VRF Lite" chapter, *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, ONS 15454, and ONS 15327*, Release 6.0

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

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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents the following modified command only.

- **logging host**

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-number*]] [**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.
12.4(13)	This command was integrated into Cisco IOS Release 12.4(13).
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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 in a given syslog session.

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

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

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

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

Examples

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

```
Router(config)# logging host 192.168.202.169
Router(config)# logging trap 5
```

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

```
Router(config)# logging host 192.168.200.225
Router(config)# logging host 192.168.200.226 xml
Router(config)# logging host 192.168.200.227 filtered stream 10
Router(config)# logging host 192.168.202.129 filtered stream 20
```

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

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

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

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

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

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

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

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

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

```
Router(config)# logging host host2 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.

Feature Information for VRF Aware System Message Logging

Table 2 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.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 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 2 Feature Information for VRF Aware System Message Logging

Feature Name	Releases	Feature Information
VRF Aware System Message Logging (Syslog)	12.4(4)T 12.2(33)SRA 12.2(31)SB2 12.4(13) 12.2(33)SXH	The VRF Aware System Message Logging feature allows a router to send syslog messages to a syslog server host connected through a VRF interface. In 12.4(4)T, this feature was introduced. In 12.2(33)SRA, this feature was integrated into a 12.2SRA release. In 12.2(31)SB, support was added for the Cisco 10000 series routers. In 12.4(13), this feature was integrated into a 12.4 release. In 12.2(33)SXH, this feature was integrated into a 12.2SXH release. The following sections provide information about this feature: • VRF Aware System Message Logging Benefit—Monitoring and Troubleshooting Network Traffic Connected Through a VRF, page 2 • VRF Aware System Message Logging on Provider Edge Router in an MPLS VPN Network, page 3 • VRF Aware System Message Logging on a Customer Edge Device with VRF-Lite Configured, page 3 • Message Levels for Logging Commands, page 4 • Configuring a VRF on a Routing Device, page 5 • Configuring VRF Aware System Message Logging on a Routing Device, page 8 • Verifying VRF Aware System Message Logging Operation, page 10 The following command was modified by this feature: **logging host**.

Glossary

CE router—customer edge router. A router on the border between a VPN provider and a VPN customer that belongs to the customer.

LSR—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

MPLS—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS VPN—Multiprotocol Label Switching Virtual Private Network. An IP network infrastructure delivering private network services over a public infrastructure using a Layer 3 backbone. Using MPLS VPNs in a Cisco IOS network provides the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.

PE router—provider edge router. A router on the border between a VPN provider and a VPN customer that belongs to the provider.

VPN—Virtual Private Network. A group of sites that, as the result of a set of administrative policies, are able to communicate with each other over a shared backbone network. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone. *See also* MPLS VPN.

VRF—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.