



SNMP Support for VPNs

Feature History

Feature History

Release	Modification
12.2(2)T	This feature was introduced.
12.0(23)S	This feature was integrated into Cisco IOS Release 12.0 S.

The document describes the SNMP Support for VPNs feature in Cisco IOS Release 12.2(2)T. It includes the following sections:

- Feature Overview, page 1
- Benefits, page 2
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Configuration Tasks, page 4
- Configuration Examples, page 4
- Command Reference, page 5

Feature Overview

The SNMP Support for VPNs feature allows the sending and receiving of SNMP notifications (traps and informs) using VPN routing/forwarding (VRFs) tables. In particular, this feature adds support to Cisco IOS software for the sending and receiving of SNMP notifications (traps and informs) specific to individual Virtual Private Networks (VPNs).

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A Virtual Private Network (VPN) is a network that provides high connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet over IP, Frame Relay, or ATM networks.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support for VPNs feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

Benefits

This feature allows users to configure an SNMP agent to only accept SNMP requests from a certain set of VPNs. With this configuration, providers can provide network management services to their customers, so customers can manage all user VPN devices.

Related Documents

For details on configuring SNMP, refer to the following documents:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2

For information about configuring a VRF table, refer to the “Configuring Multiprotocol Label Switching” chapter of the *Cisco IOS Switching Services Configuration Guide*, Release 12.2.

Supported Platforms

This feature is supported in images for the following platforms:

- Cisco 800 series
- Cisco 1000 series
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2600 series
- Cisco 2900 series
- Cisco 3620 routers
- Cisco 3640 routers
- Cisco 3660 routers
- Cisco 3800 series
- Cisco 4000 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco AS5300
- Cisco AS5800
- Cisco AS5350
- Cisco LightStream1010 ATM switch
- Cisco RPM Images
- Cisco VG200
- Cisco 8510 switch
- Cisco 8540 switch
- Cisco 15104 ONS (regen images)

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the SNMP Support over VPNs feature. Each task in the list is identified as either required or optional:

- Configuring SNMP Support for a VPN (required)
- Verifying SNMP Support for VPNs (optional)

Configuring SNMP Support for a VPN

To configure SNMP over a specific VPN, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server host <i>host-address</i> [traps informs][version { 1 2c 3 [auth noauth priv]}] <i>community-string</i> [udp-port <i>port</i>][<i>notification-type</i>][vrf <i>vrf-name</i>]	Specifies the recipient of an SNMP notification operation and specifies the VRF table to be used for the sending of SNMP notifications.

To configure SNMP over a specific VPN for a remote SNMP user, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server engineID remote <i>ip-address</i> [udp-port <i>udp-port-number</i>][vrf <i>vrf-name</i>] <i>engineid-string</i>	Configures a name for the remote SNMP engine on a router.

Verifying SNMP Support for VPNs

To verify that the SNMP Support over VPNs feature is configured properly, use the **show snmp-server host EXEC** command.

Configuration Examples

This section provides the following configuration example:

- Configuring SNMP Support over VPNs Example

Configuring SNMP Support over VPNs Example

The following example sends all SNMP notifications to xyz.com over the VRF named “trap-vrf”:

```
Router(config)# snmp-server host xyz.com vrf trap-vrf
```

The following example configures the VRF named “traps-vrf” for the remote server 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf  
80000009030000B064EFE100
```

Command Reference

This section documents the following modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **snmp-server engineID remote**
- **snmp-server host**
- **snmp-server user**

snmp-server engineID remote

To configure a name for the remote Simple Network Management Protocol (SNMP) engine on a router, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

```
snmp-server engineID remote ip-address [udp-port udp-port-number] [vrf vrf-name]
engineid-string
```

```
no snmp-server engineID remote
```

Syntax Description		
	<i>ip-address</i>	The IP address of the device that contains the remote copy of SNMP.
	udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
	<i>udp-port-number</i>	(Optional) The socket number on the remote device that contains the remote copy of SNMP. The default is 161.
	vrf	(Optional) Instance of a routing table.
	<i>vrf-name</i>	(Optional) Name of the VPN routing/forwarding (VRF) table to use for storing data.
	<i>engineid-string</i>	The name of a copy of SNMP.

Defaults UDP port: 161

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.2(2)T	The vrf keyword and <i>vrf-name</i> argument were introduced.

Usage Guidelines You need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. To configure an engine ID of 123400000000000000000000, you can specify the value 1234, for example, **snmp-server engineID remote 1234**.

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples The following example configures the VRF name traps-vrf for the remote server 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

Related Commands	Command	Description
	show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
	snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server host

To specify the recipient of a SNMP notification operation and the VRF table to be used for the sending of SNMP notifications, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

```
snmp-server host host-address [traps | informs][version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port][notification-type] [vrf vrf-name]
```

```
no snmp-server host host-address [traps | informs]
```

Syntax Description	
<i>host-address</i>	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> • 1 —SNMPv1. This option is not available with informs. • 2c —SNMPv2C. • 3 —SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> – auth—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – noauth—The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified. – priv—Enables Data Encryption Standard (DES) packet encryption (also called ‘privacy’).
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string using the snmp-server host command by itself, we recommend you define this string using the snmp-server community command prior to using the snmp-server host command.
udp-port <i>port</i>	(Optional) User Datagram Protocol (UDP) port of the host to use. The default is 162.

<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • config—Sends configuration notifications. • dspu—Sends downstream physical unit (DSPU) notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • frame-relay—Sends Frame Relay notifications. • hsrp—Sends Hot Standby Routing Protocol (HSRP) notifications. • isdn—Sends ISDN notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • repeater—Sends standard repeater (hub) notifications. • rsrb—Sends remote source-route bridging (RSRB) notifications. • rsvp—Sends Resource Reservation Protocol (RSVP) notifications. • rtr—Sends Service Assurance Agent (RTR) notifications. • sdlc—Sends Synchronous Data Link Control (SDLC) notifications. • sdllc—Sends SDLC Logical Link Control (SDLLC) notifications. • snmp—Sends SNMP notifications (as defined in RFC 1157). • stun—Sends serial tunnel (STUN) notifications. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command. • tty—Sends Cisco enterprise-specific notifications when a TCP connection closes. • x25—Sends X.25 event notifications.
vrf <i>vrf-name</i>	<p>(Optional) Instance of a Virtual Private Network (VPN) routing/forwarding (VRF) table. Name of the VRF that should be used to send SNMP notifications.</p>

Defaults

version: noauth

port: 162

If no **version** keyword is present, the default is version 1. The **no snmp-server host** global configuration command with no keywords will disable all of the notifications (both traps and informs). In order to disable informs, use the **no snmp-server host informs** global configuration command.



Note

If the community string is not defined using the **snmp-server community** global configuration command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password

(*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later releases.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: <ul style="list-style-type: none"> • version 3 [auth noauth priv] • hsrp
12.2(2)T	The vrf <i>vrf-name</i> keyword/argument combination was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are less reliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host but with different variables, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** global configuration command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

Availability of notification type option depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system.

The added **vrf** keyword allows users to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so data is stored using the VPN.

Examples

The following example sends all SNMP notifications to xyz.com over the VRF named trap-vrf:

```
Router(config)# snmp-server host xyz.com vrf trap-vrf
```

Related Commands

Command	Description
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often attempts are made to resend trap messages on the retransmission queue.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of the command.

```
snmp-server user username groupname [remote host [udp-port udp-port-number]] {v1 | v2c | v3
encrypted} [auth {md5 | sha} auth-password] [access access-list] [vrf vrf-name]
```

```
no snmp-server user
```

Syntax Description

<i>username</i>	The name of the user on the host that connects to the agent.
<i>groupname</i>	The name of the group to which the user belongs.
remote <i>host</i>	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IP address of that entity.
udp-port <i>port</i>	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted and/or auth keywords.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
<i>auth-password</i>	A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
access <i>access-list</i>	(Optional) Specifies an access list to be associated with this SNMP user. The <i>access-list</i> argument represents a value between 1 and 99 that is the identifier of the standard IP access list.
vrf <i>vrf-name</i>	(Optional) Instance of a Virtual Private Network (VPN) routing/forwarding (VRF) table. For the <i>vrf-name</i> argument, specify the remote SNMP entity's VPN Routing instance.

Defaults

Table 1 describes default behaviours for encryption, passwords and access lists.

Table 1 *snmp-server user* Default Descriptions

Characteristic	Default
encryption	Not present by default. The encrypted keyword is used to specify that the auth and priv passwords are MD5 digests and not text passwords.
passwords	Assumed to be text strings.

Table 1 *snmp-server user Default Descriptions*

Characteristic	Default
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the remote keyword.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(2)T	The vrf vrf-name keyword/argument combination was introduced

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the command **snmp-server engineID** with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication/privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

If a VPN table (VRF) is specified, the vrf-name should match the VRF specified with the **ip vrf vrf-name** command.

Examples

In the following example, the SNMP user "usmusr" in the SNMP group "group1" is configured to use the VRF "6400-private":

```
Router(config)# snmp-server group group1 v3 noauth
Router(config)# snmp-server user usmusr group1 v3
Router(config)# snmp-server host 10.100.100.100 vrf 6400-private version 3 noauth trapusr
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode and defines a VPN routing instance by assigning a VRF name.
show snmp user	Displays information on each SNMP username in the group username table.

