Configure Supported Cisco IOS SNMP Traps

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Commands

- The snmp-server host Command
- Syntax Description

Defaults

Command Modes

- Global Configuration - Command History
- Use Guidelines
- Configure Informs
- Examples

The snmp-server enable traps Command

- Syntax Description
- Defaults

Command Modes

- Global Configuration - Command History
- Use Guidelines

Related Information

Introduction

This document describes how to configure supported Cisco IOS® SNMP Traps.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

You do not want a Cisco device to send all of the SNMP traps that the device knows how to send. For instance, if you enable all traps in a Remote Access Server with 64 dial-in lines, you get a trap whenever a user dials in and whenever a user terminates the connection. This creates too many traps. Cisco IOS Software defines groups of traps that you can enable or disable. There are two global configuration commands that you use to configure SNMP traps into a Cisco IOS Software device:

- <#root>

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

Issue the snmp-server host global configuration command to specify the recipient of an SNMP notification operation. Issue the **no** form of this command to remove the specified host.

- <#root>

```
snmp-server enable traps [notification-type] [notification-option]
```

Issue the **snmp-server enable traps global configuration** command to enable the router to send SNMP traps. Issue the **no** form of this command in order to disable SNMP notifications.

The types of traps can be specified in both commands. You must issue the **snmp-server host** command in order to define the Network Management Systems where traps are to be sent. You must specify the trap types if you do not want all traps to be sent. Issue multiple **snmp-server enable traps** commands, one for each of the trap types that you used in the **snmp host** command.

Note: Not all [notification-type] options are supported on both of these commands. For example, [notification-type] x25 and teletype (tty) are not used for **snmp-server enable trap** x25, and tty traps are enabled by default.

For example, issue these commands to make a Cisco IOS Software device report only configuration, Border Gateway Protocol (BGP), and tty traps to Network Management System 10.10.10.10:

<#root>

```
snmp-server host 10.10.10.10 public config bgp tty
snmp-server enable traps config
snmp-server enable traps bgp
```

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Note: Cisco IOS Software Release 12.1(3)T was used to prepare this document. When you use an

---

earlier Cisco IOS Software Release, not all options are supported. When you use a Cisco IOS Software release later than 12.1(3)T, additional [notification-type] options can be supported. You can find a current list of all supported Cisco IOS Software Simple Network Management Protocol (SNMP) trap Object Identifiers (OIDs) in this document.

Cisco devices that run the standard Cisco IOS Software (routers, Asynchronous Transfer Mode (ATM) switches and Remote Access Servers) can generate many SNMP traps.

Commands

The snmp-server host Command

Issue the **snmp-server host global configuration** command to specify the recipient of an SNMP notification operation. Issue the **no** form of this command to remove the specified host.

<#root>

```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type]
no snmp-server host host [traps | informs]
```

Syntax Description

host-addr	The name or Internet address of the host (the targeted recipient).
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) The version of the SNMP used to send the traps. Version 3 is the most secure model, as this model allows packet encryption with the **priv** keyword. If you use the version keyword, you must specify one of these options: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C • **3**—SNMPv3. These three optional keywords can be after the version 3 keyword: ◦ **auth** (Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. ◦ **noauth** (Default) The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified. ◦ **priv** (Optional) Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	The password-like community string sent with the notification operation. Though you can set this string with the **snmp-server host** command by itself, Cisco recommends that you define this string with the **snmp-server community** command before you issue the **snmp-server host** command.
udp-port*port*	User Datagram Protocol (UDP) port of the host to use. The default is 162.
notification-type	(Optional) The 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 these keywords: • **aaa-server** — Sends AAA notifications. • **bgp** — Sends Border Gateway Protocol (BGP) state change notifications.

	• **bstun**— Sends Block Serial Tunneling (BSTUN) notifications. • **calltracker**— Sends CallTracker notifications. • **config**— Sends configuration notifications. • **dlsw**— Sends data-link switching (DLSw) notifications. • **ds0-busyout**— Sends ds0-busyout notifications. • **ds1-loopback**— Sends ds1-loopback notifications. • **dspu**— Sends downstream physical unit (DSPU) notifications. • **dsp**— Sends digital signal processing (DSP) notifications. • **entity**— Sends Entity Management Information Base (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 Router Protocol (HSRP) notifications. • **isdn** — Sends Integrated Services Digital Network (ISDN) notifications. • **msdp** — Sends Multicast Source Discovery Protocol (MSDP) 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 SA Agent (RTR) notifications. • **sdlc** — Sends Synchronous Data Link Control (SDLC) notifications. • **snmp** — Sends Simple Network Management Protocol (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 Transmission Control Protocol (TCP) connection closes. • **voice**— Sends voice notifications. • **x25**— Sends X.25 event notifications. • **xgcp**— Sends External Media Gateway Control Protocol (XGCP) notifications.

Defaults

The **snmp-server host** command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host.

No informs are sent to this host. If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. Issue the **no snmp-server host informs** command to disable informs.

Note: If the *community-string* is not defined with the **snmp-server community** command before you use this command, the default form of the **snmp-server community** command is automatically inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** is the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Software Release 12.0(3) and later.

Command Modes

Global Configuration - Command History

Cisco IOS Software Release	Modification
10.0	Command introduced.
12.0(3)T	These keywords have been added: • **version 3 [auth | noauth | priv]** • **hsrp**

Use Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device 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 protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Therefore, 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. Traps are sent only once, while an inform can 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 command overwrites the previous command. Only the last **snmp-server host** command is taken into account. 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, the second command replaces the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Issue the **snmp-server enable** command in order to specify which SNMP notifications are sent globally. In order 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.

The availability of a 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.

Configure Informs

Complete these steps to be able to send an inform:

1. Configure a remote engine ID.

2. Configure a remote user.
3. Configure a group on a remote device.
4. Enable traps on the remote device.
5. Enable the SNMP manager.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration must include an access-list. In this example, the community string is named **comaccess**, and the access list is numbered 10:

```
<#root>

snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

This example sends the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
<#root>

snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

This example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
<#root>

snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

This example enables the router to send all traps to the host myhost.cisco.com with the community string public:

```
<#root>

snmp-server enable traps
snmp-server host myhost.cisco.com public
```

This example does not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

<#root>

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

This example enables the router to send all inform requests to the host myhost.cisco.com with the community string public:

<#root>

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version
```

This example sends HSRP SNMPv2c traps to the host specified by the name myhost.cisco.com. The community string is defined as public.

<#root>

```
snmp-server enable traps
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The snmp-server enable traps Command

Use the **snmp-server enable traps** global configuration command to enable the router to send SNMP traps. Use the **no** form of this command to disable SNMP notifications.

<#root>

```
snmp-server enable traps [notification-type] [notification-option]
```

```
no snmp-server enable traps [notification-type] [notification-option]
```

Syntax Description

notification-type	(Optional) The type of notification to enable. If no type is specified, all notifications are sent (that includes the **envmon** and **repeater** notifications). The notification type can be one of these keywords: • **aaa-server**— Sends AAA Server notifications. This keyword is added since Cisco IOS Software Release 12.1(3)T for Cisco AS5300 and AS5800 platforms only. This is from the CISCO-AAA-SERVER-MIB and the notifications are: enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange

- **bgp** — Sends Border Gateway Protocol (BGP) state change notifications. This is from the BGP4-MIB, and the notifications are: enterprise 1.3.6.1.2.1.15.7 1 bgpEstablished 2 bgpBackwardTransition
- **calltracker** — Sends a notification whenever a new active call entry is created in the cctActiveTable or a new history call entry is created in the cctHistoryTable This is from the CISCO-CALL-TRACKER-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTerminateNotification
- **config** — Sends configuration notifications. This is from the CISCO-CONFIG-MAN-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent
- **dial** — Sends a notification whenever a successful call clears, a failed call attempt is determined to have ultimately failed, or whenever a call setup message is received or sent. This is from the DIAL-CONTROL-MIB, and the notifications are: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup
- **dlsw** — Sends notifications from DLSw agents When the **dlsw** keyword is used, you can specify a*notification-option*value. This is from the CISCO-DLSW-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProtViolation 3 ciscoDlswTrapTConnUp 4 ciscoDlswTrapTConnDown 5 ciscoDlswTrapCircuitUp 6 ciscoDlswTrapCircuitDown
- **ds0-busyout**— Sends a notification whenever the busyout of a DS0 interface changes state. This keyword is added since Cisco IOS Software Release 12.1(3)T for the Cisco AS5300 platform only. This is from the CISCO-POP-MGMT-MIB, and the notification is: enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification
- **ds1-loopback**— Sends a notification whenever the DS1 interface goes into loopback mode. This keyword is added since Cisco IOS Software Release 12.1(3)T for the Cisco AS5300 platform only. This is from the CISCO-POP-MGMT-MIB, and the notification is: enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification
- **dspu**— Sends a notification whenever the operational state of the physical unit (PU) or the logical unit (LU) changes or activation failure is detected. This is from the CISCO-DSPU-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap enterprise 1.3.6.1.4.1.9.9.24.1.5.3 1 newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap
- **dsp**— Sends a notification whenever the DSP card goes up or down. This is from the CISCO-DSP-MGMT-MIB, and the notification is: enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- **entity**— Sends Entity MIB modification notifications. This is from the ENTITY-MIB, and the notifications are: enterprise 1.3.6.1.2.1.47.2 1 entConfigChange
- **envmon**— Sends Cisco enterprise-specific environmental monitoring notifications when an environmental threshold is exceeded. When the **envmon** keyword is used, you can specify a*notification-option*value. This is from the CISCO-ENVMON-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification
- **frame-relay**— Sends Frame Relay notifications. This is from the RFC1315-MIB, and the notifications are: enterprise 1.3.6.1.2.1.10.32 1 frDLCIStatusChange
- **hsrp**— Sends Hot Standby Router Protocol (HSRP) notifications. This feature is supported since Cisco IOS Software Release 12.0(3)T. This is from the CISCO-HSRP-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange
- **isdn**— Sends ISDN notifications. When the **isdn** keyword is used, you can specify a*notification-option*value. This is from the CISCO-ISDN-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.26.2 1 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Change [supported since Cisco IOS Software Release 12.1(1)T] 4 demandNbrCNANotification [supported since Cisco IOS Software Release 12.1(5)T] This is from the CISCO-ISDNU-IF-MIB, and the notifications are: enterprise

	1.3.6.1.4.1.9.9.18.2 1 ciuIfLoopStatusNotification • **msdp**— Sends Multicast Source Discovery Protocol (MSDP) notifications. This is from the MSDP-MIB, and the notifications are: enterprise 1.3.6.1.3.92.1.1.7 1 msdpEstablished 2 msdpBackwardTransition • **repeater** — Sends Ethernet hub **repeater** notifications. When the **repeater** keyword is selected, you can specify a notification-option value. This is from the CISCO-REPEATER-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap • **rsvp** — Sends Resource Reservation Protocol (RSVP) notifications. This feature is supported since Cisco IOS Software Release 12.0(2)T. This is from the RSVP-MIB, and the notifications are: enterprise 1.3.6.1.3.71.2 1 newFlow 2 lostFlow • **rtr** — Sends Service Assurance Agent RTR (RTR) notifications. This is from the CISCO-RTTMON-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification • **snmp** — Sends Simple Network Management Protocol (SNMP) notifications. When the**snmp**keyword is used, you can specify a notification-option value. This is from the CISCO-GENERAL-TRAPS, and the notifications are: enterprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborLoss enterprise 1.3.6.1.4.1.9 0 reload **Note**:This trap is controlled by the notification-type "tty": 1 tcpConnectionClose • **syslog**— Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. This is from the CISCO-SYSLOG-MIB, and the notifications are: enterprise 1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated • **voice**— Sends poor quality of voice notifications. This is from the CISCO-VOICE-DIAL-CONTROL-MIBSMI, and the notifications are: enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification • **xgcp**— Sends External Media Gateway Control Protocol (XGCP) notifications. This is from the XGCP-MOB, and the notifications are: enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification
notification-option	(Optional) • **dlsw [circuit | tconn]** — When the**dlsw**keyword is used, you can specify the specific notification type you wish to enable or disable. If no keyword is used, all DLSw notification types are enabled. The option can be one or more of these keywords: ◦ **circuit** — Enables DLSw circuit traps. ◦ **tconn** — Enables DLSw peer transport connection traps. • **envmon [voltage | shutdown | supply | fan | temperature]**— When the**envmon**keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of these keywords:**voltage,shutdown,supply,fan,** and**temperature.** • **isdn [call-information | isdn u-interface | chan-not-avail | layer2]** — When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdn u-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem. • **repeater [health | reset]** — When the **repeater** keyword is used, you can specify the repeater option. If no option is specified, all repeater notifications are enabled. The option can be

	one or more of these keywords: health--Enables Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification. reset--Enables IETF Repeater Hub MIB (RFC 1516) reset notification. ◦ **health** — Enables the Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification. ◦ **reset** — Enables the IETF Repeater Hub MIB (RFC 1516) reset notification. • **snmp [authentication | linkup | linkdown | coldstart]** keywords **linkup | linkdown | coldstart** added since Cisco IOS Software Release 12.1(3)T. — When the **snmp** keyword is used, you can specify the specific notification type you wish to enable or disable. If no keyword is used, all SNMP notification types are enabled (or disabled, if the no form is used). The notification types available are: ◦ **authentication** — Controls the distribution of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. ◦ **linkup** — Controls the sending of SNMP linkup notifications. A linkUp(3) trap signifies that the sending protocol entity recognizes that one of the communication links represented in the configuration of the agent has come up. ◦ **linkdown** — Controls the how SNMP linkdown notifications are sent. A linkDown(2) trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the configuration of the agent. ◦ **coldstart** — Controls the sending of SNMP coldstart notifications. A coldStart(0) trap signifies that the sending protocol entity is reinitializes itself such that the configuration of the agent or the protocol entity implementation can be altered.

Defaults

SNMP notifications are disabled.

If you enter this command with no notification-type keywords, the default is to enable all notification types controlled by this command.

Command Modes

Global Configuration - Command History

Cisco IOS Software Release	Modification
11.1	This command was introduced.
12.0(2)T	The **rsvp** keyword was added.
12.0(3)T	The **hsrp** keyword was added.
12.1(3)T	These keywords have been added to the **snmp-server enable traps snmp** form of this command: • **linkup** • **linkdown** • **coldstart** These notification type keywords have been added for the Cisco AS5300 platform only:

	• **ds0-busyout** • **isdn chan-not-avail** • **modem-health** • **ds1-loopback** This notification type keyword has been added for the Cisco AS5300 and AS5800 platforms only: • **aaa-server**

Use Guidelines

The **snmp-server enable traps snmp [linkup] [linkdown]** form of this command replaces the **snmp trap link-status interface** configuration mode command.

The **no** form of the **snmp-server enable traps** command is useful in order to disable notifications that generate a large amount of unneeded noise on your network.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Issue the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

In order for a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, only the appropriate **snmp-server host** command must be enabled.

The notification types used in this command all have an associated MIB object that allows them to be enabled or disabled (for example, HSRP traps are defined with the HSRP MIB, repeater traps are defined with the Repeater Hub MIB, and so on). Not all of the notification types available in the **snmp-server host** command have **notificationEnable MIB** objects, so some of these cannot be controlled with the **snmp-server enable** command.

Related Information

- **Cisco Technical Support & Downloads**