snmp-server engineID local through snmp trap link-status

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*
no snmp-server engineID local *engineid-string*

Syntax Description

engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administrative purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.

If you specify your own ID, note that the entire 24-character engine ID is not needed if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify **snmp-server engineID local 1234**.

The value for the engine ID is displayed in hexadecimal value pairs. If the length of the input is an odd number, the last digit will be prepended with a zero ("0"). For example, if the engine ID is 12345, the ID is treated as 12:34:05 internally. Hence, the engine ID is displayed as 123405 in the **show running configuration** command output.

Changing the value of the SNMP engine ID has significant effects. A user's password (entered on the command line) is converted to a message digest5 algorithm (MD5) or Secure Hash Algorithm (SHA) security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the engineID changes, the security digests of SNMPv3 users will become invalid, and the users will have to be reconfigured.

Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 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 specifies the local SNMP engine ID:

```
Router(config)# snmp-server engineID local
```

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 file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group {*acl-numberacl-name*} [**protocol** *p-name*]
no snmp-server file-transfer access-group {*acl-numberacl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.
protocol	(Optional) Enables the user to associate a named protocol with an access group.
p-name	(Optional) Name of a transfer protocol. Valid values are: **ftp**, **rcp**, **scp**, **sftp**, and **tftp**.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration

Command History

Release	Modification
12.4(12)	This command was introduced.
	This command replaces the **snmp-server tftp-server-list** command.

Usage Guidelines

The **snmp-server tftp-server-list** command is still supported in Cisco IOS software, but if it is configured as **snmp-server tftp-server-list 10**, it will be substituted with the **snmp-server file-transfer access-group 10 protocol tftp**command.

Use the **snmp-server file-transfer access-group**command to restrict configuration transfers that are initiated via Simple Network Management Protocol (SNMP). You can restrict transfers for specific transfer protocols by associating an access list to the protocol.

Examples

The following example associates access group 10 to the transfer protocols FTP and RCP:

```
Router(config)# snmp-server file-transfer access-group 10 protocol ftp
Router(config)# snmp-server file-transfer access-group 10 protocol rcp
```

Related Commands

Command	Description
snmp-server tftp-server-list	Associates TFTP servers used via SNMP controlled TFTP operations to the servers specified in an access list.

snmp-server group

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

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [{*acl-numberacl-name*}]]
no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description		
group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model.
	The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model.
	SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view.
	The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view.
	The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view.
	By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user).
	Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default   No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The notify-view option is available for two reasons:

   • If a group has a notify view that is set using SNMP, you may need to change the notify view.

   • The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

   • The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.

   • Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1.   **snmp-server user** --Configures an SNMP user.

2.   **snmp-server group** --Configures an SNMP group, without adding a notify view .

3.   **snmp-server host** --Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

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

no snmp-server host {*hostnameip-address*} [{**vrf** *vrf-name* | **informs** | **traps** | **version** {**1** | **2c** | **3** [{**auth** | **noauth** | **priv**}]}}] *community-string* [{**udp-port** *port* [*notification-type*]*notification-type*}]

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

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

no snmp-server host *ip-address* {*community-string* | **informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth**}}} {*community-string* | **vrf** *vrf-name* {**informs** | **traps**}} [{*notification-type*}]

Command Syntax on Cisco 7600 Series Router

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

no snmp-server host *ip-address* {*community-string* | {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string* | **vrf** *vrf-name* {**informs** | **traps**} {*community-string* | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}} *community-string*}}} [*notification-type*]

Syntax Description		
hostname	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.	
ip-address	IPv4 address or IPv6 address of the SNMP notification host.	
vrf	(Optional) Specifies that a VPN routing and forwarding (VRF) instance should be used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the **vrf** keyword is required.	
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the *vrf-name* argument is required.	
informs	(Optional) Specifies that notifications should be sent as informs. • In Cisco IOS Release 12.2(54)SE, the **informs** keyword is required.	
traps	(Optional) Specifies that notifications should be sent as traps. This is the default. • In Cisco IOS Release 12.2(54)SE, the **traps** keyword is required.	

version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1.
	• In Cisco IOS Release 12.2(54)SE, the **version** keyword is required and the **priv** keyword is not supported.
	If you use the **version** keyword, one of the following keywords must be specified:
	• **1** --SNMPv1.
	• **2c** --SNMPv2C.
	• **3** --SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**.
	One of the following three optional security level keywords can follow the **3** keyword:
	• **auth** --Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
	• **noauth** --Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
	• **priv** --Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation.
	Note You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command.
	Note The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an network management system (NMS) host.
	• In Cisco IOS Release 12.2(54)SE, the **udp-port** keyword is not supported.
port	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162.
	• In Cisco IOS Release 12.2(54)SE, the *port* argument is not supported.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the "Usage Guidelines" section for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was modified. • The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
	12.1(3)T	This command was modified. The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
	12.2(2)T	This command was modified. • The **vrf** *vrf-name* keyword-argument pair was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series routers.
	12.2(4)T	This command was modified. • The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
	12.2(8)T	This command was modified. • The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
	12.2(13)T	This command was modified. • The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
	12.3(2)T	This command was modified. • The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
	12.3(4)T	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf notification-type** keyword was added.

Release	Modification
12.3(8)T	This command was modified. The **iplocalpool notification-type** keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	This command was modified. The **vrrp** keyword was added.
12.3(14)T	This command was modified. • Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	This command was modified. The **license** notification-type keyword was added.
15.0(1)M	This command was modified. • The **nhrp** notification-type keyword was added. • The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, was changed. The **snmp-server community** command must be manually configured.
12.0(17)ST	This command was modified. The **mpls-traffic-eng** notification-type keyword was added.
12.0(21)ST	This command was modified. The **mpls-ldp notification-type** keyword was added.
12.0(22)S	This command was modified. • All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	This command was modified. The **l2tun-session** notification-type keyword was added.
12.0(26)S	This command was modified. The **memory** notification-type keyword was added.
12.0(27)S	This command was modified. • Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	This command was modified. The **l2tun-pseudowire-status** notification-type keyword was added.

Release	Modification
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was 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.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	This command was modified. • The **dhcp-snooping** notification-type keyword was added. • The **errdisable** notification-type keyword was added.
12.2(54)SE	This command was modified. See the SNMP server host commands for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The **public storm-control** notification-type keyword was added.
15.0(1)S	This command was modified. The **flowmon notification-type** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(1)S	This command was modified. The **p2mp-traffic-eng** notification-type keyword was added.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

> **Note** If a community string is not defined using the **snmp-server community** 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** command will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the **snmp-server community** command. That is, the **snmp-server community** command will not be seen in the configuration.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable 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 protocol data unit (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 than traps.

Compared to traps, 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; an inform may be tried 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. 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 optional keywords, all trap types are enabled for the host.

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, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** 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.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others 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 notification-type options depends on the router type and the 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. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

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

In the case of the NMS sending the query having a correct SNMP community but not having a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.

- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The notification type can be one or more of the following keywords.

> **Note** The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server** --Sends SNMP authentication, authorization, and accounting (AAA) traps.

- **adslline** --Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.

- **atm** --Sends ATM notifications.

- **authenticate-fail** --Sends an SNMP 802.11 Authentication Fail trap.

- **auth-framework** --Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.

- **bgp** --Sends Border Gateway Protocol (BGP) state change notifications.

- **bridge** --Sends SNMP STP Bridge MIB notifications.

- **bstun** --Sends Block Serial Tunneling (BSTUN) event notifications.

- **bulkstat** --Sends Data-Collection-MIB notifications.

- **c6kxbar** --Sends SNMP crossbar notifications.

- **callhome** --Sends Call Home MIB notifications.

- **calltracker** -- Sends Call Tracker call-start/call-end notifications.

- **casa** --Sends Cisco Appliances Services Architecture (CASA) event notifications.

- **ccme** --Sends SNMP Cisco netManager Event (CCME) traps.

- **cef** --Sends notifications related to Cisco Express Forwarding.

- **chassis** --Sends SNMP chassis notifications.

- **cnpd** --Sends Cisco Network-based Application Recognition (NBAR) Protocol Discovery (CNPD) traps.

- **config** --Sends configuration change notifications.

- **config-copy** --Sends SNMP config-copy notifications.

- **config-ctid** --Sends SNMP config-ctid notifications.

- **cpu** --Sends CPU-related notifications.

- **csg** --Sends SNMP Content Services Gateway (CSG) notifications.

- **deauthenticate** --Sends an SNMP 802.11 Deauthentication trap.

- **dhcp-snooping** --Sends DHCP snooping MIB notifications.

- **director** --Sends notifications related to DistributedDirector.

- **disassociate** --Sends an SNMP 802.11 Disassociation trap.

- **dlsw** --Sends data-link switching (DLSW) notifications.

- **dnis** --Sends SNMP Dialed Number Identification Service (DNIS) traps.

- **dot1x** --Sends 802.1X notifications.

- **dot11-mibs** --Sends dot11 traps.

- **dot11-qos** --Sends SNMP 802.11 QoS Change trap.

- **ds1** --Sends SNMP digital signaling 1 (DS1) notifications.

- **ds1-loopback** --Sends ds1-loopback traps.

- **dspu** --Sends downstream physical unit (DSPU) notifications.

- **eigrp** --Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.

- **energywise** --Sends SNMP energywise notifications.

- **entity** --Sends Entity MIB modification notifications.

- **entity-diag** --Sends SNMP entity diagnostic MIB notifications.

- **envmon** --Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.

- **errdisable** --Sends error disable notifications.

- **ethernet-cfm** --Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.

- **event-manager** --Sends SNMP Embedded Event Manager notifications.

- **firewall** --Sends SNMP Firewall traps.

- **flash** --Sends flash media insertion and removal notifications.

- **flexlinks** --Sends FLEX links notifications.

- **flowmon** --Sends flow monitoring notifications.

- **frame-relay** --Sends Frame Relay notifications.

- **fru-ctrl** --Sends entity field-replaceable unit (FRU) control notifications.

- **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications.

- **icsudsu** --Sends SNMP ICSUDSU traps.

- **iplocalpool** --Sends IP local pool notifications.

- **ipmobile** --Sends Mobile IP notifications.

- **ipmulticast** --Sends IP multicast notifications.

- **ipsec** --Sends IP Security (IPsec) notifications.

- **isakmp** --Sends SNMP ISAKMP notifications.

- **isdn** --Sends ISDN notifications.

- **l2tc** --Sends SNMP L2 tunnel configuration notifications.

- **l2tun-pseudowire-status** --Sends pseudowire state change notifications.

- **l2tun-session** --Sends Layer 2 tunneling session notifications.

- **license** --Sends licensing notifications as traps or informs.

- **llc2** --Sends Logical Link Control, type 2 (LLC2) notifications.

- **mac-notification** --Sends SNMP MAC notifications.

- **memory** --Sends memory pool and memory buffer pool notifications.

- **module** --Sends SNMP module notifications.

- **module-auto-shutdown** --Sends SNMP module autoshutdown MIB notifications.

- **mpls-fast-reroute** --Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.

- **mpls-ldp** --Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.

- **mpls-traffic-eng** --Sends MPLS traffic engineering notifications, indicating changes in the status of MPLS traffic engineering tunnels.

- **mpls-vpn** --Sends MPLS VPN notifications.

- **msdp** --Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.

- **mvpn** --Sends multicast VPN notifications.

- **nhrp** --Sends Next Hop Resolution Protocol (NHRP) notifications.

- **ospf** --Sends Open Shortest Path First (OSPF) sham-link notifications.

- **pim** --Sends Protocol Independent Multicast (PIM) notifications.

- **port-security** --Sends SNMP port-security notifications.

- **power-ethernet** --Sends SNMP power Ethernet notifications.

- **public storm-control** --Sends SNMP public storm-control notifications.

- **pw-vc** --Sends SNMP pseudowire virtual circuit (VC) notifications.

- **p2mp-traffic-eng**--Sends SNMP MPLS Point to Multi-Point MPLS-TE notifications.

- **repeater** --Sends standard repeater (hub) notifications.

- **resource-policy** --Sends CISCO-ERM-MIB notifications.

- **rf** --Sends SNMP RF MIB notifications.

- **rogue-ap** --Sends an SNMP 802.11 Rogue AP trap.

- **rsrb** --Sends remote source-route bridging (RSRB) notifications.

- **rsvp** --Sends Resource Reservation Protocol (RSVP) notifications.

- **rtr** --Sends Response Time Reporter (RTR) notifications.

- **sdlc** --Sends Synchronous Data Link Control (SDLC) notifications.

- **sdllc** --Sends SDLC Logical Link Control (SDLLC) notifications.

- **slb** --Sends SNMP server load balancer (SLB) notifications.

- **snmp** --Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC-2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet** --Sends SNMP SONET notifications.

- **srp** --Sends Spatial Reuse Protocol (SRP) notifications.

- **stpx** --Sends SNMP STPX MIB notifications.

- **srst** --Sends SNMP Survivable Remote Site Telephony (SRST) traps.

- **stun** --Sends serial tunnel (STUN) notifications.

- **switch-over** --Sends an SNMP 802.11 Standby Switchover trap.

- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.

- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.

- **tty** --Sends Cisco enterprise-specific notifications when a TCP connection closes.

- **udp-port** --Sends the notification host's UDP port number.

- **vlan-mac-limit** --Sends SNMP L2 control VLAN MAC limit notifications.

- **vlancreate** --Sends SNMP VLAN created notifications.

- **vlandelete** --Sends SNMP VLAN deleted notifications.

- **voice** --Sends SNMP voice traps.

- **vrrp** --Sends Virtual Router Redundancy Protocol (VRRP) notifications.

- **vsimaster** --Sends Virtual Switch Interface (VSI) notifications.

- **vswitch** --Sends SNMP virtual switch notifications.

- **vtp** --Sends SNMP VLAN Trunking Protocol (VTP) notifications.

- **wlan-wep** --Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.

- **x25** --Sends X.25 event notifications.

• **xgcp** --Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* argument used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the *notification-type* argument applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. The table below maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 1: snmp-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng [1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**
snmp-server host *host-address community-string* **udp-port** *port* **p2mp-traffic-eng**	**snmp-server enable traps mpls p2mp-traffic-eng** [**down**	**up**]

[1] See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 10.0.0.0 comaccess
Router(config)# access-list 10 deny any
```

Note   The "at" sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community @VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 10.0.0.0 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 10.0.0.0 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will 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. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

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

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.0.1.1 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.0.1.1 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 10.0.0.0 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 10.0.0.0 traps version 2c public nhrp
```

The following example shows how to enable all P2MP MPLS-TE SNMP traps, and send them to the notification receiver with the IP address 172.20.2.160 using the community string "comp2mppublic":

```
Router(config)# snmp-server enable traps mpls p2mp-traffic-eng
Router(config)# snmp-server host 172.20.2.160 comp2mppublic udp-port 162 p2mp-traffic-eng
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.

snmp-server inform

To specify inform request options, use the **snmp-server inform**command in global configuration mode. To return settings to their default values, use the **no** form of this command.

snmp-server inform [**pending** *pending*] [**retries** *retries*] [**timeout** *seconds*]
no snmp-server inform [**pending** *pending*] [**retries** *retries*] [**timeout** *seconds*]

Syntax Description

pending	(Optional) Specifies a maximum number of informs waiting for acknowledgment at any one time. When the maximum is reached, older pending informs are discarded.
pending	(Optional) Number of unacknowledged informs to hold. The range is from 1 to 4294967295. The default is 25.
retries	(Optional) Specifies a maximum number of times to resend an inform request.
retries	(Optional) Number of retries. The range is from 1 to 100. The default value is 3.
timeout	(Optional) Specifies a number of seconds to wait for an acknowledgment before resending.
seconds	(Optional) Time in seconds. The range is from 0 to 42949671. The default is 15.

Command Default

Inform requests are resent three times. Informs are resent after 30 seconds if no response is received. The maximum number of informs waiting for acknowledgment at any one time is 25.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples

The following example shows how to increase the pending queue size when several informs drop:

```
Router(config)# snmp-server inform pending 50
```

The following example shows how to increase the default timeout when you send informs over slow network links. Because informs will remain in the queue longer than other types of messages, you also may need to increase the pending queue size.

```
snmp-server inform timeout 60 pending 40
```

The following example shows how to decrease the default timeout when you send informs over very fast links:

```
Router(config)# snmp-server inform timeout 5
```

The following example shows how to increase the retry count when you send informs over unreliable links. Because informs will remain in the queue longer than other types of messages, you may need to increase the pending queue size.

```
Router(config)# snmp-server inform retries 10 pending 45
```

Related Commands	Command	Description
	snmp-server enable traps	Enables a router to send SNMP traps and informs.

snmp-server ip dscp

To set the IP Differentiated Services Code Point (DSCP) value for Simple Network Management Protocol (SNMP) traffic, use the **snmp-server ip dscp** command in global configuration mode. To disable the configured value, use the **no** form of this command.

snmp-server ip dscp *value*
no snmp-server ip dscp *value*

Syntax Description

value	The IP DSCP value to apply to SNMP traffic. Valid values for IP DSCP are 0 through 63. The default is 0.

Command Default   The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global config

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines   Use this command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

The following example shows how to set the IP DSCP value to 45:

```
Router(config)# snmp-server ip dscp 45
```

Related Commands

Command	Description
snmp-server ip precedence	Configures the IP Precedence value.

snmp-server ip precedence

snmp-server ip precedence *value*
no snmp-server ip precedence *value*

value	The IP Precedence value to apply to SNMP traffic. Valid values for IP Precedence are 0 through 7. The default is 0.

Syntax Description

Command Default

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global config.

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Examples

The following example shows how to set the IP Precedence value to 7:

```
Router(config)# snmp-server ip precedence
 7
```

Related Commands

Command	Description
snmp-server ip dscp	Configures the IP DSCP value.

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*
no snmp-server location

Syntax Description

text	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples

The following example shows how to set a system location string:

```
Router(config)# snmp-server location '{"city": "Raliegh", "zip": "00000", "site": "RTP",
"st": "NM", "bu": "TAC", "addr1": "123 TAC Rd"}'
```

Related Commands

Command	Description
show snmp location	Displays the SNMP system location string.
snmp-server contact	Sets the system contact (sysContact) string.

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager**command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager
no snmp-server manager

Syntax Description	This command has no arguments or keywords.
Command Default	Disabled
Command Modes	Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

Examples

The following example shows how to enable the SNMP manager process:

```
Router(config)# snmp-server manager
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.

Command	Description
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** command in global configuration mode. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*
no snmp-server manager session-timeout

Syntax Description

seconds	Number of seconds before an idle session is timed out. The default is 600.

Command Default

Idle sessions time out after 600 seconds (10 minutes).

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

However, sessions consume memory. A reasonable session timeout value should be large enough such that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

Examples

The following example shows how to set the session timeout to a larger value than the default:

```
Router(config)# snmp-server manager
Router(config)# snmp-server manager session-timeout 1000
```

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *byte-count*
no snmp-server packetsize

Syntax Description

| *byte-count* | Integer from 484 to 8192. The default is 1500. |

Command Default   Packet size is not configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples   The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
Router(config)# snmp-server packetsize 1024
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** command in global configuration mode.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. The default is 10.

Command Default

The queue length is set to 10.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines the length of the message queue for each trap host. When a trap message is successfully transmitted, Cisco IOS software will continue to empty the queue but never faster than at a rate of four trap messages per second.

During device bootup, some traps could be dropped because of trap queue overflow on the device. If you think that traps are being dropped, you can increase the size of the trap queue (for example, to 100) to determine if traps can then be sent during bootup.

Examples

The following example shows how to set the Simple Network Management Protocol (SNMP) notification queue to 50 events:

```
Router(config)# snmp-server queue-length 50
```

Related Commands

Command	Description
snmp-server packetsize	Establishes control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

snmp-server queue-limit

To establish the message queue size for various queues, use the **snmp-server queue-limit** command in global configuration mode. To disable the configured settings, use the **no** form of this command.

snmp-server queue-limit {**dispatcher** | **engine** | **notification-host**} *queue-length*
no snmp-server queue-limit {**dispatcher** | **engine** | **notification-host**}

Syntax Description		
dispatcher	Specifies the SNMP PDU dispatcher queue length.
engine	Specifies the SNMP engine queue length.
notification-host	Specifies the message queue length for each notification host.
queue-length	Length of the queue. The range for **dispatcher** and **engine** is 1 to 1000. The range for **notification-host** is 1 to 5000. The default *queue-length* value for notification-host is 10.

Command Default

By default, message queue size is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. The range of queue length for notification host was changed to 1 to 5000.

Usage Guidelines

Use the **snmp-server queue-limit** command to set the message queue size for different queues. Using this command you can resize the queue for dispatcher, engine, and host traps.

Examples

The following example shows how to set the message queue length of each notification host to 50:

```
Router(config)# snmp-server queue-limit notification-host 50
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

snmp-server source-interface {**traps** | **informs**} *interface*
no snmp-server source-interface {**traps** | **informs**} [*interface*]

Syntax Description		
traps	Specifies SNMP traps.
informs	Specifies SNMP informs.
interface	The interface type and the module and port number of the source interface.

Command Default No interface is designated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXB2	This command was introduced.
12.2(18)SXF6	The **informs** keyword was added. This command replaced the **snmp-server trap-source** command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command replaced the **snmp-server trap-source** command.

> **Note** The **snmp-server trap-source** command is available in other versions of Cisco IOS software for backward compatibility.

The source interface must have an IP address. Enter the *interface* argument in the following format: *interface-type module / port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples The following example shows how to specify that Gigabit Ethernet interface 5/2 is the source for all informs:

```
snmp-server source-interface informs gigabitethernet5/2
```

The following example shows how to specify that the Gigabit Ethernet interface 5/3 is the source for all traps:

```
snmp-server source-interface traps gigabitethernet5/3
```

The following example shows how to remove the source designation for all traps for a specific interface:

```
no snmp-server source-interface traps gigabitethernet5/3
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which a SNMP trap should originate.

snmp-server system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no**form of this command.

snmp-server system-shutdown
no snmp-server system-shutdown

Syntax Description   This command has no arguments or keywords.

Command Default   This command is not included in the configuration file.

Command Modes
Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples   The following example enables the SNMP message reload feature:

```
Router(config)# snmp-server system-shutdown
```

snmp-server tftp-server-list

Note This command was replaced with the **snmp-server file-transfer access-group**command in Cisco IOS Release 12.4(12). Use the **snmp-server file-transfer access-group** command in Cisco IOS Release 12.4(12) and in later releases.

To limit the TFTP servers used via Simple Network Management Protocol (SNMP) controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** command in global configuration mode. To disable this function, use the **no** form of this command.

snmp-server tftp-server-list {*acl-number*/*acl-name*}
no snmp-server tftp-server-list {*acl-number*/*acl-name*}

Syntax Description

| *acl-number* | Integer from 1 to 99 that specifies a standard access control list (standard ACL). |
| *acl-name* | String (not to exceed 64 characters) that specifies a standard ACL. |

Command Default Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.3(2)T	Support for standard named access lists was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples

The following example shows how to limit the TFTP servers that can be used for saving and loading configuration files via SNMP to the servers specified in the standard named access list lmnop:

Router(config)# **snmp-server tftp-server-list lmnop**

The following example shows how to limit the TFTP servers that can be used for copying configuration files via SNMP to the servers in access list 44:

```
Router(config)# snmp-server tftp-server-list 44
```

snmp-server trap authentication unknown-context

To enable the Simple Network Management Protocol (SNMP) authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context
no snmp-server trap authentication unknown-context

Syntax Description   This command has no arguments or keywords.

Command Default   No authFail traps are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.4(22)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(22)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples   The following example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap authentication vrf

To enable virtual private network (VPN) routing and forwarding (VRF) instance context authentication notifications, use the **snmp-server trap authentication vrf**command in global configuration mode. To suppress authentication notifications for Simple Network Management Protocol (SNMP) packets dropped due specifically to VRF context mismatches while keeping all other SNMP authentication notifications enabled, use the **no** form of this command.

snmp-server trap authentication vrf
no snmp-server trap authentication vrf

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF-specific authentication notifications are enabled when SNMP authentication notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp-server enable traps snmp authentication**command controls SNMP authentication traps and the **no** form of this command disables all SNMP authentication failure notifications. The **snmp-server trap authentication vrf** command provides more granular control of these notifications.

With context-based MIB access, SNMP requests on each VRF are tied to a specific context. This context is used for access control. If SNMP contexts are configured for VPNs, any SNMP request not matching the configured context will generate an SNMP authentication failure notification.The **no snmp-server trap authentication vrf** command allows you to suppress the authentication failure notifications that are specific to these VRF contexts, while keeping all other SNMP authentication failure notifications enabled.

The **no snmp-server trap authentication vrf** command has no effect if the **snmp-server enable traps snmp authentication**command has not been configured..

Examples

The following example shows how to enable a router to send SNMP authentication traps to host myhost.cisco.com using the community string public while disabling all VRF authentication traps:

```
Router(config)# snmp-server enable traps snmp authentication

Router(config)# no snmp-server trap authentication vrf
Router(config)# snmp-server host myhost.cisco.com public
```

	Command	Description
Related Commands	**snmp-server enable traps snmp**	Enables the sending of RFC 1157 SNMP notifications.
	snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps that are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF- compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server trap link ietf
no snmp-server trap link ietf

Syntax Description

ietf	Notifies the command parser to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (instead of the previous Cisco implementation).

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snmp-server trap link ietf** command is used to configure your router to use the RFC2233 IETF standards-based implementation of linkUp/linkDown traps. This command is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the default Cisco object definitions, linkUp/linkDown traps are not generated correctly for sub-interfaces. In the default implementation an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for sub-interfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for sub-interfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus,ifOperStatus, if Descr, ifType}. The *locIfReason* object will also be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured sub-interface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason* , so it will be omitted from the trap message.

Examples

The following example shows the enabling of the RFC 2233 linkUp/linkDown traps, starting in privileged EXEC mode:

```
Router#
configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
snmp-server trap link ietf

Router(config)#
end
Router#
 more system:running configuration
.
.
.
!
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

Related Commands	Command	Description
	debug snmp packets	Displays information about every SNMP packet sent or received by the router for the purposes of troubleshooting.

snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command in global configuration mode. To disable linkdown during a switch failover, use the **no** form of this command.

snmp-server trap link switchover
no snmp-server trap link switchover

Syntax Description   This command has no arguments or keywords.

Command Default   This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   By default, no link traps are generated during a switchover.

Examples   This example shows how to enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover:

```
snmp-server trap link switchover
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
no snmp-server trap link switchover
```

snmp-server trap retry

To define the number of times the Simple Network Management Protocol (SNMP) agent on a device tries to find a route before it sends traps, use the **snmp-server trap retry** command in global configuration mode.

snmp-server trap retry *number*

Syntax Description

number	Integer from 0 to 10 that sets the number of times the message will be retransmitted. The default is 3.

Command Default   Messages are not retransmitted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines   The SNMP agent looks for a configured route in the system before sending a trap out to a destination. If a route is not present, traps are queued in the trap queue and discarded when the queue becomes full. When the **snmp-server trap retry** command is configured, the route search retry number tells the agent how many times to look for the route before sending the trap out.

Configuring the **snmp-server trap retry** command also ensures that policy-based routing traps are sent and not discarded. Policy-based traps must be sent immediately and routes are not needed. The number of retries must be set to 0 so that policy-based traps are sent immediately.

Examples   The following example shows how to set the number of times a SNMP agent on a device tries to find a route to 10:

```
Router(config)# snmp-server trap retry 10
```

Related Commands

Command	Description
snmp-server trap timeout	Defines an interval of time between retransmissions of traps on a retransmission queue.

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

snmp-server trap timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced. This command replaces the **snmp-server trap-timeout** command in Cisco IOS Release 12.2SR only.

Usage Guidelines

Before a trap is sent, the SNMP agent looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Issue the **snmp-server trap timeout** command to configure the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between retransmissions of traps:

```
Router(config)# snmp-server trap timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap-source

Note Effective with Cisco IOS Release 12.2(18)SXB6, the **snmp-server trap-sourc**e command is replaced by the **snmp-server source-interface**command. See the **snmp-server source-interface**command for more information.

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in global configuration mode. To remove the source designation, use the **no** form of the command.

snmp-server trap-source *interface*
no snmp-server trap-source

Syntax Description

interface	Interface from which the SNMP trap originates. Includes the interface type and number in platform-specific syntax (for example, *typeslot* /*port*).

Command Default No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated in to Cisco IOS Release 12.2(33)SRA.
12.2(18)SXB6	This command was replaced by the **snmp-server source-interface**commandin Cisco IOS Release 12.2(18)SXB6.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines An SNMP trap or inform sent from a Cisco SNMP server has a notification address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples The following example shows how to set the IP address for Ethernet interface 0 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 0
```

The following example shows how to set the IP address for the Ethernet interface in slot 2, port 1 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 2/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of a SNMP notification operation.

snmp-server trap-timeout

> ✎
>
> **Note** This command is not supported in Cisco IOS Release 12.2SR. For Cisco IOS Release12.2SR, use the **snmp-server trap timeout** command.

To define an interval of time before resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode.

snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default   30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was replaced by the **snmp-server trap timeout** command in Cisco IOS Release 12.2SR.

Usage Guidelines   The **snmp-server trap-timeout** command remains in Cisco IOS software for compatibility but is written in the configuration as **snmp-server trap timeout**.

Before the Cisco IOS software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. The **snmp-server trap-timeout** command determines the number of seconds between retransmission attempts.

Examples   The following example shows how to set an interval of 20 seconds between resending trap messages on the retransmission queue:

```
Router(config)# snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server user

To configure a new user for 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 this command.

snmp-server **user** *username* *groupname* [**remote** *host* [**udp-port** *port*] [**vrf** *vrfname*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** | **sha-2** { **256** | **384** | **512** } } *authpassword*] } [**access** [**ipv6** *nacl*] [**privacy** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privacypassword*] { *aclnumber aclname* }]

no **snmp-server** **user** *username* *groupname* [**remote** *host* [**udp-port** *port*] [**vrf** *vrfname*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** | **sha-2** { **256** | **384** | **512** } } *authpassword*] } [**access** [**ipv6** *nacl*] [**privacy** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privacypassword*] { *aclnumber aclname* }]

Syntax Description		
	username	Name of the user on the host that connects to the agent.
	groupname	Name of the group to which the user belongs.
	remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
	host	(Optional) Name or IP address of the remote SNMP host.
	udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
	port	(Optional) Integer value that identifies the UDP port. The default is 162.
	vrf	(Optional) Specifies an instance of a routing table.
	vrfname	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
	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** keyword or **auth** keyword or both.
	encrypted	(Optional) Specifies whether the password appears in encrypted format.
	auth	(Optional) Specifies which authentication level should be used.
	md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
	sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
	sha-2	(Optional) Specifies the HMAC-SHA-2 authentication level.

256	(Optional) Specifies the use of SHA-256 (a part of the SHA-2 family). The resulting message digest is truncated to 192 bits.
384	(Optional) Specifies the use of SHA-384 (a part of the SHA-2 family). The resulting message digest is truncated to 256 bits.
512	(Optional) Specifies the use of SHA-512 (a part of the SHA-2 family). The resulting message digest is truncated to 384 bits.
authpassword	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
privacy	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption. **Note** The SHA-2 authentication level only supports AES (128, 192, and 256) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privacypassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
aclnumber	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
aclname	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default See the table in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.3(2)T	Support for named standard access lists was added.
	12.0(27)S	The **ipv6** keyword and *nacl*argument were added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
	12.3(14)T	The **ipv6** keyword and *nacl*argument were integrated into Cisco IOS Release 12.3(14)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the USM for SNMP version 3 for SNMP message level security.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
	Cisco IOS XE Release 17.10.1a	The **sha-2** keyword was introduced to provide support for SHA-2 as an additional authentication protocol to create an SNMPv3 user and associate a security level to each user.

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 **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privacypassword* and *authpassword*arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers. The recommended maximum length is 64 characters.

The table below describes the default user characteristics for encryption, passwords, and access lists.

Table 2: snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are message digest algorithm 5 (MD5)digests and not text passwords.
Passwords	Assumed to be text strings.

Characteristic	Default
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

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.

Note Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. The recommended maximum length of a password is 64 characters. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

From Cisco IOS XE Release 17.10.1a, the SHA-2 algorithm is implemented as an additional authentication protocol to create an SNMPv3 user and associate a security level to each user, extending the authentication level from the existing MD5 and SHA protocols.

This feature provides HMAC-SHA-2 authentication protocols for USM using a Hashed Message Authentication Code (HMAC) based on the SHA-2 family of hash functions. The resulting message digest (output of HMAC) is truncated as follows:

- 192 bits (24 octets) for SHA-256 protocol.

- 256 bits (32 octets) for SHA-384 protocol.

- 384 bits (48 octets) for SHA-512 protocol.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Device(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

```
Device(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

Device(config)# **snmp-server user abcd public v3 auth md5 cisco123**

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the show snmp user command.

✎

Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

Device(config)# **snmp-server user abcd public v3 encrypted auth md5**
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF

In the following example, the user abcd is removed from the SNMP server group named public:

Device(config)# **no snmp-server user abcd public v2c**

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with secure3des as the password.

Device(config)# **snmp-server user abcd public priv v2c 3des secure3des**

The following example shows how to create the user abcd for the SNMP server group public with a plain-text password pass1234 using SHA-2 512 authentication protocol. The 128-bit AES algorithm is used for privacy encryption with priv1234 as the password.

Device(config)# **snmp-server user abcd public v3 auth sha-2 512 pass1234 priv aes 128 priv1234**

The following example shows how to create the user abcd for the SNMP server group public with an encrypted password pass1234 using SHA-2 512 authentication protocol. The 128-bit AES algorithm is used for privacy encryption with priv1234 as the password.

Device(config)# **snmp-server user abcd public v3 encrypted auth sha-2 512 pass1234 priv aes**
 128 priv1234

Related Commands	**Command**	**Description**
	show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
	show snmp user	Displays information on each SNMP username in the group username table.
	snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the device.

snmp-server usm cisco

To enable Cisco-specific error messages for Simple Network Management Protocol Version 3 (SNMPv3), which is a User-based Security Model (USM), use the **snmp-server usm cisco** command in global configuration mode. To disable the Cisco-specific error messages for SNMPv3 USM, use the **no** form of this command.

snmp-server usm cisco
no snmp-server usm cisco

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco-specific error messages for SNMPv3 USM are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The RFC 3414-compliant error messages are descriptive and can lead to misuse of information by malicious users. Use the **snmp-server usm cisco** command to enable Cisco-specific messages that help to hide the exact error condition. Enabling Cisco-specific messages for SNMPv3 is a deviation from RFC 3414.

Examples

The following example shows how to enable the Cisco-specific error messages for SNMPv3 USM:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server usm cisco
Router(config)# exit
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no**form of this command.

snmp-server view *view-name* *oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.
excluded	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be explicitly excluded from the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to exclude USM, VACM, and Community MIBs from any parent OIDs in a configured view by default.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted,*which indicates that the

user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

✎

Note   Beginning in Release 12.0(26)S and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

The first **snmp-server** command that you enter enables SNMP on your routing device.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

In the following example, the USM, VACM, and Community MIBs are explicitly included in the view "test" with all other MIBs under the root parent "internet":

```
! -- include all MIBs under the parent tree "internet"
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP protocol.

snmp trap if-monitor

To enable if-monitor traps for a particular interface, use the **snmp trap if-monitor**command in interface configuration mode. To disable traps on an interface, use the **no** form of this command.

snmp trap if-monitor
no snmp trap if-monitor

Syntax Description	This command has no arguments or keywords.
Command Default	Traps are not generated.
Command Modes	Interface configuration (config-if)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Traps are sent for the interface only if they have been enabled globally by issuing the **snmp-server enable traps if-monitor** command and then explicitly on that interface by issuing the **snmp trap if-monitor**command.

Examples

The following example shows how to enable if-monitor traps on a specific interface:

```
Router(config)# snmp-server enable traps if-monitor
Router(config)# interface ethernet 1/1
Router(config-if)# snmp trap if-monitor
```

Related Commands

Command	Description
snmp-server enable traps if-monitor	Globally enables if-monitor traps.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]
no snmp trap link-status [**permit duplicates**]

Syntax Description

| **permit duplicates** | (Optional) Permits duplicate SNMP linkup and linkdown traps. |

Command Default SNMP link traps are generated when an interface goes up or down.

Command Modes

Interface configuration (config-if)
Service instance configuration (config-if-srv)

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	This command was modified. The **permit duplicates** keyword pair was added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode.
12.2(33)SRE6	This command was modified. This command must be enabled on each subinterface from this release onwards.
15.1(3)S3	This command was integrated into Cisco IOS Release 15.1(3)S3.

Usage Guidelines By default, SNMP link traps are sent when an interface goes up or down. For interfaces such as ISDN interfaces, expected to go up and down during normal usage, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode, SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

The **snmp trap link-status** command must be used in conjunction with the **snmp-server enable traps atm subif** command in order to enable SNMP trap notifications on ATM subinterfaces. The **snmp-server enable traps atm subif** command must be configured in global configuration mode, and then the **snmp trap link-status** command must be configured on each ATM subinterface for which you want to enable SNMP trap notifications.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the device no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the device displays a configuration error message such as the following:

```
Device(config)# interface virtual-template 1
Device(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the device reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI interface 0:

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Device(config)# interface ethernet 0/1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
Device(config-if-srv)# end
```

Related Commands

Command	Description
snmp-server enable traps atm subif	Enables the sending of ATM subinterface SNMP notifications.
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.