



SNMP Commands

This chapter describes commands used to configure Simple Network Management Protocol (SNMP) on your routers for the purposes of network monitoring and management.

For SNMP configuration tasks and examples, refer to the “Configuring SNMP Support” chapter in the Release 12.1 *Cisco IOS Configuration Fundamentals Configuration Guide*.

no snmp-server

To disable Simple Network Management Protocol agent operation, use the **no snmp-server** command.

no snmp-server

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command disables all running versions of SNMP (SNMPv1, SNMPv2C, SNMPv3) on the device.

Examples The following example disables the current running version of SNMP:

```
no snmp-server
```

show snmp

To check the status of SNMP communications, use the **show snmp** EXEC command.

show snmp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	The command was introduced.

Usage Guidelines This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Examples

The following is sample output from the **show snmp** command:

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
  0 Bad SNMP version errors
  4 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  24 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  28 Get-next PDUs
  0 Set-request PDUs
78 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  24 Response PDUs
  13 Trap PDUs

SNMP logging: enabled
  Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
  4 Get-request PDUs
  4 Get-next PDUs
  6 Get-bulk PDUs
  4 Set-request PDUs
  23 Inform-request PDUs
  30 Timeouts
  0 Drops
SNMP Manager-role input packets
  0 Inform response PDUs
  2 Trap PDUs
  7 Response PDUs
  1 Responses with errors

SNMP informs: enabled
  Informs in flight 0/25 (current/max)
  Logging to 171.69.217.141.162
    4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
  Logging to 171.69.58.33.162
    0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Table 39 describes the fields shown in the display.

Table 39 *show snmp* Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.

Table 39 *show snmp Field Descriptions (continued)*

Field	Description
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets which were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified an MIB object which does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for an MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the snmp-server queue-length command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.

Table 39 *show snmp Field Descriptions (continued)*

Field	Description
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

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 chassis-id	Provides a message line identifying the SNMP server serial number.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a non-active session is destroyed.
snmp-server queue-length	Establishes the message queue length for each trap host.

show snmp engineID

To display the identification of the local Simple Network Management Protocol engine and all remote engines that have been configured on the router, use the **show snmp engineID EXEC** command.

show snmp engineID

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines An SNMP engine is a copy of SNMP that can reside on a local or remote device.

Examples The following example specifies 0000000902000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 171.69.37.61 as the IP address of the remote engine, or copy of SNMP, and 162 as the port from which the remote device is connected to the local device:

```
router# show snmp engineID

Local SNMP engineID: 0000000902000000C025808
Remote Engine IDIP-addrPort
123456789ABCDEF000000000171.69.37.61162
```

Table 1 describes the fields shown in the example.

Table 40 show snmp engineID Field Descriptions

Field	Definition
Local SNMP engine ID	A string that identifies the copy of SNMP on the local device.
Remote Engine ID	A string that identifies the copy of SNMP on the remote device.
IP-addr	The IP address of the remote device.
Port	The port number on the local device to which the remote device is connected.

Related Commands	Command	Description
	snmp-server engineID	Configures a name for either the local or remote SNMP engine on the router.

show snmp group

To display the names of groups on the router and the security model, the status of the different views, and the storage type of each group, use the **show snmp group** EXEC command.

show snmp group

Syntax Description This command has no keywords or arguments.

Command Modes EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Examples The following example specifies the group name as `public`, the security model as `v1`, the read view name as `v1default`, the notify view name as `*tv.FFFFFFFF`, and the storage type as `volatile`:

```
router# show snmp group

groupname: publicsecurity model:v1
readview:v1default
writeview: no writeview specified
notifyview: *tv.FFFFFFFF
storage-type: volatile
```

Table 41 describes the fields shown in the example.

Table 41 *show snmp group* Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users who have a common access policy.
security model	The security model used by the group, either v1, v2c, or v3.
readview	A string identifying the read view of the group.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands	Command	Description
	snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.

show snmp pending

To display the current set of pending Simple Network Management Protocol requests, use the **show snmp pending EXEC** command.

show snmp pending

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	The command was introduced.

Usage Guidelines After the SNMP manager sends a request, the request is “pending” until the manager receives a response or the request timeout expires.

Examples The following is sample output from the **show snmp pending** command:

```
Router# show snmp pending
```

```
req id: 47, dest: 171.69.58.33.161, V2C community: public, Expires in 5 secs
req id: 49, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 51, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 53, dest: 171.69.58.33.161, V2C community: public, Expires in 8 secs
```

Table 42 describes the fields shown in the display.

Table 42 *show snmp pending Field Descriptions*

Field	Description
req id	ID number of the pending request.
dest	IP address of the intended receiver of the request.
V2C Community	SNMP version 2C community string sent with the request.
Expires in	Remaining time before request timeout expires.

Related Commands	Command	Description
	show snmp	Checks the status of SNMP communications.
	show snmp sessions	Displays the current SNMP sessions.
	snmp-server manager	Starts the SNMP manager process.
	snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp sessions

To display the current SNMP sessions, use the **show snmp sessions** EXEC command.

show snmp sessions [brief]

Syntax Description	brief (Optional) Displays a list of sessions only. Does not display session statistics.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.3 T	This command was introduced.

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 corresponding session will be deleted.
-------------------------	---

Examples The following is sample output from the **show snmp sessions** command:

```
Router# show snmp sessions

Destination: 171.69.58.33.162, V2C community: public
Round-trip-times: 0/0/0 (min/max/last)
packets output
  0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
  0 Timeouts, 0 Drops
packets input
  0 Traps, 0 Informs, 0 Responses (0 errors)
Destination: 171.69.217.141.162, V2C community: public, Expires in 575 secs
Round-trip-times: 1/1/1 (min/max/last)
packets output
  0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
  0 Timeouts, 0 Drops
packets input
  0 Traps, 0 Informs, 4 Responses (0 errors)
```

The following is sample output from the **show snmp sessions brief** command:

```
Router# show snmp sessions brief

Destination: 171.69.58.33.161, V2C community: public, Expires in 55 secs
```

Table 43 describes the fields shown in these displays.

Table 43 *show snmp sessions Field Descriptions*

Field	Description
Destination	IP address of the remote agent.
V2C community	SNMP version 2C community string used to communicate with the remote agent.
Expires in	Remaining time before the session timeout expires.
Round-trip-times	Minimum, maximum, and the last round-trip time to the agent.
packets output	Packets sent by the router.
Gets	Number of get requests sent.
GetNexts	Number of get-next requests sent.
GetBulks	Number of get-bulk requests sent.
Sets	Number of set requests sent.
Informs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of packets that could not be sent.
packets input	Packets received by the router.
Traps	Number of traps received.
Informs	Number of inform responses received.
Responses	Number of request responses received.
errors	Number of responses that contained an SNMP error code.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

show snmp user

To display information on each Simple Network Management Protocol username in the group username table, use the **show snmp user** EXEC command.

show snmp user

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines An SNMP user is a remote user for which an SNMP management operation is performed. For example, inform operations can be sent to a user on a remote SNMP engine. The user is designated using the **snmp-server user** command.

Examples The following example specifies the username as `authuser`, the engine ID string as `00000009020000000C025808`, and the storage-type as `nonvolatile`:

```
router# show snmp user
```

```
User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile
```

Table 44 describes fields shown in the example.

Table 44 *show snmp user Field Descriptions*

Field	Definition
User name	A string identifying the name of the SNMP user.
Engine ID	A string identifying the name of the copy of SNMP on the device.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands	Command	Description
	snmp-server user	Configures a new user to an SNMP group.

snmp-server access-policy

This command is no longer valid. The functionality provided by this command has been removed from the Cisco IOS software.

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol server serial number, use the **snmp-server chassis-id** global configuration command. Use the **no** form of this command to restore the default value, if any.

snmp-server chassis-id *text*

no snmp-server chassis-id

Syntax Description

<i>text</i>	Message you want to enter to identify the chassis serial number.
-------------	--

Defaults

On hardware platforms where the serial number can be machine read, the default is the serial number. For example, a Cisco 7000 has a default chassis-id value of its serial number.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco MIB provides a chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, chassis type, chassis hardware version, chassis ID string, software version of ROM monitor, software version of system image in ROM, bytes of processor RAM installed, bytes of NVRAM installed, bytes of NVRAM in use, current configuration register setting, and the value of the configuration register at the next reload. The following installed card information is provided: type of card, serial number, hardware version, software version, and chassis slot number.

The chassis ID message can be seen with the **show snmp** command.

Examples

In the following example, the chassis serial number specified is 1234456:

```
snmp-server chassis-id 1234456
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol protocol, use the **snmp-server community** global configuration command. The **no** form of this command removes the specified community string.

```
snmp-server community string [view view-name] [ro | rw] [number]
```

```
no snmp-server community string
```

Syntax Description

<i>string</i>	Community string that acts like a password and permits access to the SNMP protocol.
view <i>view-name</i>	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
<i>number</i>	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

Defaults

By default, an SNMP community string permits read-only access to all objects.



Note

If the **snmp-server community** command is not used during the SNMP configuration session, it will automatically be added to the configuration after the **snmp host** command is used. In this case, the default password (*string*) for the **snmp-server community** will be taken from the **snmp host** command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3). The first **snmp-server** command that you enter enables all versions of SNMP.

Examples

The following example assigns the string comaccess to SNMP allowing read-only access and specifies that IP access list 4 can use the community string:

```
snmp-server community comaccess ro 4
```

The following example assigns the string mgr to SNMP allowing read-write access to the objects in the restricted view:

```
snmp-server community mgr view restricted rw
```

The following example removes the community comaccess:

```
no snmp-server community comaccess
```

The following example disables all versions of SNMP:

```
no snmp-server
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
snmp-server view	Creates or updates a view entry.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** global configuration command. Use the **no** form to remove the system contact information.

snmp-server contact *text*

no snmp-server contact

Syntax Description	<i>text</i>	String that describes the system contact information.				
Defaults	No system contact string is set.					
Command Modes	Global configuration					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.	
Release	Modification					
10.0	This command was introduced.					
Examples	<p>The following is an example of a system contact string:</p> <pre>snmp-server contact Dial System Operator at beeper # 27345</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>snmp-server location</td> <td>Sets the system location string.</td> </tr> </tbody> </table>	Command	Description	snmp-server location	Sets the system location string.	
Command	Description					
snmp-server location	Sets the system location string.					

snmp-server context

This command is no longer valid. The functionality provided by this command has been removed from the Cisco IOS software.

snmp-server enable informs

This command has no functionality. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** *[notification-type]* command combined with the **snmp-server host** *host-addr* **informs** command.

snmp-server enable traps

To enable the router to send Simple Network Management Protocol traps or informs (SNMP notifications), use the **snmp-server enable traps** global configuration command. Use the **no** form of this command to disable SNMP notifications.

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

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

Syntax Description

<i>notification-type</i>	<p>(Optional) Type of notification to enable. If no type is specified, all notifications available on your device are sent. The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • atm pvc—Enables ATM permanent virtual circuit (PVC) notifications. When the atm pvc keywords are used, you can specify additional <i>notification-option</i> values (see below). The ATM PVC failure notification is defined as "enterprise 1.3.6.1.4.1.9.10.29.2.1; 1 atmIntfPvcFailuresTrap" in the CISCO-IETF-ATM2-PVCTRAP-MIB. ATM PVC failure notifications are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the interval keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the fail-interval has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN. No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router. • bgp—Enables Border Gateway Protocol (BGP) state change notifications. • config—Enables configuration notifications. • entity—Enables Entity MIB modification notifications. • envmon—Enables Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the envmon keyword is used, you can specify a <i>notification-option</i> value. • frame-relay—Enables Frame Relay notifications. • hsrp—Enables Hot Standby Routing Protocol (HSRP) notifications. • isdn—Enables Integrated Services Digital Network (ISDN) notifications. When the isdn keyword is used, you can specify a <i>notification-option</i> value. • repeater—Enables Ethernet hub repeater notifications. When the repeater keyword is selected, you can specify a <i>notification-option</i> value. • rsvp—Enables Resource Reservation Protocol (RSVP) notifications. • rtr—Enables Service Assurance Agent / Response Time Reporter (RTR) notifications.
--------------------------	--

<i>notification-type</i>	<ul style="list-style-type: none"> • snmp [authentication]—Enables RFC 1157 SNMP notifications. Note that use of the authentication keyword produces the same effect as not using the authentication keyword. Both the snmp-server enable traps snmp and snmp-server enable traps snmp authentication forms of this command will globally enable (or, if using the no form, disable) the following SNMP traps: <ul style="list-style-type: none"> – authentication Failure – linkUp – linkDown – coldstart <p>(This behavior is corrected in Cisco IOS Release 12.1(3)T and 12.0(20)S.)</p> • syslog—Enables error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
<i>notification-option</i>	<p>(Optional)</p> <ul style="list-style-type: none"> • atm pvc [interval seconds] [fail-interval seconds] <ul style="list-style-type: none"> — The optional interval seconds keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30. —The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0. • envmon [voltage shutdown supply fan temperature] <ul style="list-style-type: none"> —When the envmon keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: voltage, shutdown, supply, fan, and temperature. • isdn [call-information isdn u-interface] <ul style="list-style-type: none"> —When the isdn keyword is used, you can specify the call-information keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the isdnu-interface keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem. • repeater [health reset] <ul style="list-style-type: none"> —When the repeater keyword is used, you can specify the repeater option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords: <ul style="list-style-type: none"> – health—Enables IETF Repeater Hub MIB (RFC 1516) health notification. – reset—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command.

If you enter this command with no *notification-type* keywords, the default is to enable all notification types controlled by this command (EXCEPTION: ATM PVC notifications are not enabled unless the **atm pvc** keywords are used.)

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	The snmp-server enable traps snmp authentication form of this command was introduced to replace the snmp-server trap-authentication command.
12.0(1)T	The snmp-server enable traps atm pvc interval seconds fail-interval seconds form of this command was introduced.
12.0(2)T	The rsvp keyword was added.
12.0(3)T	The hsrp keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host [traps | informs]** command.

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

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

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

The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these cannot be controlled using the **snmp-server enable** command.

Examples

The following example enables the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

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

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
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 the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

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

The following example enables the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

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

The following example sends HSRP MIB traps to the host myhost.cisco.com using the community string public.

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.

snmp-server engineID

To configure a name for either the local or remote Simple Network Management Protocol engine on the router, use the **snmp-server engineID** global configuration command. To remove the configured engine ID, use the **no** form of this command .

```
snmp-server engineID [local engineid-string] | [remote ip-address udp-port port
engineid-string]
```

```
no snmp-server engineID
```

Syntax Description		
local	(Optional)	Specifies the local copy of SNMP on the router.
<i>engineid-string</i>	(Optional)	The name of a copy of SNMP.
remote	(Optional)	Specifies the remote copy of SNMP on the router.
<i>ip-address</i>	(Optional)	The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional)	Specifies a UDP port of the host to use.
<i>port</i>	(Optional)	The socket number on the remote device that contains the remote copy of SNMP. The default is 161.

Defaults 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 EXEC** command.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines Note that you need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the Engine ID up until the point where only zeros remain in the value. To configure an engine ID of 1234000000000000000000, you can specify the value 1234, for example, **snmp-server engineID** local 1234.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or 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 engineID changes, the security digests of SNMPv3 users will be 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. Please refer to the examples in the Configuring Informs section in the **snmp-server host** command reference page.

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 group

To configure a new Simple Network Management Protocol group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** global configuration command. To remove a specified SNMP group, use the **no** form of this command.

```
snmp-server group [groupname {v1 | v2c | v3 {auth | noauth | priv}}] [read readview] [write
writeview] [notify notifyview] [access access-list]
```

```
no snmp-server group
```

Syntax Description		
	<i>groupname</i>	(Optional) The name of the group.
	v1	(Optional) The least secure of the possible security models.
	v2c	(Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
	v3	(Optional) The most secure of the possible security models.
	auth	(Optional) Specifies authentication of a packet without encrypting it.
	noauth	(Optional) Specifies no authentication of a packet.
	priv	(Optional) Specifies authentication of a packet with encryption.
	read	(Optional) The option that allows you to specify a read view.
	<i>readview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent.
	write	(Optional) The option that allows you to specify a write view.
	<i>writeview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
	notify	(Optional) The option that allows you to specify a notify view
	<i>notifyview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
	access	(Optional) The option that enables you to specify an access list.
	<i>access-list</i>	(Optional) A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 45 describes default values for the different views.

Table 45 *snmp server group Default Descriptions*

Default	Definition
<i>readview</i>	Assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless the user uses the read option to override this state.

Table 45 *snmp server group Default Descriptions (continued)*

Default	Definition
<i>writeview</i>	Nothing is defined for the write view (that is, the null OID). You must configure write access.
<i>notifyview</i>	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated will be sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Command Modes Global configuration

Release	Modification
11.(3)T	This command was introduced.

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.

Configuring Notify Views

Do not specify a notify view when configuring an SNMP group 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.

The *notifyview* 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.

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

Step	Command	Purpose
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.

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 eight characters for security. 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.

The following example shows how to enter a plain-text password for the string arizona2 for user John in group Johngroup, type the following command line:

```
snmp-server user John Johngroup v3 auth md5 arizona2.
```

When you enter a **show running-config** command, you will not see a line for this user. To see if this user has been added to the configuration, type 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 hex values. Also, the digest should be exactly 16 octets long.

The following example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
snmp-server user John Johngroup v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

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-server host

To specify the recipient of an Simple Network Management Protocol notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

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

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

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

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

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.



Note

If the *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** will be the same as specified in the **snmp-server host** command. This is the default behavior for IOS 12.0(3) and later.

Command Modes Global configuration

Command History

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

Usage Guidelines

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 PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

```
snmp-server enable traps
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.

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

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

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

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

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

snmp-server informs

To specify inform request options, use the **snmp-server informs** global configuration command. The **no** form of this command returns the settings to the defaults.

snmp-server informs [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]

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

Syntax Description	
retries <i>retries</i>	(Optional) Maximum number of times to resend an inform request. The default is 3.
timeout <i>second</i>	(Optional) Number of seconds to wait for an acknowledgment before resending. The default is 30 seconds.
pending <i>pending</i>	(Optional) Maximum number of informs waiting for acknowledgments at any one time. When the maximum is reached, older pending informs are discarded. The default is 25.

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

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Examples The following example increases the pending queue size if you are seeing a large number of inform drops:

```
snmp-server informs pending 50
```

The following example increases the default timeout if you are sending informs over slow network links. Because informs will be sitting in the queue for a longer period of time, you may also need to increase the pending queue size.

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

The following example decreases the default timeout if you are sending informs over very fast links:

```
snmp-server informs timeout 5
```

The following example increases the retry count if you are sending informs over unreliable links. Because informs will be sitting in the queue for a longer period of time, you may need to increase the pending queue size.

```
snmp-server informs retries 10 pending 45
```

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

snmp-server location

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

snmp-server location *text*

no snmp-server location

Syntax Description	<i>text</i>	String that describes the system location information.
--------------------	-------------	--

Defaults	No system location string is set.
----------	-----------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Examples	The following example illustrates a system location string: <code>snmp-server location Building 3/Room 214</code>
----------	--

Related Commands	Command	Description
	snmp-server contact	Sets the system contact (sysContact) string.

snmp-server manager

To start the Simple Network Management Protocol manager process, use the **snmp-server manager** global configuration command. The **no** form of this command stops the SNMP manager process.

snmp-server manager

no snmp-server manager

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

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 enables the SNMP manager process:

```
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.
	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** global configuration command. The **no** form of this command returns the value to its default.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description	<i>seconds</i>	Number of seconds before an idle session is timed out. The default is 600 seconds.
---------------------------	----------------	--

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

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines	<p>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.</p> <p>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.</p> <p>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.</p>
-------------------------	---

Examples	The following example sets the session timeout to a larger value than the default:
-----------------	--

```
snmp-server manager
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 packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** global configuration command. Use the **no** form of this command to restore the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Syntax Description	<i>byte-count</i>	Integer byte count from 484 to 8192. The default is 1500 bytes.
---------------------------	-------------------	---

Defaults	1500 bytes
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

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

```
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** global configuration command.

snmp-server queue-length *length*

Syntax Description	<i>length</i>	Integer that specifies the number of trap events that can be held before the queue must be emptied.
---------------------------	---------------	---

Defaults	10 events
-----------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

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

Examples	The following example establishes a message queue that traps four events before it must be emptied: <pre>snmp-server queue-length 4</pre>
-----------------	--

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 system-shutdown

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

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description This command has no arguments or keywords.

Defaults This command is not included in the configuration file.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example enables the SNMP message reload feature:

```
snmp-server system-shutdown
```

snmp-server tftp-server-list

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

snmp-server tftp-server-list *number*

no snmp-server tftp-server-list

Syntax Description	<i>number</i>	Standard IP access list number from 1 to 99.			
Defaults	Disabled				
Command Modes	Global configuration				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>10.2</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	10.2	This command was introduced.
Release	Modification				
10.2	This command was introduced.				
Examples	The following example limits the TFTP servers that can be used for configuration file copies via SNMP to the servers in access list 44: <pre>snmp-server tftp-server-list 44</pre>				

snmp-server trap-authentication

The **snmp-server enable traps snmp authentication** command replaces this command. See the **snmp-server host** command in this chapter for more information.

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) that an Simple Network Management Protocol trap should originate from, use the **snmp-server trap-source** global configuration command. Use the **no** form of the command to remove the source designation.

snmp-server trap-source *interface*

no snmp-server trap-source

Syntax Description	<i>interface</i>	Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax.
---------------------------	------------------	---

Defaults	No interface is specified.
-----------------	----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	When an SNMP trap is sent from a Cisco SNMP server, it has a trap address of whatever interface it happened to go out of at that time. Use this command if you want to use the trap address to trace particular needs.
-------------------------	--

Examples	The following example specifies that the IP address for interface Ethernet 0 is the source for all traps:
	<pre>snmp-server trap-source ethernet 0</pre>

The following example specifies that the IP address for interface Ethernet 2/1 on a Cisco 7000 is the source for all traps:

```
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 an SNMP notification operation.

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** global configuration command.

snmp-server trap-timeout *seconds*

Syntax Description	<i>seconds</i>	Integer that sets the interval, in seconds, for resending the messages.
---------------------------	----------------	---

Defaults	30 seconds
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	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 server trap-timeout command determines the number of seconds between retransmission attempts.
-------------------------	--

Examples	The following example sets an interval of 20 seconds to try resending trap messages on the retransmission queue:
-----------------	--

```
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 to an Simple Network Management Protocol group, use the **snmp-server user** global configuration command. To remove a user from an SNMP group, use the **no** form of the command.

```
snmp-server user username [groupname remote ip-address [udp-port port] {v1 / v2c / v3}
[encrypted] [auth {md5 / sha} auth-password [priv des56 priv password]] [access access-list]
```

```
no snmp-server user
```

Syntax Description

<i>username</i>	The name of the user on the host that connects to the agent.
<i>groupname</i>	(Optional) The name of the group to which the user is associated.
remote	(Optional) Specifies the remote copy of SNMP on the router.
<i>ip-address</i>	(Optional) The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
<i>port</i>	(Optional) A UDP port number that the host uses. The default is 162.
v1	(Optional) The least secure of the possible security models.
v2c	(Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	(Optional) The most secure of the possible security models.
<i>encrypted</i>	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Initiates an authentication level setting session.
md5	(Optional) The HMAC-MD5-96 authentication level.
sha	(Optional) The HMAC-SHA-96 authentication level.
<i>auth-password</i>	(Optional) A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) The option that initiates a privacy authentication level setting session.
<i>des56</i>	(Optional) The CBC-DES privacy authentication algorithm.
<i>priv password</i>	(Optional) A string (not to exceed 64 characters) that enables the host to encrypt the contents of the message it sends to the agent.
<i>access</i>	(Optional) The option that enables you to specify an access list.
<i>access-list</i>	(Optional) A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 46 describes default values for the **encrypted** option, passwords and access lists.

Table 46 *snmp-server user Default Descriptions*

Default	Description
encrypted	Not present by default. It is used to specify that the auth and priv passwords are MD5 digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the remote option.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

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

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

Related Commands

Command	Description
show snmp user	Displays information on each SNMP username in the group username table.

snmp-server view

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified Simple Network Management Protocol 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		
<i>view-name</i>		Label for the view record that you are updating or creating. The name is used to reference the record.
<i>oid-tree</i>		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 <i>1.3.6.2.4</i> , or a word, such as <i>system</i> . Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example <i>1.3.*.4</i> .
included excluded		Type of view. You must specify either included or excluded .

Defaults No view entry exists.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Other SNMP commands require a view as an argument. You use this command to create a view to be used as arguments for other commands that create records including a view.

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.

The first **snmp-server** command that you enter enables both versions of SNMP.

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 phred system included
snmp-server view phred 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
```

Related Commands

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

snmp trap link-status

To enable Simple Network Management Protocol link trap generation, use the **snmp trap link-status** interface configuration command. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description This command has no arguments or keywords.

Defaults SNMP link traps are sent when an interface goes up or down.

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

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

Examples The following example disables the sending of SNMP link traps related to the ISDN BRI 0 interface:

```
interface bri 0
no snmp trap link-status
```

