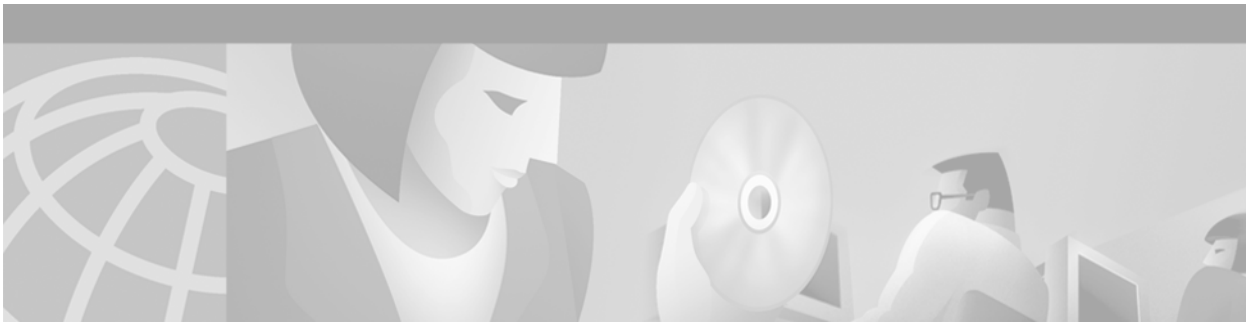

SNMP Commands

This chapter describes Cisco IOS Release 12.2 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 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** global configuration command.

no snmp-server

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example disables the current running version of SNMP:

```
Router(config)# no snmp-server
```

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged EXEC mode.

show management event

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The Event MIB allows you to configure your own traps, informs, or set operations through the use of an external network management application. The **show management event** command is used to display the values for the Events configured on your system. There are no Cisco IOS CLI commands for configuring Event MIB values. For information on Event MIB functionality, see RFC 2981, available at http://www.ietf.org.

Examples

The following example shows sample output of the **show management event** command:

```
Router# show management event

Mgmt Triggers:
 (1): Owner: aseem
   (1): 01, Comment: TestEvent, Sample: Abs, Freq: 120
         Test: Existence Threshold Boolean
         ObjectOwner: aseem, Object: sethi
         OID: ifEntry.10.3, Enabled 1, Row Status 1
      Existence Entry: , Absent, Changed
      StartUp:  Present, Absent
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Boolean Entry:
         Value: 10, Cmp: 1, Start: 1
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Threshold Entry:
         Rising: 50000, Falling: 20000
         ObjOwn: ase, Obj: 01 RisEveOwn: ase, RisEve: 09 , FallEveOwn: ase, FallEve: 09

      Delta Value Table:
   (0): Thresh: Rising, Exis: 1, Read: 0, OID: ifEntry.10.3 , val: 69356097


 Mgmt Events:
```

```
(1): Owner: aseem
  (1)Name: 09 , Comment: , Action: Set, Notify, Enabled: 1 Status: 1
     Notification Entry:
        ObjOwn: , Obj: , OID: ifEntry.10.1
     Set:
        OID: ciscoSyslogMIB.1.2.1.0, SetValue: 199, Wildcard: 2 TAG: , ContextName:

Object Table:
(1): Owner: aseem
  (1)Name: sethi, Index: 1, OID: ifEntry.10.1, Wild: 1, Status: 1
```

Related Commands

Command	Description
debug management event	Allows real-time monitoring of Event MIB activities for the purposes of debugging.

show snmp

To check the status of Simple Network Management Protocol (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	This 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** global configuration 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 106 describes the fields shown in the display.

Table 106 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.
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 a MIB object that does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a 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.

Table 106 show snmp Field Descriptions (continued)

Field	Description
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** global configuration 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.
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 nonactive 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 (SNMP) 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 00000090200000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 171.69.37.61 as the IP address of the remote engine (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: 00000090200000000C025808
Remote Engine ID           IP-addr          Port
123456789ABCDEF000000000   171.69.37.61     162
```

Table 107 describes the fields shown in the example.

Table 107 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: public     security model:v1
readview:v1default
writeview:  no writeview specified
notifyview: *tv.FFFFFFFF
storage-type: volatile
```

Table 108 describes the fields shown in the example.

Table 108 show snmp group Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users that 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 nonvolatile 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 (SNMP) 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	This 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 109 describes the fields shown in the display.

Table 109 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 Simple Network Management Protocol (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 110 describes the fields shown in these displays.

Table 110 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 (SNMP) 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 00000090200000000C025808, and the storage-type as nonvolatile:

```
router# show snmp user

User name: authuser
Engine ID: 00000090200000000C025808
storage-type: nonvolatile
```

Table 111 describes fields shown in the example.

Table 111 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 (SNMP) server serial number, use the **snmp-server chassis-id** global configuration command. To restore the default value, if any, use the **no** form of this command.

snmp-server chassis-id *text*

no snmp-server chassis-id

Syntax Description

text	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 router 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:

```
Router(config)# 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 (SNMP), use the **snmp-server community** global configuration command. To remove the specified community string, use the **no** form of this command.

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

no snmp-server community *string*

Syntax Description

string	Community string that acts like a password and permits access to the SNMP protocol. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view *view-name*	(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.
number	(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.

The @ symbol 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. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

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:

```
Router(config)# 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:

```
Router(config)# snmp-server community mgr view restricted rw
```

The following example removes the community `comaccess`:

```
Router(config)# no snmp-server community comaccess
```

The following example disables all versions of SNMP:

```
Router(config)# 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. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Defaults

No system contact string is set.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

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 Simple Network Management Protocol (SNMP) inform notifications, use one of the **snmp-server enable traps** *notification-type* global configuration commands combined with the **snmp-server host** *host-addr* **informs** global configuration command.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server enable traps** global configuration command. To disable all available SNMP notifications, use the **no** form of this command.

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

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

Syntax Description

notification-type — (Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:

- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.
- **dlsw** [**circuit** | **tconn**]**—**Controls DLSw notifications, as defined in the CISCO-DLSW-MIB (enterprise 1.3.6.1.4.1.9.10.9.1.7). When the dlsw keyword is used, you can specify the specific notification types you wish to enable or disable. If no keyword is used, all DLSw notification types are enabled. The option can be one of the following keywords:
  - **circuit**—Enables DLSw circuit traps:
    (5) ciscoDlswTrapCircuitUp
    (6) ciscoDlswTrapCircuitDown
  - **tconn**—Enables DLSw peer transport connection traps:
    (1) ciscoDlswTrapTConnPartnerReject
    (2) ciscoDlswTrapTConnProtViolation
    (3) ciscoDlswTrapTConnUp
    (4) ciscoDlswTrapTConnDown
- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This is from the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is:(1) cpmDS0BusyoutNotification
- **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as: (2) cpmDS1LoopbackNotification.
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is: (1) cHsrpStateChange.

- **ipmulticast**—Controls IP Multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Controls Service Assurance Agent / Response Time Reporter (RTR) notifications.
- **syslog**—Controls error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my and the notifications are: enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification

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.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced with the **frame-relay**, **isdn**, and **envmon** trap types.
12.0(2)T	The **rsvp** keyword was added.
12.0(3)T	The **hsrp** keyword was added.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

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. 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.

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:

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

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

```
Router(config)# snmp-server enable traps bgp
Router(config)# 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:

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

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

Related Commands

Command	Description
snmp-server enable traps atm pvc	Controls (enables or disables) ATM PVC SNMP notifications.
snmp-server enable traps bgp	Controls (enables or disables) BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Controls (enables or disables) Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Controls (enables or disables) environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Controls (enables or disables) Frame Relay DLCI link staus change SNMP notifications.
snmp-server enable traps isdn	Controls (enables or disables) ISDN SNMP notifications.
snmp-server enable traps snmp	Controls (enables or disables) RFC 1157 SNMP notifications.
snmp-server enable traps repeater	Controls (enables or disables) RFC 1516 Hub notifications.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.
snmp-server informs	Specifies inform request options.

Command	Description
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 enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server** global configuration command. To disable AAA sever state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an “up” to “dead” state or when a server moves from a “dead” to “up” state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)—Server is responding to requests.
- dead(2)—Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send AAA Server up/down informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
aaa session-mib disconnect	Allows a remote network management system to perform Set operations and disconnect users on the configured device using SNMP.
show caller	Displays caller information for Async, Dialer, and Serial interfaces.
show radius statistics	Displays AAA Server MIB statistics for AAA functions.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc** global configuration command. To disable ATM PVC-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

no snmp-server enable traps atm pvc

Syntax Description

interval *seconds*	(Optional) 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.
fail-interval *seconds*	(Optional) Minimum period for storing the failed time stamp, in the range from 0 to 3600.

Defaults

SNMP notifications are disabled by default.

The default **interva**l is 30.

The default **fail-interval** is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced for those platforms that support ATM PVC Management.

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. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

ATM PVC failure notification 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.

The **snmp-server enable traps atm pvc** 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.

Examples

The following example shows the enabling of ATM PVC traps on a router, so that if PVC 0/1 goes down, host 172.16.61.90 will receive the notifications:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
show atm pvc	Displays all ATM permanent virtual circuits (PVCs) and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps bgp** global configuration command. To disable BGP state-change SNMP notifications, use the no form of this command.

snmp-server enable traps bgp

no snmp-server enable traps bgp

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Border Gateway Protocol server state change notifications, as defined in the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

(1) bgpEstablished

(2) bgpBackwardTransition.

The BGP notifications are defined in the BGP-4 MIB as follows:

```
bgpTraps                OBJECT IDENTIFIER ::= { bgp 7 }

bgpEstablished NOTIFICATION-TYPE
    OBJECTS { bgpPeerLastError,
              bgpPeerState      }
    STATUS  current
    DESCRIPTION
            "The BGP Established event is generated when
            the BGP FSM enters the ESTABLISHED state."
    ::= { bgpTraps 1 }

bgpBackwardTransition NOTIFICATION-TYPE
    OBJECTS { bgpPeerLastError,
              bgpPeerState      }
    STATUS  current
    DESCRIPTION
            "The BGPBackwardTransition Event is generated
            when the BGP FSM moves from a higher numbered
            state to a lower numbered state."
    ::= { bgpTraps 2 }
```

For a complete description of these notifications and additional MIB functions, see the BGP4-MIB.my file, available through the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

Note You may notice incorrect BGP trap OID output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

The **snmp-server enable traps bgp** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps calltracker

To enable Call Tracker CallSetup and Call Terminate Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps calltracker** global configuration command. To disable Call Tracker SNMP notifications, use the **no** form of this command.

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS580 access servers.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Call Tracker CallSetup and CallTerminate notifications. CallSetup notifications are generated at the start of each call, when an entry is created in the active table (cctActiveTable), and CallTerminate notifications are generated at the end of each call, when an entry is created in the history table (cctHistoryTable).

For a complete description of these notifications and additional MIB functions, refer to the CISCO-CALL-TRACKER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

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

Examples

The following example enables the router to send call-start and call-stop informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
calltracker call-record	Enables call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
calltracker enable	Enables the Call Tracker feature on an access server.
isdn snmp busyout b-channel	Enables PRI B channels to be busied out via SNMP.
show call calltracker	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
show modem calltracker	Displays all of the information stored within the Call Tracker Active or History Database for the latest call assigned to specified modem.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps envmon

To enable Environmental Monitor Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps envmon** global configuration command. To disable environmental monitor SNMP notifications, use the **no** form of this command.

snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

no snmp-server enable traps envmon [**shutdown**] [**voltage**] [**temperature**] [**fan**] [**supply**]

Syntax Description

shutdown	(Optional) Controls shutdown notifications. A ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1) is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.
voltage	(Optional) Controls voltage notifications. A ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2) is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).
temperature	(Optional) Controls temperature notifications. A ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3) is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).
fan	(Optional) Controls fan failure notifications. A ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4) is sent if any one of the fans in a fan array fails.
supply	(Optional) Controls Redundant Power Supply (RPS) failure notifications. A ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5) is sent if a redundant power supply fails.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3(6)AA	Support for this command was introduced for the Cisco AS5300 access server.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Environmental Monitor (EnvMon) status notifications for supported systems. Cisco enterprise EnvMon notifications are triggered when an environmental threshold is exceeded. If none of the optional keywords are specified, all available environmental notifications are enabled.

For a complete description of these notifications and additional MIB functions, see the CISCO-ENVMON-MIB.my and CISCO-ACCESS-ENVMON-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Status of the Environmental Monitor can be viewed using the **show environment** command.

The **snmp-server enable traps envmon** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables a Cisco 12000 GSR to send environmental failure informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
show environment	Displays environmental conditions on the system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay

To enable Frame Relay DLCI link status Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** global configuration command. To disable Frame Relay link status SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Data Link Connection Identifier (DLCI) Frame Relay notifications, as defined in the RFC1315-MIB (enterprise 1.3.6.1.2.1.10.32).

The notification type is frDLCIStatusChange (1). This trap indicates that the indicated Virtual Circuit (VC) has changed state, meaning that the VC has either been created or invalidated, or has toggled between the active and inactive states.

Note For large scale configurations (systems containing hundreds of Frame Relay point-to-point subinterfaces), note that having Frame Relay notifications enabled could potentially have a negative impact on network performance when there are line status changes.

For a complete description of this notification and additional MIB functions, see the RFC1315-MIB.my file and the CISCO-FRAME-RELAY-MIB.my file, available in the "v1" and "v2" directories, repectively, at the Cisco.com MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

The **snmp-server enable traps frame-relay** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following examplethe router is configured to send Frame Relay DLCI state change informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN) specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn** global configuration command. To disable ISDN-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

no snmp-server enable traps isdn [**call-information**] [**chan-not-avail**] [**isdnu-interface**] [**layer2**]

Syntax Description

call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.
layer2	(Optional) Controls SNMP ISDN layer2 transition notifications.

Defaults

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	The **snmp-server enable traps isdn** command was introduced.
11.3	The **call-information** and **isdnu-interface** keywords were added for the Cisco 1600 series router.

Release	Modification
12.0	Support for the **call-information** and **isdnu-interface** keywords was introduced for most voice platforms.
12.1(5)T	Support for the **isdn chan-not-available** option was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers only.

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. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn** 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 isdn** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows the checking of what notification types are available on a Cisco AS5300, and the enabling of channel-not-available and layer2 informs:

```
NAS(config)#snmp-server enable traps isdn ?
  call-information  Enable SNMP isdn call information traps
  chan-not-avail    Enable SNMP isdn channel not avail traps
  layer2            Enable SNMP isdn layer2 transition traps
  <cr>

NAS(config)#snmp-server enable traps isdn chan-not-avail layer2
NAS(config)#snmp-server host myhost.cisco.com informs version 2c public isdn
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
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 that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** global configuration command. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string . For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the authoritative SNMP engine's window (for example, falls outside of configured access lists or time ranges).
linkup	(Optional) Controls the sending of SNMP linkUp notifications. A linkUp(3) trap signifies that the sending device recognizes that one of the communication links represented in the agent's configuration has come up.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications. A linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications. A coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications. A warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

Defaults

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all RFC 1157 SNMP notifications are enabled (or disabled, if using the **no** form).

Command Modes

Global configuration

Command History

Release	Modification
11.3	The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command.
12.1(3)T	The following keywords were added: • **linkup** • **linkdown** • **coldstart**
12.1(5)T	The **warmstart** 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.

If you do not enter an **snmp-server enable traps snmp** 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 snmp** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** 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 **snmp-server enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable these traps on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. Note that on the interface level, linkUp and linkDown traps are enabled by default. This means that you do not have to enable these notifications on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

Examples

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

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

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

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

The following example shows the enabling all SNMP trap types, then the disabling of only the linkUp and linkDown traps.

```
Router> enable
Password:
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
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 that an SNMP trap should originate from.

snmp-server enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater** global configuration command. To disable repeater notifications, use the **no** form of this command.

snmp-server enable traps repeater [**health**] [**reset**]

no snmp-server enable traps repeater [**health**] [**reset**]

Syntax Description

health	(Optional) The rptrHealth trap conveys information related to the operational status of the repeater. This trap is sent either when the value of rptrOperStatus changes, or upon completion of a non-disruptive test. The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows: • other(1)—undefined or unknown status • ok(2)—no known failures • rptrFailure(3)—repeater-related failure • groupFailure(4)—group-related failure • portFailure(5)—port-related failure • generalFailure(6)—failure, unspecified type
reset	(Optional) The rptrResetEvent trap is sent on completion of a repeater reset action (triggered by the transition to a START state by a manual command). The rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

Defaults

SNMP notifications are disabled by default.

If no keywords are specified, all repeater notifications available on your system are enabled or disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

There are two sets of notifications available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at http://www.cisco.com/public/mibs/.

The **snmp-server enable traps repeater** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

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

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps voice poor-qov

To enable poor quality of voice Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps voice poor-qov** global configuration command. To disable poor quality of voice SNMP notifications, use the **no** form of this command.

snmp-server enable traps voice poor-qov

no snmp-server enable traps voice poor-qov

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) poor-quality-of-voice notifications. The poor-quality-of-voice notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

For a complete description of this notification and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps voice poor-qov** 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. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server engineID

To configure a name for either the local or remote Simple Network Management Protocol (SNMP) 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	Specifies the local copy of SNMP on the router. (You must specify either **local** or **remote**.)
engineid-string	The name of a copy of SNMP.
remote	Specifies the remote copy of SNMP on the router. (You must specify either **local** or **remote**.)
ip-address	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.
port	(Optional) The socket number on the remote device that contains the remote copy of SNMP.

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.

The default **udp-port** for remote engines is 161.

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 123400000000000000000000, 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 (SNMP) 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

groupname	The name of the group.
v1	The least secure of the possible security models.
v2c	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	The most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	(Optional) The option that allows you to specify a read view.
readview	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.
writeview	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
notifyview	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.
access-list	A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 112 describes default values for the different views.

Table 112 snmp-server group Default Descriptions

Default	Definition
readview	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 112 snmp-server group Default Descriptions (continued)

Default	Definition
writeview	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notifyview	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

Command History

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:

```
Router(config)# 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 a Simple Network Management Protocol (SNMP) 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

host-addr	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C. • **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword: – **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – **noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified. – **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	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. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
udp-port *port*	(Optional) UDP port of the host to use. The default is 162.

notification-type	(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: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **calltracker**—Sends Call Tracker call-start/call-end 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 any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications. • **stun**—Sends serial tunnel (STUN) notifications. • **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. • **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command. • **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 Cisco IOS Release 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: • **version 3** [**auth** | **noauth** | **priv**] • **hsrp**
11.3(1) MA, 12.0(3)T	The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.

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. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The @ symbol 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. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

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:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

The following example sends RFC 1157 SNMP traps to the host specified by the name 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 sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# 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:

```
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.

```
Router(config)# snmp-server enable traps bgp
Router(config)# 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:

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

The following example sends 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
```

Related Commands

Command	Description
snmp-server enable peer-trap poor qov	Enable 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 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. To return the settings to the defaults, use the **no** form of this command.

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

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

Syntax Description

retries *retries*	(Optional) Maximum number of times to resend an inform request. The default is 3.
timeout *seconds*	(Optional) Number of seconds to wait for an acknowledgment before resending. The default is 30 seconds.
pending *pending*	(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. 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.

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:

```
snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
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** global configuration command. 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.

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. 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 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

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 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 (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** global configuration command. 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 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

length	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.

During device bootup, there is a possibility that some traps could be dropped because of trap queue overflow on the device. If you suspect this is occuring, you can increase the size of the trap queue (for example, to 100) to determine if traps are then able to be sent during bootup.

Examples

In the following example, the SNMP notification queue is increased 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 system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** global configuration command. 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.

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 (SNMP) 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

number	Standard IP access list number from 1 to 99.

Defaults

Disabled

Command Modes

Global configuration

Command History

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:

```
snmp-server tftp-server-list 44
```

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 link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps which 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	This required keyword indicates to the command parser that you would like to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (as opposed to the previous Cisco implementation).

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

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# config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server trap link ietf
Router(config)# end
Router# more system:running config
.
.
.
!
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-source

To specify the interface (and hence the corresponding IP address) that an Simple Network Management Protocol (SNMP) trap should originate from, use the **snmp-server trap-source** global configuration command. 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. The argument includes the interface type and number in platform-specific syntax (for example, *type*/*slot*/*port*).

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 or inform is sent from a Cisco SNMP server, it has a notification address of whatever interface it happened to go out of at that time. Use this command monitor notifications from a particular interface.

Examples

The following example specifies that the IP address for interface Ethernet 0 is the source for all SNMP notifications:

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

The following example specifies that the IP address for the ethernet interface in slot2, port 1 is 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 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

seconds	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 a Simple Network Management Protocol (SNMP) 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** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]

no snmp-server user

Syntax Description

username	The name of the user on the host that connects to the agent.
groupname	The name of the group to which the user belongs.
remote *host*	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IP address of that entity.
udp-port *port*	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** and/or **auth** keywords.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
auth-password	A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
access *access-list*	(Optional) Specifies an access list to be associated with this SNMP user. The *access-list* argument represents a value from1 to 99 that is the identifier of the standard IP access list.

Defaults

Table 113 describes default behaviors for encryption, passwords and access lists.

Table 113 snmp-server user Default Descriptions

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

Command Modes

Global configuration

Command History

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

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 (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 | **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 (SNMP) 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

Command History

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
```