SNMP Commands

This chapter contains the following sections:

snmp-server community

To set the community access string (password) that permits access to SNMP commands (v1 and v2), use the **snmp-server community** Global Configuration mode command. This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community *community-string [***ro** | **rw** | **su***]* [*ip-address* | *ipv6-address*] *[***mask** *mask* | **prefix** *prefix-length] [***view** *view-name]* [**type** {**router** | **oob**}]

no snmp-server community *community-string [ip-address]* [**type** {**router** | **oob**}]

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- **ro**—(Optional) Specifies read-only access (default)
- **rw**—(Optional) Specifies read-write access
- **su**—(Optional) Specifies SNMP administrator access
- **ip-address**—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address.
- **mask**—(Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—(Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- **view** *view-name*—(Optional) Specifies the name of a view configured using the command snmp-server view, on page 9 (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for **su**, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables , are available. (Range: 1–30 characters)
- **type** *router*—(Optional) Indicates whether the IP address is on the out-of-band or in-band network.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

The logical key of the command is the pair (community, ip-address). If ip-address is omitted, the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The *view-name* is used to restrict the access rights of a community string. When a view-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

Example

Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

snmp-server community-group

To configure access rights to a user group, use **snmp-server community-group**. The group must exist in order to be able to specify the access rights. This command configures both SNMP v1 and v2.

Syntax

snmp-server community-group *community-string group-name [ip-address | ipv6-address]* **[mask** *mask* | **prefix** *prefix-length]* [**type** {**router** | **oob**}]

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- **group-name**—This is the name of a group configured using snmp-server group, on page 11 with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)
- **ip-address**—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address.
- **mask**—(Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—(Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- **type** *router*—(Optional) Indicates whether the IP address is on the out-of-band or in-band network.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

The *group-name* is used to restrict the access rights of a community string. When a group-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Example

Defines a password *tom* for the group *abcd* that enables this group to access the management station 1.1.1.121 with prefix 8.

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

snmp-server server

To enable the device to be configured by the SNMP protocol, use the **snmp-server server** Global Configuration mode command. To disable this function, use the **no** form of this command.

Syntax

snmp-server server

no snmp-server server

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# snmp-server server
```

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in Global Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

snmp-server source-interface {**traps** | **informs**} *interface-id*

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

Parameters

- **traps**—Specifies the SNMP traps interface.
- **informs**—Specifies the SNMP informs.
- **interface-id**—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

If no parameters are specified in **no snmp-server source-interface**, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the **no snmp-server source-interface traps** command to remove the source interface for SNMP traps.

Use the **no snmp-server source-interface informs** command to remove the source interface for SNMP informs.

Use the **no snmp-server source-interface** command to remove the source interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface for traps.

```
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```

snmp-server source-interface-ipv6

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in Global Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

snmp-server source-interface-ipv6 {**traps** | **informs**} *interface-id*

no snmp-server source-interface-ipv6 [**traps** | **informs**]

Parameters

- **traps**—Specifies the SNMP traps interface.
- **informs**—Specifies the SNMP traps informs.
- **interface-id**—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address of the outgoing interface and selected in accordance with RFC6724.

If no parameters are specified in **no snmp-server source-interface**, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces is selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the **no snmp-server source-interface-ipv6 traps** command to remove the source IPv6 interface for SNMP traps.

Use the **no snmp-server source-interface-ipv6 informs** command to remove the source IPv6 interface for SNMP informs.

Use the **no snmp-server source-interface-ipv6** command to remove the source IPv6 interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

snmp-server view

To create or update an SNMP view, use the **snmp-server view** Global Configuration mode command. To remove an SNMP view, use the **no** form of this command.

Syntax

snmp-server view *view-name oid-tree {***included** | **excluded***}*

no snmp-server view *view-name* [*oid-tree*]

Parameters

- **view-name**—Specifies the name for the view that is being created or updated. (Length: 1–30 characters)
- **included**—Specifies that the view type is included.
- **excluded**—Specifies that the view type is excluded.
- **oid-tree**—(Optional) Specifies the ASN.1 subtree object identifier 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 and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.

Default Configuration

The following views are created by default:

- **Default**—Contains all MIBs except for those that configure the SNMP parameters themselves.
- **DefaultSuper**—Contains all MIBs.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view.

The command's logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example

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 interface group (this format is specified on the parameters specified in ifEntry).

```
switchxxxxxx(config)# snmp-server view user-view system included
switchxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

snmp-server group

To configure an SNMP group, use the **snmp-server group** Global Configuration mode command. Groups are used to map SNMP users to SNMP views. To remove an SNMP group, use the **no** form of this command.

Syntax

snmp-server group *groupname* {***v1*** | **v2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*]} [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* {**v1** | **v2** | **v3** [**noauth** | **auth** | **priv**]}

Parameters

- **group** *groupname*—Specifies the group name. (Length: 1–30 characters)
- **v1**—Specifies the SNMP Version 1 security model.
- **v2**—Specifies the SNMP Version 2 security model.
- **v3**—Specifies the SNMP Version 3 security model.
- **noauth**—Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.
- **auth**—Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.
- **priv**—Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.
- **notify** *notifyview*—(Optional) Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgment. Applicable only to the SNMP version 3 security model. (Length: 1–32 characters)
- **read** *readview*—(Optional) Specifies the view name that enables viewing only. (Length: 1–32 characters)
- **write** *writeview*—(Optional) Specifies the view name that enables configuring the agent. (Length: 1–32 characters)

Default Configuration

No group entry exists.

If *notifyview* is not specified, the notify view is not defined.

If *readview* is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval.

If *writeview* is not specified, the write view is not defined.

Command Mode

Global Configuration mode

User Guidelines

The group defined in this command is used in the snmp-server user , on page 16 command to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is (**groupname, snmp-version, security-level**). For snmp-version v1/v2 the security-level is always **noauth**.

Example

The following example attaches a group called *user-group* to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called *user-view* to read-only. User *tom* is then assigned to *user-group*. So that user *tom* has the rights assigned in *user-view*.

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

show snmp views

To display SNMP views, use the **show snmp views** Privileged EXEC mode command.

Syntax

show snmp views [*viewname*]

Parameters

viewname—(Optional) Specifies the view name. (Length: 1–30 characters)

Default Configuration

If viewname is not specified, all views are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP views.

```
switchxxxxxx# show snmp views

Name                OID Tree                Type
----------------    ----------------------  ----------
Default             iso                     Included
Default             snmpNotificationMIB     Excluded
DefaultSuper        iso                     Included
```

show snmp groups

To display the configured SNMP groups, use the **show snmp groups** Privileged EXEC mode command.

Syntax

show snmp groups [*groupname*]

Parameters

groupname—(Optional) Specifies the group name. (Length: 1–30 characters)

Default Configuration

Display all groups.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP groups.:

switchxxxxxx# **show snmp groups**							
Name		Security				Views	
------------- user-group managers-group	Model ----- V2 V2		Level ---- no_auth no_auth		Read ------- Default Default	Write ------- "" Default	Notify ------- "" ""

The following table describes significant fields shown above.

Field		Description
Name		**Group name.**
Security	Model	SNMP model in use (v1, v2 or v3).
Security	Level	Packet security. Applicable to SNMP v3 security only .

Field		Description
Views	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

snmp-server user

To configure a new SNMP user, use the **snmp-server user** Global Configuration mode command. To remove a user, use the **no** form of the command. To enter the authentication and privacy passwords in encrypted form (see SSD), use the **encrypted** form of this command.

Syntax

snmp-server user *username groupname* {**v1** | **v2c** | [**remote** *host*] **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *auth-password* [***priv*** *priv-password*]]}

encrypted snmp-server user *username groupname* {**v1** | **v2c** | [**remote** *host]* **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *encrypted-auth-password* [**priv** *encrypted-priv-password*]]}

no snmp-server user *username* {**v1** | **v2c** | [**remote** *host*] ***v3***}

Parameters

- **username**—Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters).
- **groupname**—The name of the group to which the user belongs. The group should be configured using the command snmp-server group, on page 11 with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- **v1**—Specifies that the user is a v1 user.
- **v2c**—Specifies that the user is a v2c user..
- **v3**—Specifies that the user is a v3 user..
- **remote** *host*—(Optional) IP address (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host.
- **auth**—(Optional) Specifies which authentication level is to be used.

  Sha—(Optional) Specifies the HMAC-SHA-96 authentication level.

  Sha224—(Optional) Specifies the HMAC-SHA-224-128 authentication level.

  Sha256—(Optional) Specifies the HMAC-SHA-256-192 authentication level.

  Sha384—(Optional) Specifies the HMAC-SHA-384-256 authentication level.

  Sha512—(Optional) Specifies the HMAC-SHA-512-384 authentication level.
- ***auth-password***—(Optional) Specifies the authentication password. Range: Up to 32 characters.
- ***encrypted-auth-password***—(Optional) Specifies the authentication password in encrypted format.
- **priv** *priv-password*—(Optional) specifies private (priv) encryption and the privacy password (Range: Up to 32 characters). The encryption algorithm used is Advanced Encryption Standard (AES) privacy algorithm in Cipher Feedback Mode (CFB) using 128 bits encryption keys),
- ***encrypted-priv-password***—(Optional) Specifies the privacy password in encrypted format.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

For SNMP v1 and v2, this command performs the same actions as snmp-server community-group, except that snmp-server community-group configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

A local SNMP EngineID must be defined in order to add SNMPv3 users to the device. For remote hosts users a remote SNMP EngineID is also required.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users' database.

The logical key of the command is username.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgment. A configured remote host is also able to manage the device (besides getting the informs).

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the snmp-server engineID remote , on page 26 command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.

Example

This example assigns user *tom* to group *abcd* using SNMP v1 and v2c. . User *jerry* is assigned to group *efgh* using SNMP v3.

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user jerry efgh v3 auth sha pass1234
```

show snmp users

To display the configured SNMP users, use the **show snmp users** Privileged EXEC mode command.

Syntax

show snmp users [*username*]

Parameters

username—(Optional) Specifies the user name. (Length: 1–30 characters)

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example

The following examples displays the configured SNMP users:

```
switchxxxxxx# show snmp users
User name                          :u1rem
  Group name                       :group1
  Authentication Method      : None
  Privacy Method             : None
  Remote                           :11223344556677
  Auth Password                    :
  Priv Password                    :
User name                          : qqq
  Group name                       : www
  Authentication Method      : SHA256
  Privacy Method             : None
  Remote                           :
  Auth Password                    : helloworld1234567890987665
  Priv Password                    :
User name                          : hello
  Group name                       : world
  Authentication Method      :  SHA256
  Privacy Method             :  AES-128
  Remote                           :
  Auth Password (encrypted): Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLRdAgOE6XQKTC
                             qMlrnpWuHraRlZj
  Priv Password (encrypted) : kN1ZHzSLo6WWxlkuZVzhLOo1gI5waaNf7Vq6yLBpJdS4N68tL
                             1tbTRSz2H4c4Q4o
User name                          : u1noAuth
  Group name                       : group1
  Authentication Method            : None
  Privacy Method                   : None
  Remote                             :
  Auth Password (encrypted)        :
  Priv Password (encrypted)        :
User name                          : u1OnlyAuth
  Group name                       : group1
  Authentication Method      : SHA1
```

```
Privacy Method               : None
Remote                         :
Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
Priv Password (encrypted) :
```

snmp-server filter

To create or update an SNMP server notification filter, use the **snmp-server filter** Global Configuration mode command. To remove a notification filter, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree {***included** | **excluded***}*

no snmp-server filter *filter-name* [*oid-tree*]

Parameters

- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the filter in other commands. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier 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 sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.

Default Configuration

No view entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).

Example

The following example creates a filter 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 (this format depends on the parameters defined in ifEntry).

```
switchxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

show snmp filters

To display the defined SNMP filters, use the **show snmp filters** Privileged EXEC mode command.

Syntax

show snmp filters [*filtername*]

Parameters

filtername—Specifies the filter name. (Length: 1–30 characters)

Default Configuration

If filtername is not defined, all filters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP filters.

```
switchxxxxxx# show snmp filters user-filter

Name            OID Tree                 Type
------------    ---------------------    ---------
user-filter     1.3.6.1.2.1.1            Included
user-filter     1.3.6.1.2.1.1.7          Excluded
user-filter     1.3.6.1.2.1.2.2.1.*.1    Included
```

snmp-server host

To configure the host for SNMP notifications: (traps/informs), use the **snmp-server host** Global Configuration mode command. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server host *{host-ip | hostname} [***traps** | **informs***] [***version** *{**1** | **2c** | **3** [***auth** | **noauth** | **priv***]}] community-string [***udp-port** *port] [***filter** *filtername] [***timeout** *seconds] [***retries** *retries]*

no snmp-server host *{ip-address | hostname} [***traps** | **informs***] [***version** *{***1** | **2c** | **3***}]*

Parameters

- **host-ip**—IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address.
- **hostname**—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- **trap**—(Optional) Sends SNMP traps to this host (default).
- **informs**—(Optional) Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- ***version* 1**—(Optional) SNMPv1 traps are used.
- ***version* 2c**—(Optional) SNMPv2 traps or informs are used
- ***version* 3**—(Optional) SNMPv2 traps or informs are used
- Authentication options are available for SNMP v3 only. The following options are available:

  noauth—(Optional) Specifies no authentication of a packet.

  auth—(Optional) Specifies authentication of a packet without encryption.

  priv—(Optional) Specifies authentication of a packet with encryption.
- **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in snmp-server user (ISCLI) command for v3.
- **udp-port** *port*—(Optional) UDP port of the host to use. The default is 162. (Range: 1–65535)
- **filter** *filtername*—(Optional) Filter for this host. If unspecified, nothing is filtered. The filter is defined using **snmp-server filter** (no specific order of commands is imposed on the user). (Range: Up to 30 characters)
- **timeout** *seconds*—(Optional) (For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)
- **retries** *retries*—(Optional) (For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

Default Configuration

Version: SNMP V1

Type of notification: Traps

udp-port: 162

If informs are specified, the default for retries: 3

Timeout: 15

Command Mode

Global Configuration mode

User Guidelines

The logical key of the command is the list (ip-address/hostname, traps/informs, version).

When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

, use the commands snmp-server user (ISCLI) and snmp-server group to create a user or a group.

Example

The following defines a host at the IP address displayed.

switchxxxxxx(config)# *snmp-server host 1.1.1.121 abc*

snmp-server engineID local

To specify the SNMP engineID on the local device for SNMP v3, use the **snmp-server engineID local** Global Configuration mode command. To remove this engine ID, use the **no** form of this command.

Syntax

snmp-server engineID local {*engineid-string* | ***default***}

no snmp-server engineID local

Parameters

- **engineid-string**—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- **default**—Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is the allocated IANA Enterprise number.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.

As the engineID should be unique within an administrative domain, the following guidelines are recommended:

- Configure a non-default EngineID, and verify that it is unique within the administrative domain.
- Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users database.
- The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001.

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
switchxxxxxx(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
```

```
Do you wish to continue? [Y/N]Y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y
```

snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the **snmp-server engineID remote** Global Configuration mode command. To remove the configured engine ID, use the **no** form of this command.

Syntax

snmp-server engineID remote *ip-address engineid-string*

no snmp-server engineID remote *ip-address*

Parameters

- **ip-address** —IPv4, IPv6 or IPv6z address of the remote device.
- **engineid-string**—The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: engineid-string5–32 characters. 9–64 hexadecimal digits)

Default Configuration

The remote engineID is not configured by default.

Command Mode

Global Configuration mode

User Guidelines

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

Example

```
switchxxxxxx(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

show snmp engineID

To display the local SNMP engine ID, use the **show snmp engineID** Privileged EXEC mode command.

Syntax

show snmp engineID

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP engine ID.

```
switchxxxxxx# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
IP address Remote SNMP engineID
---------- --------------------------------
172.16.1.1 08009009020C0B099C075879
```

snmp-server enable traps

To enable the device to send SNMP traps, use the **snmp-server enable traps** Global Configuration mode command. To disable all SNMP traps, use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

If **no snmp-server enable traps** has been entered, you can enable failure traps by using snmp-server trap authentication, on page 29 as shown in the example.

Example

The following example enables SNMP traps except for SNMP failure traps.

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```

snmp-server trap authentication

To enable the device to send SNMP traps when authentication fails, use the **snmp-server trap authentication** Global Configuration mode command. To disable SNMP failed authentication traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Parameters

This command has no arguments or keywords.

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

Example

The following example disables all SNMP traps and enables only failed authentication traps.

```
switchxxxxxx(config)# no snmp-server enable traps
switchxxxxxx(config)# snmp-server trap authentication
```

snmp-server contact

To set the value of the system contact (sysContact) string, use the **snmp-server contact** Global Configuration mode command. To remove the system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

text—Specifies system contact information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the system contact information to Technical_Support.

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```

snmp-server location

To set the value of the system location string, use the **snmp-server location** Global Configuration mode command. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

Parameters

text—Specifies the system location information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the device location to New_York.

```
switchxxxxxx(config)# snmp-server location New_York
```

snmp-server set

To define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command, use the **snmp-server set** Global Configuration mode command.

Syntax

snmp-server set *variable-name name value* [*name2 value2...*]

Parameters

- **variable-name**—Specifies an SNMP MIB variable name, which must be a valid string.
- **name** *value*—Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command.

Example

The following example configures the scalar MIB sysName with the value TechSupp.

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

snmp trap link-status

To enable link-status generation of SNMP traps, use the **snmp trap link-status** Interface Configuration mode command. To disable generation of link-status SNMP traps, use the **no** form of this command.

Syntax

snmp trap link-status

no snmp trap link-status

Parameters

This command has no arguments or keywords.

Default Configuration

Generation of SNMP link-status traps is enabled

Command Mode

Interface Configuration mode

Example

The following example disables generation of SNMP link-status traps.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# # no snmp trap link-status
```

show snmp

To display the SNMP status, use the **show snmp** Privileged EXEC mode command.

Syntax

show snmp

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:

Community-String   Community-Access   View name     IP Address     Mask
----------------   ----------------   ------------  ----------     ----
public             read only          user-view     All
private            read write         Default       172.16.1.1/10
private            su                 DefaultSuper  172.16.1.1

Community-string   Group name   IP Address   Mask   Type
----------------   ----------   ----------          ------
public             user-group   All                 Router

Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications

Target Address   Type     Community   Version   UDP    Filter   TO    Retries
-----------      ----     --------    -------   Port   Name     Sec   -------
192.122.173.42   Trap     public      2         ----   ------   ---   3
192.122.173.42   Inform   public      2         162             15    3
                                                162             15

Version 3 notifications
```

Target Address	Type	Username	Security Level	UDP Port	Filter name	TO Sec	Retries
192.122.173.42	Inform	Bob	Priv	162		15	3

System Contact: Robert
System Location: Marketing

The following table describes the significant fields shown in the display.

Field	Description
Community-string	The community access string permitting access to SNMP.
Community-access	The permitted access type—read-only, read-write, super access.
IP Address	The management station IP Address.
Target Address	The IP address of the targeted recipient.
Version	The SNMP version for the sent trap.