

Network Management Configuration Commands (GTL-2091)



Table of Contents

Chapter 1 Network Management Configuration Commands	1
1.1 SNMP Commands	1
1.1.1 snmp-server community	2
1.1.2 snmp-server contact	3
1.1.3 snmp-server group	4
1.1.4 snmp-server [host hostv6]	5
1.1.5 snmp-server location	7
1.1.6 snmp-server packet-size	8
1.1.7 snmp-server queue-length	8
1.1.8 snmp-server trap-source	9
1.1.9 snmp-server trap-timeout	10
1.1.10 snmp-server user	11
1.1.11 snmp-server view	12
1.1.12 snmp-server source-addr	13
1.1.13 snmp-server udp-port	14
1.1.14 snmp-server encryption	15
1.1.15 snmp-server trap-add-hostname	16
1.1.16 snmp-server trap-logs	16

Chapter 1 Network Management Configuration Commands

1.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server group
- snmp-server host/hosts6
- snmp-server location
- snmp-server packet-size
- snmp-server queue-length
- snmp-server trap-source
- snmp-server trap-timeout
- snmp-server user
- snmp-server view
- snmp-server source-addr
- snmp-server udp-port
- snmp-server encryption
- snmp-server trap-add-hostname
- snmp-server trap-logs
- snmp-server set-snmp-dos-max
- snmp-server keep-alive
- snmp-server encode
- snmp-server event-id
- show snmp
- debug snmp

1.1.1 snmp-server community

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode.

snmp-server community [0|7] *string* [**view** *view-name*] [**ro** | **rw**] [*word*]

no snmp-server community *string*

no snmp-server community

Parameter

Parameter	Description
0	Sets the community string of the text.,
7	Sets the encrypted public string of the text.
<i>string</i>	Means the community string of the accessible SNMP protocol, which is similar to the password.
<i>view view-name</i>	(optional) stands for the previously defined view's name. In this view, the MIB objects, which are effective to the community, are defined.
<i>ro</i>	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects.
<i>rw</i>	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects.
<i>word</i>	(optional) Specifies the name of IP ACL of the SNMP proxy, which can be accessed by the community string.

Default value

By default, the SNMP community string allows the read-only permission to all objects.

Command mode

Global configuration mode

Explanation

The following command shows how to delete a designated community.

no snmp-server community *string*

The following command shows how to delete all communities.

no snmp-server community

Example

The following example shows how to distribute the “comaccess” string to SNMP, allow the read-only access and designate IP ACL to use the community string.

snmp-server community comaccess ro allowed

The following example shows how to distribute the “mgr” string to SNMP, allow to read and write the objects in the **Restricted** view.

snmp-server community mgr view restricted rw

The following example shows how to delete the “comaccess” community.

no snmp-server community comaccess

Related command

access-list

snmp-server view

1.1.2 snmp-server contact

To set the information about the contact person in a management node, run **snmp-server contact *text***.

snmp-server contact *text*

no snmp-server contact

Parameter

Parameter	Description
<i>text</i>	Means the string of the information about the contact person.

Default value

The information about contact person is not set.

Command mode

Global configuration mode

Explanation

It corresponds to the **sysContact** of the **MIB** variable in the **System** group.

Example

The following example shows the information about the contact person in a node.

```
snmp-server contact Dial_System_Operator_at_beeper_#_27345
```

1.1.3 snmp-server group

To create or update a SNMP group in global configuration mode, run the following first command; to cancel this SNMP group, run the following second command.

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

Parameter

Parameter	Description
groupname	Stands for the name of the created or modified SNMP group.
v3	Means the version ID of the SNMP protocol.
auth noauth priv	Stands for the lowest security level of users in the SNMPv3 group.
readview	Means the access permission of GET operations, which is defined by the view.
writeview	Means the access permission of SET operations, which is defined by the view.
notifyview	Stands for the access permission during the transmission of Trap packets, which is defined by the view.
access-list	Allows users in the SNMP group to get through the IP access control list.

Default value

The readview allows all leaves of the Internet sub-tree to be accessed.

Command mode:

Global configuration mode

Instruction

The SNMP group is used to designate the access permission of the users in this group.

Example

In the following example, an SNMP group is set and named as **setter**, the version ID of the SNMP protocol is 3, the security level is authentication and encryption, and the view that is accessed by the **set** operation is **v-write**.

```
snmp-server group setter v3 priv write v-write
```

Related command

```
snmp-server view
```

```
snmp-server user
```

1.1.4 snmp-server [host|hostv6]

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command.

```
snmp-server host|hostv6 host [vrf word] [udp-port port-num] [permit|deny event-id]
{version [v1 | v2c | v3]} | {[informs | traps] | [auth | noauth]}
community-string/user [authentication | configure| snmp]
```

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

Parameter

Parameter	Description
host hostv6	Sets the IPv4 or IPv6 host.
<i>host</i>	Means the host's name or the address of the Internet.
[vrf word]	(Optional) binds VRF.
[udp-port port-num]	(Optional) Specifies the ID of the UDP port, which transmits the traps.
[permit deny event-id]	(Optional) Allows or blocks to transmit a designated event.
{version [v1 v2c v3]}	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps.
[informs traps]	(Optional) Specifies the type of trap for version V2C. Informs: means the type of trap is "informs". Traps: means the type of trap is "traps".
[auth noauth]	Specifies the trap authentication mode for version V3. auth: authentication

	noauth: no authentication
<i>community-string/user</i>	Means a community string in version 1 and version 2c which is similar to the password and sent with the trap operations or means the username in version 3.
[authentication configure snmp]	(optional) if no trap is designated, all generated traps will be sent to the host. authentication: allows to transmit those authentication-error traps. configure: allows to transmit the SNMP-configure traps. snmp: allows to transmit the SNMP traps.

Default value

This command is invalid in default settings. That is to say, no trap will be sent by default.

Command mode

Global configuration mode

Explanation

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps, you must run **snmp-server host**. If the keyword “trap-type” is not contained in this command, all kinds of traps of this host will be activated. If the keyword “trap-type” is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host.

If you designate multiple **snmp-server host** commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string).

The availability of the **trap-type** option depends on the switch type and the attributes of routing software, which is supported by this switch.

Example

The following example shows how to transmit the RFC1157-defined SNMP traps to host 10.20.30.40. The community string is defined as **comaccess**.

```
snmp-server host 10.20.30.40 comaccess snmp
```

The following example shows that the switch uses the **public** community string to send all types of traps to host 10.20.30.40.

```
snmp-server host 10.20.30.40 public
```


The following example shows that only the authentication traps are effective and can be sent to host **bob**.

```
snmp-server host bob public authentication
```

Related command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

snmp-server event-id

snmp-server user

1.1.5 snmp-server location

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this location string, run the following second command.

snmp-server location *text*

no snmp-server location

Parameter

Parameter	Description
<i>text</i>	Describes the location string of a node.

Default value

The location string of a node is not set by default.

Command mode

Global configuration mode

Explanation

It corresponds to the **sysLocation** of the **MIB** variable in the **System** group.

Example

The following example shows how to define the actual location of a switch.

```
snmp-server location Building_3/Room_214
```

Related command

snmp-server contact

1.1.6 snmp-server packetsize

To define the maximum size of the SNMP packet when the SNMP server receives requests or responds, run the following first command in global configuration mode.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter

Parameter	Description
<i>byte-count</i>	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes.

Default value

3000 byte

Command mode

Global configuration mode

Explanation

It corresponds to the **sysLocation** of the **MIB** variable in the **System** group.

Example

The following example shows how to set up a filter to filter those packets whose maximum length is 1024 bytes.

snmp-server packetsize 1024

Related command

snmp-server queue-length

1.1.7 snmp-server queue-length

To set the queue length for each trap host, run the following first command in global configuration mode.

snmp-server queue-length *length*

no snmp-server queue-length

Parameter

Parameter	Description
<i>length</i>	Stands for the number of trap events which can be saved in the queue (1-1000).

Default value

10 trap events.

Command mode

Global configuration mode

Explanation

This command is used to set the queue length for each trap host. Once the trap messages are successfully transmitted, the switch will empty the queue.

Example

The following example shows how to set up a message queue which can capture four events.

```
snmp-server queue-length 4
```

Related command

snmp-server packetsize

1.1.8 snmp-server trap-source

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter

Parameter	Description
<i>interface</i>	Stands for the interface where SNMP traps generate. The parameters include the interface type and interface ID of the

	syntax mode of specific platform.
--	-----------------------------------

Default value

The interface is not designated.

Command mode

Global configuration mode

Explanation

When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command.

Example

The following example shows how to designate interface vlan1 as the source address of all traps.

```
snmp-server trap-source vlan1
```

Related command

snmp-server queue-length

snmp-server host

1.1.9 snmp-server trap-timeout

To set the timeout value of retransmitting traps, run the following first command in global configuration mode.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter

Parameter	Description
<i>seconds</i>	Means an interval for retransmitting traps, whose unit is second (1-1000).

Default value

30 seconds

Command mode

Global configuration mode

Explanation

Before switch software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The **server trap-timeout** command decides the retransmission interval.

Example

The following example shows how to set the retransmission interval to 20 seconds:

```
snmp-server trap-timeout 20
```

Related command

```
snmp-server host
```

```
snmp-server queue-length
```

1.1.10 snmp-server user

To create or update an SNMP user in global configuration mode, run the following first command; to cancel this SNMP user, run the following second command. If the **remote** parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist.命令格式如下

```
snmp-server user username groupname { v3 [ encrypted | auth ] [ md5 | sha ]  
auth-password }
```

Parameter

Parameter	Description
<i>username</i>	Stands for the name of the created or modified SNMP user.
<i>groupname</i>	Stands for the group where the user is.
v3	Stands for the SNMP version.
[encrypted auth]	Encryption type: Encrypted: packet encryption auth: packet authentication
[md5 sha]	Means the method of encryption authentication.
<i>auth-password</i>	Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key

	and the encryption key of SNMPv3.
--	-----------------------------------

Default value

N/A

Command mode

Global configuration mode

Explanation

This command is used to set the username and the password.

Example

In the following example, an SNMP user is created, whose name is **set-user** and which belongs to group **setter**, the version of the SNMP protocol is version 3, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the hash algorithm.

```
snmp-server user set-user setter v3 encrypted auth md5 12345678
```

Related command

snmp-server view

snmp-server group

1.1.11 snmp-server view

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands.

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

no snmp-server view *view-name*

Parameter

Parameter	Description
<i>view-name</i>	Updates or creates the label of a view.
<i>oid-tree</i>	Means the object IDs of the ASN.1 sub-tree that must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or

	a system sub-tree. The sub-tree name can be found in all MIB trees.
included excluded	Means the view type. The parameter "included" or "excluded" must be specified.

Default value

N/A

Command mode

Global configuration mode

Explanation

If other SNMP commands need a view as a parameter, you can use this command to create a view. By default, you need not define the view and you can see all the views, equivalent to Cisco-predefined everything views.

Example

The following example shows how to create the views of all objects in the MIB-II sub-tree.

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

The following example shows how to create the views of all objects, including those objects in the system group.

```
snmp-server view phred system included
```

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7 and interface 1.

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
```

Related command

snmp-server community

1.1.12 snmp-server source-addr

To specify a source address for answering all SNMP requests, run the second one of the following two commands in global configuration mode. To cancel this address, run the second one of the following commands.

```
snmp-server source-addr a.b.c.d
```

```
no snmp-server source-addr
```

Parameter

Parameter	Description
<i>a.b.c.d</i>	Means the source address for all SNMP requests to be answered.

Default value

The default source address is the nearest routing address.

Command mode

Global configuration mode

Explanation

When the SNMP server transmits an SNMP request, you can run this command to designate a special source address.

Example

The following example shows how to designate the IP address “1.2.3.4” of the designated interface as the source address of all SNMP packets.

```
snmp-server source-addr 1.2.3.4
```

Related command

N/A

1.1.13 snmp-server udp-port

To specify the port number for the SNMP agent to receive packets, run the following first command in global configuration mode.

snmp-server udp-port *portnum*

no snmp-server udp-port

Parameter

Parameter	Description
<i>udp-port</i>	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID.

Default value

It is the listening port of SNMP agent by default, that is, port 162.

Command mode

Global configuration mode

Explanation

The SNMP agent will listen to this port when SNMP server transmits SNMP packets.

Example

The following example shows how to specify the listening port of SNMP agent to port 1234.

```
snmp-server udp-port 1234
```

Related command

N/A

1.1.14 snmp-server encryption

TO display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run **snmp-server encryption** in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form.

snmp-server encryption**Parameter**

N/A

Default value

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.

Command mode

Global configuration mode

Explanation

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed.

Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

```
snmp-server encryption
```

Related command

snmp-server community

snmp-server user

1.1.15 snmp-server trap-add-hostname

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameter

None

Default value

Command mode

Global configuration mode

1.1.16 snmp-server trap-logs

snmp-server trap-logs

no snmp-server trap-logs

Parameter

The command has no parameters or keywords.

Command mode

Global configuration mode