Network Management Configuration Commands

Table of Contents

Chapter 1 Network Management Configuration

1.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server engine ID local
- snmp-server group
- snmp-server host/hostv6
- 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-sever 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 necode
- snmp-server event-id
- snmp-server getbulk-timeout
- snmp-server getbulk-delay
- show snmp
- debug snmp

1.1.1 snmp-server community

Syntax

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode. To delete the specified community character string, run the no form of this command.

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

no snmp-server community *string*

no snmp-server community

Parameters

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

Usage Guidelines

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

Syntax

To set the information about the contact person in a management node, run snmp-server contact text. To delete the contact information, use the no form of this command.

snmp-server contact *text*

no snmp-server contact

Parameters

Parameters	Description
text	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

Usage Guidelines

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 engineID local

Syntax

To configure the local agent SNMP engine ID, run the following command in the global configuration mode. To return to the default setting, use the no form of this command.

snmp-server engineID local *engineID*

no snmp-serverr engineID local *engineID*

Parameters

Parameters	Description
engineID	SNMP engine ID.

Default Value

SNMP engine ID is not set.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure the SNMP engine ID of the local agent.

Example

snmp-server engineID local 80000cf80300e00f3f56e3

1.1.4 snmp-server group

Syntax

To create or update a snmp-server group in global configuration mode, run the following first command; to cancel this SNMP group, run the following second command. Format of the command is as follows:

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

Parameters

Parameters	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

Usage Guidelines

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

1.1.5 snmp-server [host|hostv6]

Syntax

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*

Parameters

Parameters	Description
host|hostv6	Sets the IPv4 or IPv6 trap host.
host	Means the host's name or the address of the Internet. uses ipv4 address in host uses ipv6 address in hostv6
[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: non-authentication

community-string/user	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. If no command with any key word is entered, all traps with v1 standard are not sent by default.

Command Mode

Global configuration mode

Usage Guidelines

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

1.1.6 snmp-server location

Syntax

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

snmp-server location *text*

no snmp-server location

Parameters

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

Default Value

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

Command Mode

Global configuration mode

Usage Guidelines

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

1.1.7 snmp-server packetsize

Syntax

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

Parameters

Parameters	Description
byte-count	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes.

Default Value

3000 bytes

Command Mode

Global configuration mode

Usage Guidelines

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

1.1.8 snmp-server queue-length

Syntax

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

Parameters

Parameters	Description
length	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

Usage Guidelines

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

1.1.9 snmp-server trap-source

Syntax

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

Parameters

Parameters	Description
interface	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

Usage Guidelines

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

1.1.10 snmp-server trap-timeout

Syntax

To set the timeout value of retransmitting traps, run the following first command in global configuration mode. To return to the default setting, use the no form of this command.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameters

Parameters	Description
seconds	Means an interval for retransmitting traps, whose unit is second (1-1000).

Default Value

30 seconds

Command Mode

Global configuration mode

Usage Guidelines

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

1.1.11 snmp-server user

Syntax

To create or update an**snmp-server 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. Format of the command is as follows:

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

Parameters

Parameters	Description
username	Stands for the name of the created or modified SNMP user.
groupname	Stands for the group where the user is.
v3	Stands for the SNMP version.
[encrypted | auth]	Encryption type: **encrypted**: Encrypted: packet encryption **auth**: packet authentication
[md5 | sha]	Means the method of encryption authentication.
auth-password	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

None

Command Mode

Global configuration mode

Usage Guidelines

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 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 harsh algorithm.

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

Related Command

snmp-server view

snmp-server group

1.1.12 snmp-server view

Syntax

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*

Parameters

Parameters	Description
view-name	Updates or creates the label of a view.
oid-tree	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. Means the view type. The parameter "included" or "excluded" must be specified.
included | excluded	Means the view type. The parameter "included" or "excluded" must be specified.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

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. The command is used to define the object the view sees.

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(sysServices.7) and interface 1.

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

Related Command

snmp-server community

1.1.13 snmp-server source-addr

Syntax

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 interface, run the following second command.

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

no snmp-server source-addr

Parameters

Parameters	Description
a.b.c.d	Means the source address for all SNMP requests to be answered. Designate the source address of SNMP generating packets. The parameter is the IP address the device has set.

Default Value

The default source address is the nearest routing address.

Command Mode

Global configuration mode

Usage Guidelines

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

None

1.1.14 snmp-server udp-port

Syntax

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

Parameters

Parameters	Description
udp-port	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

Usage Guidelines

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

None

1.1.15 snmp-server encryption

Syntax

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. Format of the command is as follows:

snmp-server encryption

Parameters

None

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

Usage Guidelines

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

1.1.16 snmp-server trap-add-hostname

Syntax

To add the host name to the binding variable when SNMP sends traps, run the first one of the following two commands.

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameters

None

Default Value

The hostname is not added to the binding variable list when traps are being transmitted.

Command Mode

Global configuration mode

Usage Guidelines

This command is a great help in some cases when the NMS needs to locate which host sends these traps.

Example

The following example shows how to enable the trap-to-hostname binding function.

Router_config# snmp-server trap-add-hostname

1.1.17 snmp-server trap-logs

Syntax

To write the trap transmission records into logs, run the first one of the following two commands.

snmp-server trap-logs

no snmp-server trap-logs

Parameters

The command has no parameters or keywords.

Default Value

The transmitted traps are not recorded by default.

Command Mode

Global configuration mode

Usage Guidelines

After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device.

Example

The following example shows how to the trap logs function.

Router_config# snmp-server trap-logs

1.1.18 snmp-server set-snmp-dos-max

Syntax

To set the incorrect community login retry times in five minutes on the SNMP server, run the first one of the following two commands.

snmp-server set-snmp-dos-max *retry times*

no snmp-server set-snmp-dos-max

Parameters

The retry times parameter stands for the login times for a user to conduct the incorrect community login in five minutes.

Default Value

The incorrect community login times is not limited.

Command Mode

Global configuration mode

Usage Guidelines

This command can be used to prevent those SNMP host from guessing the device's community viciously, which lessening unnecessary CPU consumption of the device.

Example

The following example shows how to enable the refuse service function and set the max trying times to 10 in five minutes.

Router_config# snmp-server set-snmp-dos-max 10

1.1.19 snmp-server keep-alive

Syntax

To set the timely sending heartbeat trap, run **snmp-server keep-alive** in global configuration mode. The time interval is times.

snmp-server keep-alive *times*

no snmp-server keep-alive

Parameters

Parameters	Description
times	The time interval of heartbeat trap.

Default Value

The command is not configured by default.

Command Mode

Global configuration mode

Usage Guidelines

The command must be used with snmp-server host.

Example

The following example shows how to set the device sending heartbeat trap every 3 seconds.

snmp-server keep-alive 3

Related Command

snmp-server host

snmp-server hostv6

1.1.20 snmp-server necode

Syntax

To set the information about the management node (the unique identifier of the device), run snmp-server necode text. To delete the identifier information, use the no form of this command.

snmp-server necode *text*

no snmp-server necode

Parameters

Parameters	Description
text	Sets the information about the management node (the unique identifier of the device).

Default Value

The node identifier is not set.

Command Mode

Global configuration mode

Usage Guidelines

The command is corresponding to the snmp private MIB variable.

Example

The following example shows the information about the node.

snmp-server necode Dial_System_Operator_at_beeper_#_27345

1.1.21 snmp-server event-id

Syntax

To create and set event list, run command snmp-server event-id in the global configuration mode. To delete the event list, use the no form of this command.

snmp-server event-id *number* **trap-oid** *oid*

no snmp-server event-id *number* [**trap-oid** *oid*]

Parameters

Parameters	Description
number	The only identifier of event-id.
oid	trap OID included in event-id.

Default Value

The event list information is not set by default.

Command Mode

Global configuration mode

Usage Guidelines

The command is used in host configuration.

Example

The following example shows how to set trap whose trap OID is 1.2.3.4.5 to event ID 1.

snmp-server event-id 1 trap-oid 1.2.3.4.5

1.1.22 snmp-server getbulk-timeout

Syntax

To set the timeout of processing getbulk request, run command snmp-server getbulk-timeout in the global configuration mode. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly. To delete the configuration, use the no form of this command.

snmp-server getbulk-timeout *seconds*

no snmp-server getbulk-timeout

Parameters

Parameters	Description
seconds	The timeout of processing getbulk request.

Default Value

The timeout of processing getbulk request is not set by default.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set the timeout of processing getbulk request. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly.

Example

The following example shows how to set getbulk-timeout and set the timeout to 5 seconds.

snmp-server getbulk-timeout 5

1.1.23 snmp-server getbulk-delay

Syntax

To set getbulk-delay time to prevent snmp occupying excessive cpu when snmp agent processing getbulk request, run command snmp-server getbulk-delay in the global configuration mode. The unit is 0.01 seconds. To delete the configuration, use the no form of this command.

snmp-server getbulk-delay *ticks*

no snmp-server getbulk-delay

Parameters

Parameters	Description
ticks	Sets CPU interval time in processing getbulk request. The unit is 0.01s.

Default Value

The command is not configured when CPU is processing getbulk request in full load.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set getbulk-delay time to prevent snmp from occupying excessive cpu when snmp agent processing getbulk request. The unit is 0.01s.

Example

The following example shows how snmp agent pauses one ticks when getting one result in configuring getbulk.

snmp-server getbulk-delay 1

1.1.24 show snmp

Syntax

To monitor SNMP input and output statistics, including illegal community character strings, the number of errors and request variables, run command show snmp. To show SNMP engine information, run command show snmp engineID. To show SNMP trap host information, run command show snmp host. To show SNMP view information, run command **show snmp view**. To show snmp mibs registration information, run command **show snmp mibs**. To show snmp group information, run command show snmp group. To show SNMP user information, run command show snmp user.

show snmp [engineID |host | view | mibs |group|user]

Parameters

Parameters	Description
engineID	Shows SNMP engine information.
host	Shows SNMP trap host information.
View	Shows SNMP view information.
mibs	Shows SNMP MIB registration information.
group	Shows SNMP group information.
user	Shows SNMP user information.

Default Value

None

Command Mode

EXEC and global configuration mode

Usage Guidelines

The command **show snmp** is used to show SNMP input and output statistics.

To show SNMP engine information, run command show snmp engine ID.

The command **show snmp host** is used to show SNMP trap host information.

The command **show snmp view** is used to show SNMP view information.

The command **show snmp mibs** is used to show mib registration information.

The command **show snmp group** is used to show SNMP group information.

The command **show snmp user** is used to show SNMP user information.

Example

The following example shows how to list SNMP input and output statistics.

#**show snmp**
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Snmp 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 Get-response PDUs PDUs
13 SNMP trap PDUs

Meaning of statistics information of SNMP Agent receiving and sending packets:

Displayed Information	Meaning
Unknown community name	Unknown community name
Illegal operation for community name supplied	Illegal operation
Encoding errors	Encoding errors
Get-request PDUs	Get-request PDUs
Get-next PDUs	Get-next PDUs
Set-request PDUs	Set-request PDUs
Too big errors	The packets are too big to generate response packets.
No such name errors	No such name errors
Bad values errors	Bad values errors
General errors	General errors
Get-response PDUs	Get-response PDUs
Trap PDUs	SNMP trap packets

The following example shows how to show SNMP trap host information.

#show snmp host
Notification host: 192.2.2.1 udp-port: 162 type: trap
user: public security model: v1

The following example shows how to show SNMP view information.

#show snmp view
mib2 mib-2 - included permanent active

Related Command

snmp-server host

snmp-server view

1.1.25 debug snmp

Syntax

To show SNMP event, packet sending and receiving process and error information, run command **debug snmp.**

debug snmp [*error* | *event* | *packet*]

To stop showing the information, run command **no debug snmp.**

no debug snmp

Parameters

Parameters	Description
error	Enable the debug OLT of SNMP error information.
event	Enable the debug OLT of SNMP event information.
packet	Enable the debug OLT of SNMP input/output packets.

Command Mode

EXEC

Usage Guidelines

The command is used to enable SNMP debug information switch and output SNMP event, information of sending and receiving packets, which is helpful for SNMP fault diagnosis.

Example

The following example shows how to debug SNMP receiving and sending packets.

```
switch#debug snmp packet
Received 49 bytes from 192.168.0.29:1433
0000: 30 82 00 2D   02 01 00 04   06 70 75 62   6C 69 63 A0    0..-.....public.
0016: 82 00 1E 02   02 7D 01 02   01 00 02 01   00 30 82 00    .....}.......0..
0032: 10 30 82 00   0C 06 08 2B   06 01 02 01   01 03 00 05    .0.....+........
0048: 00                                                       .
Sending 52 bytes to 192.168.0.29:1433
0000: 30 82 00 30   02 01 00 04   06 70 75 62   6C 69 63 A2    0..0.....public.
0016: 82 00 21 02   02 7D 01 02   01 00 02 01   00 30 82 00    ..!..}.......0..
0032: 13 30 82 00   0F 06 08 2B   06 01 02 01   01 03 00 43    .0.....+.......C
0048: 03 00 F4 36                                              ...6
Received 51 bytes from 1192.168.0.29:1434
0000: 30 82 00 2F   02 01 00 04   06 70 75 62   6C 69 63 A0    0../.....public.
0016: 82 00 20 02   02 6B 84 02   01 00 02 01   00 30 82 00    .. ..k.......0..
0032: 12 30 82 00   0E 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 05 00                                                 ...
Sending 62 bytes to 192.168.0.29:1434
0000: 30 82 00 3A   02 01 00 04   06 70 75 62   6C 69 63 A2    0..:.....public.
0016: 82 00 2B 02   02 6B 84 02   01 00 02 01   00 30 82 00    ..+..k.......0..
0032: 1D 30 82 00   19 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 04 0B 45   74 68 65 72   6E 65 74 30   2F 31          ...Ethernet0/1
```

Domain	Description
Received	Stands for SNMP receiving packets
192.168.0.29	Stands for source IP address
1433	Stands for source address port number
51 bytes	Stands for the length of receiving packets
30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00	Stands for packets after SNMP ASN encoding

10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00	
0..-.....public. .....}.....0.. .0.....+..... .	Stands for ASCII character of receiving packets. "." means not in the range of ASCII character.
sending	SNMP sending packets
192.168.0.29	Stands for the destination IP address
1433	Stands for the source address port number
52 bytes	Stands for the length of sending and receiving packets
30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 03 00 F4 36	Stands for packets after SNMP ASN encoding
0..0.....public. ..!..}.....0.. .0.....+.....C ...6	Stands for ASCII character of sending and receiving packets. "." means not in the range of ASCII character.

The following example shows how to debug SNMP events.

```
switch#debug snmp event
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipReasmFails.0
  SNMP: Response
   >> ip.ipFragOKs.0 = 1
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipFragOKs.0
  SNMP: Response
   >> ip.ipFragFails.0 = 0
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipFragFails.0
  SNMP: Response
      >> ip.ipFragCreates.0 = 2
```

Domain	Description
SNMP	Stands for the current debug SNMP protocol.
GETNEXT request	SNMP getnext request
RESPONSE	SNMP response

--	Stands for receiving packets
>>	Transmitting packets
ip.ipReasmFails.0	Stands for MIB OID of access request
ip.ipFragOKs.0 = 1	Stands for being accessed MIB OID and the return value

1.2 RMON Configuration Commmands

RMON configuration commands include:

- rmon alarm
- rmon event
- rmon collection stat
- rmon collection history
- show rmon

1.2.1 rmon alarm

Syntax

To configure a rmon alarm entry, run the following command.

rmon alarm *index variable interval* {absolute | delta} rising-threshold *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [repeat] [owner *string*]

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
variable	Stands for the object needs to be monitored. Value range: oid of the monitored object.
interval	Stands for the sampling interval Value range: 1~ 2147483647
value	Stands for the alarm threshold Value range: -2147483648~ 2147483647.
eventnumber	Stands for the event index generated after reaching the threshold. Value range: 1~65535.
repeat	Stands for the repeat trigger event.
string	Stands for the owner description information Value range: the length of the character string is 1~31.

Default Value

eventnumber is not set by default.

repeat is not set by default.

Usage Guidelines

The command is used to monitor the value of specified object. The certain event will be triggered when the value exceeds the threshold.

Example

The following example shows how to set an alarm entry to monitor the object ifInOctets.2 and the sampling interval is 10. When the sampling interval increases more than15, the event 1 will be triggered. When the sampling interval decreases more than 25, the event 2 will be triggered.

rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2 repeat owner switch

1.2.2 rmon event

Syntax

To configure a rmon event entry, run the following command.

rmon event *index* [description *des-string*] [log] [owner *owner-string*] [trap *community*] [ifctrl *interface*]

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
des-string	Stands for the event description character string. Value range: 1~127.
owner-string	Stands for the owner character string. Value range: 1~31.
community	Stands for the community name when generating trap. Value range: 1~31.
interface	Stands for the shutdown port that the event controls.

Default Value

None

Usage Guidelines

The command is used to set a rmon event entry. It is used for alarm.

Example

The following example shows to set one rmon event entry to 6 and the description character string to example; add one item in the log entry when triggering the event and generates trap with public as the community name.

rmon event 6 log trap public description example owner switch

1.2.3 rmon collection stats

Syntax

To set rmon statistics function, run the following command.

rmon collection stats *index* [*owner string*]

Parameters

Parameters	Description
index	Stands for the index of the statistics entry. Value range: 1~65535.
string	Stands for the owner character string. Value range: the length of the character string is 1~31.

Default Value

None

Usage Guidelines

The command must be configured in the interface mode.

Example

The following example shows how to enable the statistics function on gigabit Ethernet interface g0/1.

int g0/1
rmon collection stats 2 owner switch

1.2.4 rmon collection history

Syntax

To configure a history control entry, run the following command.

rmon collection history *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]

Parameters

Parameters	Description
index	index Value range: 1-65535
bucket-number	The entry of all history record control entries nearest to the bucket-number need to be reserved. Value range: 1~65535.
second	Stands for the time interval. Value range: 1~3600.
owner-name	Stands for the owner character string. Value range: the length of the character string is 1~31.

Default Value

The default bucket-number is 50 and the default second is 1800.

Usage Guidelines

The command is used to configure in the interface mode. It is used for adding one entry to the history control table.

Example

The following example shows how to add the history control entry on the gigabit Ethernet interface g0/1 and save the statistics of latest 20 time intervals. (Each time interval is 10 seconds.)

int g0/1
rmon collection history 2 buckets 20 interval 10 owner switch

1.2.5 show rmon

Syntax

To show rmon configuration, run the following command.

show rmon [**alarm**] [**event**] [**statistics**] [**history**]

Parameters

None

Default Value

None

Usage Guidelines

The command is used to show rmon configuration.

Example

The following example shows how to show rmon configuration, run the following command.

show rmon