Network Management Configuration Commands

Оглавление

CHAPTER 1 NETWORK MANAGEMENT CONFIGURATION COMMANDS

1.1. SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server engineID local
- snmp-server group
- snmp-server host/hostv6
- snmp-server location
- snmp-server packetsize
- 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 encode
- snmp-server event-id
- 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.

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.
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*

snmp-server contact *text*

no snmp-server contact

Parameter

Parameter	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 SNMP engineID of the local agent, run the following command. To return to the default setting, use the no form of this command.

snmp-server engineID local *engineID*

no snmp-serverr engineID local *engineID*

Parameter

Parameter	Description
engineID	SNMP engine ID.

Default value

No setting.

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 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

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*

Parameter

Parameter	Description
host|hostv6	Sets the IPv4 or IPv6 host.

host	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 authenticatication
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.

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 location string, run the following second command.

snmp-server location *text*

no snmp-server location

Parameter

Parameter	Description
text	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.

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

Parameter

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

Default value

3000 byte.

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

Parameter

Parameter	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

Parameter

Parameter	Description
interface	Stands for the number of trap events which can be saved in the queue (1-1000).

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.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter

Parameter	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 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. The command format is as follows:

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

Parameter

Parameter	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: 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

N/A

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 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 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*

Parameter

Parameter	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.
included | excluded	Means the view type. The parameter “included” or “excluded” must be specified.

Default value

N/A

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.

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

1.1.13. 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 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

a.b.c.d	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.

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

N/A

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

Parameter

Parameter	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

N/A

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.

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.

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

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameter

None.

Default value

None.

Command mode

Global configuration mode.

1.1.17. snmp-server trap-logs

Syntax

snmp-server trap-logs

no snmp-server trap-logs

Parameter

The command has no parameters or keywords.

Command mode

Global configuration mode.

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

Parameter

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 set the maximum retry times in five minutes to **10**:

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

1.1.19. snmp-server keep-alive

Syntax

To set the interval for a device to send the heart-beat trap, run the first one of the following two commands in global mode.

snmp-server keep-alive *times*

no snmp-server keep-alive

Parameter

Parameter	Description
times	Stands for the interval of transmitting heart-beat traps.

Default value

This command does not exist in the default settings and the heart-beat traps are not sent.

Command Mode

Global configuration mode.

Usage guidelines

This command is used together with the **snmp-server host** command.

Example

The following example shows how to set the heart-beat traps to be transmitted 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 management node (unique device ID), run the first one of the following two commands in global mode.

snmp-server necode *text*

no snmp-server necode

Parameter

Parameter	Description
text	Stands for the information of the management node (unique device ID).

Default value

The management node is not set.

Command Mode

Global configuration mode.

Usage guidelines

It corresponds to the value of the private SNMP MIB variable.

Example

The following example shows how to set the information about a management node.

snmp-server necode Dial_System_Operator_at_beeper_#_27345

1.1.21. snmp-server event-id

Syntax

To create and set the event list, run the first one of the following two commands in global mode.

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

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

Parameter

Parameter	Description
number	Stands for the unique code of event ID.
oid	Stands for the trap OID which is contained by the event ID.

Default value

The event list is not set.

Command Mode

Global configuration mode.

Usage guidelines

It is used in the host configuration.

Example

The following example shows how to configure an event list by setting a trap OID from

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 maximum timeout time of GetBulk request, run the first one of the following two commands in global mode.

snmp-server getbulk-timeout *seconds*

no snmp-server getbulk-timeout

Parameter

Parameter	Description
seconds	Stands for the maximum timeout time for handling the GetBulk request.

Default value

The maximum timeout time for handling the GetBulk request is not set.

Command Mode

Global configuration mode.

Usage guidelines

This command is used to set the maximum timeout time of GetBulk request. If the system cannot handle over all GetBulk requests in this timeout time, the existing result will be directly returned.

Example

The following example shows how to set the GetBulk-timeout list and how to set the maximum timeout time to 5 seconds.

snmp-server getbulk-timeout 5

1.1.23. snmp-server getbulk-delay

Syntax

To prevent SNMP occupying too much CPU when the SNMP agent handles the getbulk requests, you need to set the getbulk delay by using the first one of the following two commands.

snmp-server getbulk-delay *ticks*

no snmp-server getbulk-delay

Parameter

Parameter	Description
ticks	Sets the CPU interval when GetBulk requests are handled.

Default value

When CPU handles the Getbulk requests in its full load, the CPU interval is not employed.

Command Mode

Global configuration mode

Usage guidelines

When the SNMP agent handles the Getbulk requests, SNMP may occupy too much CPU. In this case, you need to set the getbulk-delay.

Example

The following example shows how to set the getbulk-delay to **1**.

snmp-server getbulk-delay 1

1.1.24. show snmp

Syntax

To monitor SNMP output and input, run **show snmp**. To display the information of SNMP engine information, run **show snmp engineID.** To display the information about the SNMP trap host, run **show snmp host**. To display the SNMP views, run **show snmp view**. To display the MIB registration, run **show snmp mibs**. To display the SNMP groups, run **show snmp group**. To display the SNMP users, run **show snmp user**.

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

Parameter

Parameter	Description
engineID	Displays SNMP engine.
host	Displays the SNMP trap host.
View	Displays the SNMP views.
mibs	Displays the SNMP MIB registration.
group	Displays the SNMP groups.
user	Displays the SNMP users.

Default value

None.

Command Mode

EXEC or global configuration mode.

Usage guidelines

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

The show snmp engineID command is used to display the information about SNMP engine.

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

The **show snmp view** command is used to display the SNMP views.

The **show snmp mibs** command is used to display the MIB registration information.

The **show snmp group** command is used to display the SNMP groups.

The **show snmp user** command is used to display the SNMP users.

Example

The following example shows how to list out the SNMP output/input statistics.

Switch#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

The following list shows the meanings of all the domains in the above-mentioned information about the packets transmitted and received by the SNMP agent.

Displayed Information	Meaning
Unknown community name	Stands for an unidentifiable community name.

Illegal operation for community name supplied	Stands for illegal operations.
Encoding errors	Stands for the incorrect encode.
Get-request PDUs	Stands for the Get-Request packet.
Get-next PDUs	Stands for the Get-Next packet.
Set-request PDUs	Stands for the Set-Request packet.
Too big errors	Means that the related packet is too much to respond to.
No such name errors	Means that no designated instance exists.
Bad values errors	Means that the configured value type is wrong.
General errors	Means general errors.
Get-response PDUs	Stands for the Get-Response packets.
Trap PDUs	Stands for the SNMP trap packets.

The following example displays the SNMP trap host.

Switch#show snmp host

Notification host: 192.2.2.1 udp-port: 162 type: trap

user: public security model: v1

The following example displays the SNMP views.

Switch#show snmp view

mib2 mib-2 - included permanent active

Related Command

snmp-server host

snmp-server view

1.1.25. debug snmp

Syntax

To displays SNMP events, packet transmission/reception and packet errors, run the following command.

debug snmp [error | event | packet]

no debug snmp [error | event | packet]

Parameter

Parameter	Description
error	Enables the debugging switch of the SNMP event.
event	Enables the debugging switch of the SNMP events.
packet	Enables the debugging switch of SNMP input/output packets.

Command Mode

EXEC

Usage guidelines

After the SNMP debugging switch is enabled, the SNMP events, packet transmission and reception and errors are displayed, which will help users to diagnose SNMP troubles.

Example

The following example shows how to debug SNMP 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	SNMP received packets
192.168.0.29	Source IP address
1433	Port ID of the source address
51 bytes	Length of the received packet
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 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00	Packets encoded by SNMP ASN
0..-.....public. .....}.....0.. .0.....+..... .	ASCII code presentation of packet receptionThose out of the range of ASCII code presentation are shown as “.”.
sending	SNMP-transmitted packet
192.168.0.29	Destination IP address
1433	Port ID of the destination address
52 bytes	Length of the transmitted packet
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	Packets encoded by SNMP ASN

0..0.....public. ..!..}.....0.. .0.....+.....C ...6	ASCII code presentation of packet transmission Those out of the range of ASCII code presentation are shown as “.”.

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	Currently debugged SNMP
GETNEXT request	SNMP GetNext request
RESPONSE	SNMP response
--	Received packet
>>	Transmitted packet
ip.ipReasmFails.0	MIB OID that is accessed by the request

ip.ipFragOKs.0 = 1	Accessed MIB OID and its return value

1.2. RMON Configuration Commands

Configuration commands include:

- rmon alarm
- rmon event
- show rmon

1.2.1. rmon alarm

Syntax

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

To configure an RMON alarm entry, run the above-mentioned command.

Parameter

Parameter	Description
index	Means the index of event entries. Value range: 1-65535
variable	Means those to-be-monitored objects. Value range: OID of the tested object
interval	Means the sampling interval. Range: 1-2147483647 seconds
value	Means the alarm threshold. Range: minus 2147483648-2147483647
eventnumber	Means the event index which is triggered when the threshold is reached. Range: 1-65535
repeat	Means those events that are allowed to be triggered repeatedly.
string	Means the description of the holder. Value range: 1-31

Default value

Eventnumber is not set by default.

repeat is not set by default.

Usage guidelines

This command is configured in global mode and it is used to monitor the value of a designated object. If the value surpasses the threshold, the designated event will be triggered.

Example

The following example shows that an alarm entry is set, the monitored object is **ifInOctets.2**, the sampling interval is 10, event 1 is triggered when the value excesses 15, and event 2 is triggered when the value declines more than 25.

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 collection stats

Syntax

To set rmon statistics function, run the following command.

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

Parameters

Parameter	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

1.2.3. 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

Parameter	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

1.2.4. rmon event

Syntax

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

To configure an RMON event entry, run the above-mentioned command.

Parameter

Parameter	Description
index	Means the index of event entries. Value range: 1-65535.

des-string	Stands for the character string of event's description. Value range: 1-127.
owner-string	Means the character string of the holder. Value range: 1-31.
community	Means the community name during trap generation. Value range: 1-31.
interface	Designates a shutdown port that the event needs to control.

Default value

None.

Usage guidelines

This command is used to set an RMON event entry, which is used for alarming.

Example

The following example shows that an RMON event is set. The index of this RMON event is 6, the character string of its description is **example**, and when an event is triggered, an entry will be added to the log list and also a trap whose community name is **public** is generated.

rmon event 6 log trap public description example owner switch

1.2.5. show rmon

Syntax

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

To display RMON configuration, run the above-mentioned command.

Parameter

None.

Default value

None.

Usage guidelines

This command is used to display RMON configuration.

Example

The following example shows how to display RMON configuration.

show rmon