Chapter 3:Network Management Configuration

Chapter 1 Network Management Configuration

1.1 Configuring SNMP

1.1.1 Overview

The SNMP system includes the following parts:

- SNMP management side (NMS)
- SNMP agent (AGENT)
- Management information base (MIB)

SNMP is a protocol working on the application layer. It provides the packet format between SNMP management side and agent.

SNMP management side can be part of the network management system (NMS, like CiscoWorks). Agent and MIB are stored on the system. You need to define the relationship between network management side and agent before configuring SNMP on the system.

SNMP agent contains MIB variables.SNMP management side can check or modify value of these variables. The management side can get the variable value from agent or stores the variable value to agent. The agent collects data from MIB. MIB is the database of device parameter and network data. The agent also can respond to the loading of the management side or the request to configure data. SNMP agent can send trap to the management side. Trap sends alarm information to NMS indicating a certain condition of the network. Trap can point out improper user authentication, restart, link layer state (enable or disable), close of TCP connection, lose of the connection to adjacent systems or other important events.

1. SNMP notification

When some special events occur, the system will send ‘inform’ to SNMP management side. For example, when the agent system detects an abnormal condition, it will send information to the management side.

SNMP notification can be treated as trap or inform request to send. Since the receiving side doesn’t send any reply when receiving a trap, this leads to the receiving side cannot be sure that the trap has been received. Therefore the trap is not reliable. In comparison, SNMP management side that receives “inform request” uses PDU that SNMP echoes as the reply for this information. If no “inform request” is received on the management side, no echo will be sent. If the receiving side doesn’t send any reply, then you can resend the “inform request”. Then notifications can reach their destination.

Since inform requests are more reliable, they consume more resources of the system and network. The trap will be discarded when it is sent. The “inform request” has to be stored in the memory until the echo is received or the request timeouts. In addition, the trap is sent only once, while the “inform request” can be resent for many times. Resending "inform request" adds to network communications and causes more load on

network. Therefore, trap and inform request provide balance between reliability and resource. If SNMP management side needs receiving every notification greatly, then the “inform request” can be used. If you give priority to the communication amount of the network and there is no need to receive every notification, then trap can be used.

This OLT only supports trap, but we provide the extension for "inform request". 2.

SNMP Version

System of our company supports the following SNMP versions:

- SNMPv1---simple network management protocol, a complete Internet standard, which is defined in RFC1157.
- SNMPv2C--- Group-based Management framework of SNMPv2, Internet test protocol, which is defined in RFC1901.

Layer 3 switch of our company also supports the following SNMP:

- SNMPv3--- a simple network management protocol version 3, which is defined inRFC3410.

SNMPv1 uses group-based security format. Use IP address access control list and password to define the management side group that can access to agent MIB.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are:

- Message integrity — Ensuring that a packet has not been tampered with in-transit.
- Authentication — Determining the message is from a valid source.
- Encryption — Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. SNMPv3 supports three security levels based on the user's security model, that is (from high to low), authentication and encryption, authentication and no encryption, no authentication. With MD5 or SHA hash algorithm, the password will not be revealed. With DES encryption, the device will not be wiretapped by a third party. To realize identity authentication of the device, you need to configure user/password pair and the group belongs to the user. To determine the access permission to the management information database, you need to configure group and view. Meanwhile, the group limits the lowest security level of users in the group.

You need to configure SNMP agent to the SNMP version that the management working station supports. The agent can communicate with many management sides.

3. Supported MIB

SNMP of our system supports all MIBII variables (which will be discussed in RFC 1213) and SNMP traps (which will be discussed in RFC 1215).

Our system provides its own MIB extension for each system.

1.1.2 SNMP Configuration Tasks

SNMP Configuration Tasks include:

- Configuring SNMP view
- Creating or modifying the access control for SNMP community
- Configuring the contact method of system administrator and the system's location
- Defining the maximum length of SNMP agent data packet
- Monitoring SNMP state
- Configurig SNMP local engine
- Configuring SNMP trap
- Configuring SNMPv3 group
- Configuring SNMPv3 user
- Configuring snmp-server encryption
- Configuring snmp-server trap-source
- Configuring snmp-server trap-timeout
- Configuring snmp-server trap-add-hostname
- Configuring snmp-server trap-logs
- Configuring snmp -dos-max retry times
- Configuring keep-alive times
- Configuring snmp-server necode
- Configuring snmp-server event-id
- Configuring snmp-server getbulk-timeout
- Configuring snmp-server getbulk-delay
- Showing snmp running information
- Showing snmp debug information

1. Configuring SNMP view

The SNMP view is to regulate the access rights (include or exclude) for MIB. Use the following command to configure the SNMP view.

Command	Usage Guidelines
snmp-server view *name oid* [**excluded** | **included**]	Adds the subtree or table of OID-specified MIB to the name of the SNMP view, and specifies the access right of the object identifier in the name of the SNMB view.

The subsets that can be accessed in the SNMP view are the remaining objects that "include" MIB objects are divided by "exclude" objects. The objects that are not configured are not accessible by default.

After configuring the SNMP view, you can implement SNMP view to the configuration of the SNMP group name, limiting the subsets of the objects that the group name can access.

2. Creating or modifying the access control for SNMP community

You can use the SNMP community character string to define the relationship between SNMP management side and agent. The community character string is similar to the password that enables the access system to log in to the agent. You can specify one or multiple properties relevant with the community character string. These properties are optional:

Allowing to use the community character string to obtain the access list of the IP address at the SNMP management side

Defining MIB views of all MIB object subsets that can access the specified community

Specifying the community with the right to read and write the accessible MIB objects

Configure the community character string in global configuration mode using the following command:

Command	Purpose
snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]	Defines the group access character string.

You can configure one or multiple group character strings. Run command "no snmp-server community" to remove the specified community character string.

For how to configure the community character string, refer to the part "SNMP Commands".

3. Configuring the contact method of system administrator and the system's location

SysContact and sysLocation are the management variables in the MIB's system group, respectively defining the linkman's identifer and actual location of the controlled node.

These information can be accessed through config. files. Run the following commands in global configuration mode:

Command	Purpose
snmp-server contact *text*	Sets the character string for the linkman of the node.
snmp-server location *text*	Sets character string for the node th e location.

4. Defining the maximum length of SNMP agent data packet

When SNMP agent receives requests or sends response, you can configure the maximum length of the data packet. Run the following commands in global configuration mode:

Command	Purpose
snmp-server packetsize *byte-count*	Sets the maximum length of the data packet.

5. Monitoring SNMP state

You can run the following command in global configuration mode to monitor SNMP output/input statistics, including illegal community character string items, number of mistakes and request variables.

Command	Purpose
show snmp	Monitoring SNMP state

6. Configurig SNMP local engine

Run the following command in the global mode to configure SNMP local engine.

Command	Purpose
snmp-server engineID local *engineID*	Configurig SNMP local engine

7. Configuring SNMP trap

Use the following command to configure the system to send the SNMP traps (the second task is optional):

- Configuring the system to send trap

  Run the following commands in global configuration mode to configure the system to send trap to a host.

Command	Purpose
snmp-server host|hostv6 host community-string [trap-type]	Specifies the receiver of the trap message.

snmp-server host|hostv6 *host* **[udp-port** *port-num***] [permit|deny** *event-id***] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**	Specifies the receiver, version number and username of the trap message.

When the system is started, the SNMP agent will automatically run. All types of traps are activated. You can use the command snmp-server host to specify which host will receive which kind of trap.

Some traps need to be controlled through other commands. For example, if you want SNMP link traps to be sent when an interface is opened or closed, you need to run snmp trap link-status in interface configuration mode to activate link traps. To close these traps, run the interface configuration command snmp trap link-stat.

You have to configure the command snmp-server host for the host to receive the traps.

- Modifying the running parameter of the trap

  As an optional item, it can specify the source interface where traps originate, queue length of message or value of resending interval for each host.

  To modify the running parameters of traps, you can run the following optional commands in global configuration mode.

Command	Purpose
snmp-server trap-source *interface*	Specifies the source interface where traps originate and sets the source IP address for the message. The command sets the source IP address for the information.
snmp-server queue-length *length*	Creates the queue length of the message for each host that has traps. The default value is 10.
snmp-server trap-timeout *seconds*	Defines the frequency to resend traps in the resending queue. The default value is 30 seconds.

8. Configuring the SNMP binding source address

Run the following command in the global configuration mode to set the source address for the SNMP message.

Command	Purpose
snmp source-addr *ipaddress*	Set the source for the SNMP address message.

9. Configuring snmp-server udp-port

Run the following command in the global mode to configure snmp-server udp-port.

Command	Purpose
snmp-server udp-port *portnum*	Set SNMP server udp-port number

10. Configuring SNMPv3 group

Configuring SNMPv3 group

Command	Purpose
snmp-server group [*groupname* { **v3** [**auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]	Configuring SNMPv3 group You can only read all items in the subtree of the Internet by default.

11. ConfiguringSNMPv3 user

You can run the following command to configure a local user. When an administrator logs in to a device, he has to use the username and password that are configured on the device. The security level of a user must be higher than or equals to that of the group which the user belongs to. Otherwise, the user cannot pass authentication.

Command	Purpose
snmp-server user *username groupname* **{v3 [encrypted|auth] [md5|sha]** *auth-password***}**	Configures a local SNMPv3 user.

12. Configuring 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. Format of the command is as follows:

Command	Purpose
snmp-server encryption	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.

13. Configuring 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.

Command	Purpose
snmp-server trap-source *interface*	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.

14. Configuring snmp-server trap-timeout

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

Command	Purpose

snmp-server trap-timeout *seconds*	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.

15. Configuring snmp-server trap-add-hostname

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

Command	Purpose
snmp-server trap-add-hostname	This command is a great help in some cases when the NMS needs to locate which host sends these traps.

16. Configuring snmp-server trap-logs

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

Command	Purpose
snmp-server trap-logs	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.

17. Configuring snmp -dos-max retry times

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

Command	Purpose
snmp-server set-snmp-dos-max *retry times*	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.

The command must be used with snmp-server host.

18. Configuring keep-alive times

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

Command	Purpose

snmp-server keep-alive *times*	Send keep-alive times regularly to the trap host.

19. Configuring snmp-server necode

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.

Command	Purpose
snmp-server necode *text*	The command is corresponding to the snmp private MIB variable.

20. Configuring snmp-server event-id

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.

Command	Purpose
snmp-server event-id *number* **trap-oid** *oid*	The command is used to forward the filter when sending trap in configuring host.

21. Configuring snmp-server getbulk-timeout

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.

Command	Purpose
snmp-server getbulk-timeout *seconds*	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.

22. Configuring snmp-server getbulk-delay

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.

Command	Purpose
snmp-server getbulk-delay *ticks*	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.

23. Showing snmp running information

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.

Command	Purpose
show snmp engineID	Shows SNMP engine information.
show snmp *host*	Shows SNMP trap host information.
show snmp view	Shows SNMP view information.
show snmp mibs	Shows SNMP MIB registration information.
show snmp group	Shows SNMP group information.
show snmp user	Shows SNMP user information.

24. Showing snmp debug information

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

Command	Purpose
debug snmp error	Enable the debug OLT of SNMP error information.
debug snmp event	Enable the debug OLT of SNMP event information.
debug snmp packet	Enable the debug OLT of SNMP input/output packets.

1.1.3Configuration Example

1. Example 1

```
snmp-server community public RO snmp-
server community private RW snmp-server
host 192.168.10.2 public
```

The above example shows: how to set the community string public that can only read all MIB variables. how to set the community string private that can read and write all MIB variables. The above command specifies the community string public to send traps to 192.168.10.2 when a system requires to send traps. For example, when a port of a system is in the down state, the system will send a linkdown trap information to 192.168.10.2.

2. Example 2

```
snmp-server group getter v3 auth snmp-server group setter v3 priv
write v-write snmp-server user get-user getter v3 auth sha
12345678 snmp-server user set-user setter v3 encrypted auth md5
12345678 snmp-server view v-write internet included
```

The above example shows how to use SNMPv3 to manage devices. Group getter can browse device information, while group setter can set devices. User get-user belongs to group getter while user set-user belongs to group setter. For user get-user, its security level is authenticate but not encrypt, its password is 12345678, and it uses the sha arithmetic to summarize the password.

1.2RMON Configuration

1.2.1 RMON Configuration Tasks

RMON configuration tasks include:

- Configuring the rMon alarm function for the switch
- Configuring the rMon event function for the switch
- Configuring the rMon statistics function for the switch
- Configuring the rMon history function for the switch
- Displaying the rMon configuration of the switch

1. Configuring the rMon alarm function for the switch

You can configure the rMon alarm function through the command line or SNMP NMS. If you configure through SNMP NMS, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistic value in the system. The following table shows how to set the rMon alarm function:

Command	Purpose
Config	Enters the global configuration mode.
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] **[repeat]**	Add a rMon alarm item. index is the index of the alarm item. Its effective range is from 1 to 65535. variable is the object in the monitored MIB. It must be an effective MIB object in the system. Only objects in the Integer, Counter, Gauge or TimeTicks type can be detected. interval is the time section for sampling. Its unit is second. Its effective value is from 1 to 2147483647. absolute is used to directly monitor the value of MIB object. delta is used to monitor the value change of the MIB objects between two sampling. value is the threshold value when an alarm is generated. Event number is the index of an event that is generated when a threshold is reached. Event number is optional. Owner string is to describe the information about the alarm.
	Repeat is to repeat trigger event.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

After a rMon alarm item is configured, the device will obtain the value of variable-specified oid after an interval. The obtained value will be compared with the previous value according to the alrm type (absolute or delta). If the obtained value is bigger than the previous value and surpasses the threshold value specified by rising-threshold, an event whose index is eventnumber (If the value of eventnumber is 0 or the event whose index is eventnumber does not exist in the event table, the event will not occur). If the variable-specified oid cannot be obtained, the state of the alarm item in this line is set to invalid. If you run rmon alarm many times to configure alarm items with the same index, only the last configuration is effective. You can run no rmon alarm index to cancel alarm items whose indexes are index.

2. Configuring the rMon event function for the switch

The steps to configure the rMon event are shown in the following table:

Procedure	Command	Purpose
1.	**config**	Enters the global configuration mode.
2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community] [**ifctrl** *interface*]	Add a rMon event item. index is the index of the alarm item. Its effective range is from 1 to 65535. description means the information about the event. log means to add a piece of information to the log table when a event is triggered. trap means a trap message is generated when the event is triggered. community means the name of a community. ifctrl interface is the interface controlling event shutdown. owner string is to describe the information about the alarm.
3.	**exit**	Goes back to the EXEC mode.
4.	**write**	Saves the settings.

After a rMon event is configured, you must set the domain eventLastTimeSent of the rMon event item to sysUpTime when a rMon alarm is triggered. If the log attribute is set to the rMon event, a message is added to the log table. If the trap attribute is set to the rMon event, a trap message is sent out in name of community. If you run rmon event many times to configure event items with the same index, only the last configuration is effective. You can run no rmon event index to cancel event items whose indexes are index.

3. Configuring the rMon statistics function for the switch

The rMon statistics group is used to monitor the statistics information on every port of the device. The steps to configure the rMon statistics are as follows:

Procedure	Command	Purpose
1.	**config**	Enters the global configuration mode.
2.	**interface iftype ifid**	This command is used to enter the interface configuration mode. iftype means the type of the port. ifid means the ID of the interface.
3.	**rmon collection stats index** [**owner** *string*]	Enable the statistics function on the port. index means the index of the statistics. owner string is to describe the information about the statistics.
4.	**exit**	Goes back to the global mode.
5.	**exit**	Goes back to the EXEC mode.
6.	**write**	Saves the settings.

If you run rmon event many times to configure status items with the same index, only the last configuration is effective. You can run no rmon event index to cancel event items whose indexes are index.

4. ConfiguringRMONhistoryfor switch

TheRMONhistory group is used to collect statistics information of different time sections on a port in a device. The steps to configure the rMon statistics are as follows:

Procedure	Command	Purpose
1.	**config**	Enters the global configuration mode.
2.	**interface** iftype ifid	Enters the port mode. iftype means the type of the port. ifid means the ID of the interface.
3.	**rmon history llection index** [buckets bucket-number] [interval second] owner- [owner name]	Enable the history function on the port. index means the index of the history. In statistics of all history record control entries, the entry nearest to bucket-number needs to be saved. The user can browse the Ethernet history record to obtain the statistics. The default value is 50 entries. The interval means the time between two data collection, whose default value is 1800s (half hours). owner string is to describe the information about the description information in the history control table.

4.	**exit**	Goes back to the global mode.
5.	**exit**	Goes back to the EXEC mode.
6.	**write**	Saving the Settings

After a rMon history item is added, the device will obtain statistics values from the specified port every second. The statistics value will be added to the history item as a piece of information. If you run rmon collection history index many times to configure history items with the same index, only the last configuration is effective. You can run no rmon history index to cancel history items whose indexes are index. Note:Too much system sources will be occupied in the case the value of bucket-number is too big or the value of interval second is too small.

5. DisplayingRMONconfiguration of switch

Run show to display theRMONconfiguration of the switch.

Command	Purpose
show rmon [alarm] [event] [statistics] [history]	Displays the rmon configuration information. alarm means to display the configuration of the alarm item. event means to show the configuration of the event item and to show the items that are generated by the occurrence of events and are contained in the log table. statistics means to display the configuration of the statistics item and statistics values that the device collects from the port. history means to display the configuration of the history item and statistics values that the device collects in the latest specified intervals from the port.