Network Management Configuration

Table of Contents

Chapter 1 Network Management Configuration

1.1 SNMP Configuration

1.1.1 Overview

The SNMP system includes the following 3 parts:

- SNMP management server (NMS)
- SNMP agent (agent)
- MIB

SNMP is a protocol for the application layer. It provides the format for the packets which are transmitted between NMS and agent.

SNMP management server is a part of the network management system, such as CiscoWorks. The agent and MIB are in the system. If you want to set SNMP on the system, you need to define the relationship between the SNMP management server and the agent.

SNMP agent includes the MIB variable and the SNMP management server can be used to browse or change these variables' values. The management server can get the values from the agent or save these variables in the agent. The agent collects data from MIB. MIB is the database of equipment parameters and network data. The agent can also respond to the reading request or data setting request of the SNMP management server. The SNMP agent can transmit traps to the SNMP management server positively. A trap is an alarm sent to the SNMP management server for a network event. A trap records incorrect user authentication, rebooting, link state (enabled or disabled), TCP link shutdown, loss of connection with neighboring system, or other important events.

1. SNMP Notification

When a special event occurs, the system will send an inform to the SNMP management server. For example, when the agent system runs into a incorrect condition, it will send a message to the management server.

The SNMP notification can be sent as a trap or a inform request. Because the receiver receives a trap and does not send any response, the transmitter hence cannot confirm whether the trap is received. In this way, the trap is unreliable. Comparatively, the SNMP management server uses SNMP to respond PDU, which is acted as a response of this message. If the management server does not receive the inform request, it will not transmit a response. If the transmitter does not receives the response, it will transmit the inform request again. In this way, the inform has more chance to arrive the planned destination.

The more reliable the notification requests are, the more resources of system and network they cost. The traps are dropped when being sent out. The different point is that the notification request must be saved in the memory until the response is received or the request times out.

Additionally, a trap is sent only once and a notification request can be transmitted for many times. Re-transmitting requests increases the network communication traffic and generates more load on the network. Hence, trap and notification request provide a balance between reliability and resource If the SNMP management server badly needs to receive each notification, the notification request can be used; if you care about the network traffic or the system's memory and regard it unnecessary to receive every notification, you can use traps.

Our system supports traps currently and at the same time expands the notification requests.

2. SNMP Version

Our system supports the following SNMP versions:

- SNMPv1: it is a simple network management protocol and a sound Internet standard, which is defined in RFC1157.
- SNMPv2C: it is a group-based management protocol and a Internet trial protocol, which is defined in RFC1901.

Our system supports the following SNMP versions:

- SNMPv3 。

SNMPv1 adopts the group-based security mode. The management group, which can access the proxy MIB, is defined via IP ACL and password.

You must set on the SNMP agent the SNMP version which is supported by the management workstation. The SNMP agent can communicate with multiple management terminals.

3. Supported MIB

The SNMP in our system supports all MIB II variables (told in RFC1213) and the SNMP traps (described in RFC1215).

We provide each system with its own MIB expansion.

1.1.2 SNMP Configuration Tasks

SNMP configuration tasks are listed below:

- Setting SNMP Views
- Creating or Changing the Access Control for SNMP Communities
- Setting the Contact Way and the System Location for System Administrator
- Defining the Maximum Length of SNMP Agent Packets
- Monitoring the SNMP State
- Setting SNMP Traps

1. Setting SNMP Views

The Snmp view is used to regulate the MIB access permission: access permitted or access denied. You can run the following command to set the SNMP view.

Command	Remarks
snmp-server view *name oid*] [exclude | include]	Adds the OID-designated MIB leaf or the list to the name of the SNMP view and designates the access permission of the object identifier in the name of the SNMP view.

After the SNMP view is configured, you can apply it into the configuration of SNMP community name to limit the subset of the accessible objects of this community name.

2. Creating or Changing the Access Control for SNMP Communities

The relationship between the SNMP control terminal and its proxy is defined by the SNMP community's character string. The community character string is similar with the password which allows to access the proxy on the system. As an option you can designate one or multiple features related with the community character string.

Run the following commands in global mode to configure the community character string:

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

One or multiple community character strings can be set. You can run **no snmp-server community** to delete the given community character string.

3. Setting the Contact Way and the System Location for System Administrator

sysContact and **sysLocation** are both the management variables in the system group of MIB, which define the contact person ID of managed node and the actual location respectively. These information can be accessed through the configuration files. Run the following commands in global mode:

Command	Purpose
snmp-server contact *text*	Sets the character string of the node contact person.
snmp-server location *text*	Sets the character string of the node location.

4. Defining the Maximum Length of SNMP Agent Packets

When the SNMP agent receives requests or transmits responses, the maximum length of the packet can be set. Run the following commands in global configuration mode:

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

5. Monitoring the SNMP State

To monitor SNMP output/input statistics, including those entries with illegal community character strings and the quantity of errors and request variables, run the following command in global mode.

Command	Purpose
show snmp	Monitoring the SNMP State

6. Setting SNMP Traps

Use the following command to make the system transmit SNMP traps (the second task is optional):

- Configuring the system to transmit traps

  Run the following command in global mode to enable the system to transmit traps to a host.

Command	Purpose
snmp-server host host community-string [trap-type]	Designates the receiver of the traps.

After the system is opened, the SNMP proxy automatically starts and all types of traps are activated. You can run **snmp-server host** to designate which host to receive which type of traps.

Some traps need be controlled through other commands. For example, if you want the SNMP link traps to be transmitted when an interface is opened or closed, you need to run **snmp trap link-status** in port configuration mode to activate the link traps.

- Modifying the trap running parameters

  As an option, you can designate the trap's source interface, the queue's length for each host, or the retransmission interval.

  Run the following commands in global mode to modify the trap running parameters:

Command	Purpose
snmp-server trap-source *interface*	Designates the source interface where traps are generated. This command can also be used to set the source IP address.
snmp-server queue-length *length*	Establishes the queue's length for each host. The default value is 10.
snmp-server trap-timeout *seconds*	Defines the trap retransmission frequency for the retransmission queue. The default value is 30 second.

1.1.3 Configuration Example

1. Example 1

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

2. Example 2

```
snmp-server community public view sysmib RO
snmp-server community private RW nativehost
snmp-server contact switch@company.com.cn
snmp-server host 192.168.10.2 public snmp
snmp-server location 405-room
snmp-server view sysmib system included
ip access-list standard nativehost
permit 192.168.10.2 255.255.255.255
```

1.2 Configuring RMON

1.2.1 RMON Configuration Tasks