https://community.fs.com/blog/understanding-snmp.html

Understanding SNMP

SNMP (Simple Network Management Protocol) is an application-layer protocol that contains three versions, including SNMPv1, SNMPv2c and SNMPv3. All the versions provide a standardized framework and a common language for monitoring and managing devices in a network. Devices that support SNMP include network switches, routers, printers and so on. Those devices are produced by different vendors and their management interfaces (such as CLI) vary greatly, which makes network management more complicated. SNMP is designed to solve the problem. It provides a unified interface to implement unified management on different devices from different vendors, which greatly simplify the whole network management.

How SNMP Works?

To understand SNMP working principles, it’s important to know SNMP management model first.

SNMP Components

There are four main components of an SNMP management model, including NMS (network management system), SMMP agent, MIB (management information base) and managed object. Each managed device includes agent access, MIB, and several management objects.

NMS acts as a manager on a network, and it may be a computer or server that running some kind of SNMP software to monitor and manage network devices.

Agent is a process that runs on a managed device to receive the request from NMS and then return the answers to the NMS.

MIB refers to a data base that contains the variables that the managed device maintains (information could be query and set by agent).

Management object is an object that will be managed. It could be a hardware component (like an interface board) or parameters configured for the hardware or software (like a route selection protocol).

The NMS interacts with the agent on a managed device. After the NMS sends a command to the agent, the agent will perform operations on the MIB in the managed device. Figure 2 shows SNMP model.

SNMP Working Principles

Here uses SNMPv2c to explain SNMP working principles. It performs the following operations to retrieve data, modify SNMP object variables and send notifications.

Get

It’s a request sent by the NMS to the managed device. And it’s performed to retrieve one or more values from the MIB.

GetNext

It’s similar to the GET. But it usually retrieves the value of the next OID (Object Identifier) in the MIB tree. It’s used to retrieve a mass of data from large MIB table.

GetBulk

It’s used to retrieve a mass of data from large MIB table.

Set

It’s performed by the NMS to modify the value of the managed device.

It’s performed by the agent in response to the GetRequest, GetNextRequest, GetBulkRequest and SetRequest operations.

Response

It’s performed by the agent in response to the GetRequest, GetNextRequest, GetBulkRequest and SetRequest operations.

Trap

This operation is initiated by the agent. It’s used to notify the NMS of a fault or event occurring on a managed device.

Inform

This operation is initiated by the agent. It’s similar to the TRAP, but after the agent sends an inform request, the NMS must send an InformResponse packet as a response to the agent.

Note that, SNMPv1 does not support GetBulk and Inform operations.

Figure 2 shows the Get/GetNext/GetBulk/Set process of SNMPv2c application.

When NMS sends a Get/GetNext/GetBulk/Set request packet to the agent, the agent authenticates the SNMP version and community name first. Then the agent sends the corresponding value as a response packet to the NMS when the authentication is successful. If the agent fails to obtain the corresponding value, it returns an error message to the NMS. Note that, the GetBulk operation is equal to consecutive GetNext operations. Users can set the numbers of GetNext operations that are included in one GetBulk operation, without the need for repeated GetNext operations.

Figure 3 shows the Trap/Inform process of SNMPv2c application.

Trap and Inform are spontaneous activities of the managed device. When a trap triggering condition occurs, the managed device sends a trap to the NMS for notification. Inform is similar to the Trap, but the Inform requires a confirmation from the NMS while the Trap does not. If the managed device doesn’t receive the confirmation, it saves the Inform in the buffer or repeats the Inform operation until the NMS returns a confirmation. Once the number of repeated sending reaches the maximum limit, the managed device will record a log for the Inform request.

Common FAQs and Solutions

1. How to Configure SNMP?

SNMP uses a central computer with SNMP software installed to manage network switches. Nowadays, most network switches on the market, no matter they are Gigabit switch or 40G switch, all support SNMP that provides a unified and easy way to manage those switches. Take SNMPv2c configuration as an example, the process includes:

A) Configure IP address on the computer and the managed switches.

B) Enable SNMP.

C) Configure the access rights to enable the computer to manage the specified switches.

D) Verify the configuration result.

More details about SNMP configuration, please visit SNMP Configuration on FS 3900 Series Switches.

2. NMS Failed to Receive Trap.

In the default configuration, not all Trap are enabled. In system view, users can:

view the feature list that has enabled Trap by show snmp-agent trap all

Open the corresponding Trap by snmp-agent trap enable feature-name

Open all the Trap by snmp-agent trap enable

3. SNMPv1 vs SNMPv2c vs SNMPv3, What Are the Differences?

SNMPv1 SNMPv2c SNMPv3

Access control Based on the community names and MIB view Based on the community names and MIB view Access control based on the user, user group, and MIB view

Authentication and privacy Based on the community name Based on the community name Authentication mode: MD5/SHA Encryption mode: DES56/AES128/AES192/AES256/3DES

Trap Support Support Support

Inform Not Support Support Support

GetBulk Not Support Support Support

Application Suitable for small networks with low security requirements Suitable for SMB and larger networks, with low security requirements Suitable for large and super-giant enterprises with strict security requirement