SNMP

TEXT

Introduction to SNMP

Now that your network is mapped and all of your components are using the same clock, it is time to look at how you can manage your network by using Simple Network Management Protocol (SNMP).

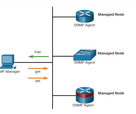
SNMP was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements:

- SNMP manager
- SNMP agents (managed node)
- Management Information Base (MIB)

To configure SNMP on a networking device, it is first necessary to define the relationship between the manager and the agent.

The SNMP manager is part of a network management system (NMS). The SNMP manager runs SNMP management software. As shown in the figure, the SNMP manager can collect information from SNMP agents by using the "get" action and can change configurations on an agent by using the "set" action. In addition, SNMP agents can forward information directly to a network manager by using "traps".



The SNMP agent and MIB reside on SNMP client devices. Network devices that must be managed, such as switches, routers, servers, firewalls, and workstations, are equipped with an SNMP agent software module. MIBs store data about the device and operational statistics and make it available to authenticated remote users. The SNMP agent is responsible for providing access to the local MIB.

Detailed device management information is provided to a management station or management applications. The SNMP manager polls the agents and queries the MIB for SNMP agents on UDP port 161. SNMP agents send any SNMP traps to the SNMP manager on UDP port 162.

TEXT

SNMP Operation

SNMP agents that reside on managed devices collect and store information about the device and its operation. This information is stored by the agent locally in the MIB. The SNMP manager then uses the SNMP agent to access information within the MIB.

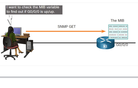
There are two primary SNMP manager requests, get and set. A get request is used by the NMS to query the device for data. A set request is used by the NMS to change configuration variables in the agent device. A set can also cause action to occur on managed devices. For example, a router can be rebooted, a port on a switch can be shut down, or a new configuration file can be sent to a configuration file. The SNMP manager uses the get and set actions to perform the operations described in the table.

Command	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
get-bulk-request	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
get-response	Responds to a **get-request**, **get-next-request**, and **set-request** sent by an NMS.
set-request	Stores a value in a specific variable.

The SNMP agent responds to SNMP manager requests as follows:

- **Get or GET-next-request.** The SNMP agent performs the function in response to a GetResponse PDU from the network manager. The agent retrieves the value of the requested MIB variable and responds to the network manager with that value.
- **Set or SET-request.** The SNMP agent performs the function in response to a GetResponse PDU from the network manager. The SNMP agent changes the value of the MIB variable to the value specified by the network SNMP manager. The agent sends a set-request response the new settings in the device.

The figure illustrates the use of an SNMP GetResponse to determine if interface G0/0/0 is up/up.



TEXT

SNMP Agent Traps

An SNMP particularly polls the SNMP agents that are residing on managed devices using the get request. The NMS queries the device for data. Using this process, a network management application can collect information to monitor traffic loads across the entire configurations of managed devices. This information can be displayed on a variety of graphical formats, to allow for easier analysis of the network. However, polling can cause a lot of traffic on the network, which can reduce the bandwidth available for other network traffic. For example, if there are 1000 nodes to poll, it could take a long time for all the information to be displayed. Also, polling is not efficient because it requires bandwidth to be used even when there is no new information to be reported.

Periodic SNMP polling does have disadvantages. First, there is a delay between the time that an event occurs and the time that it is noticed (via polling) by the NMS. Second, there is a trade-off between polling frequency and bandwidth usage.

To mitigate these disadvantages, it is possible for SNMP agents to generate and send traps to inform the NMS immediately of certain events. Traps are unsolicited messages that inform the SNMP manager that an event has occurred on the managed device. The SNMP manager can then retrieve the MIB information, if necessary, remains, the status (up or down), BGP, address binding, pinning of IP conflictions, level of connectivity to a neighbor, or other significant events. Trap checksum authentication and timestamps are included in the trap messages to provide security and to ensure that the information is current.

The figure illustrates the use of an SNMP trap to alert the network administrator that interface G0/0/0 has failed. The NMS software can send the network administrator a text message, pop up a window on the NMS software, or turn the icon red on the NMS GUI.

The exchange of all SNMP messages is illustrated in the figure.

TEXT

SNMP Versions

There are several versions of SNMP:

- **SNMPv1** – This is the Simple Network Management Protocol, a Full Internet Standard, that is defined in RFC 1157.
- **SNMPv2c** – This is defined in RFCs 1901 to 1908. It uses a community-string based Administrative Framework.
- **SNMPv3** – This is an interoperable standards-based protocol that is defined in RFCs 2273 to 2275. It offers secure access to devices by authenticating and encrypting packets over the network. It includes these security features: message integrity to ensure that a packet was not tampered with in transit, authentication to determine that the message is from a valid source, and encryption to prevent the contents of a message from being read by an unauthorized source.

All versions use SNMP managers, agents, and MIBs. Cisco IOS software supports the above three versions. Version 1 is a legacy solution and is not often encountered in networks today; therefore, this course focuses on versions 2c and 3.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers that is able to access the MIB of the agent is defined by a community string.

Unlike SNMPv1, SNMPv2c includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round trips required. The SNMPv2c improved error handling includes expanded error codes that distinguish different kinds of error conditions. These conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2c include the error type.

Note: SNMPv1 and SNMPv2c offer minimal security features. Specifically, SNMPv1 and SNMPv2c can neither authenticate the source of a management message nor provide encryption. SNMPv3 is most currently deployed of the three versions of SNMP. It adds methods to ensure the secure transmission of critical data between managed devices.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determines which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2c, and SNMPv3.

The table describes the characteristics of the different combinations of security models and levels.

Click each button for more information about the characteristics of the different combinations of security models and levels.

Security Model	SNMPv1
Security Level	noAuthNoPriv
Authentication	Community string
Encryption	No
Result	Uses a community string match for authentication.

A network administrator must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple SNMP managers, it is possible to configure the software to support communications by using SNMPv1, SNMPv2c, or SNMPv3.

TEXT

Check Your Understanding - SNMP Versions

Check your understanding of SNMP versions by choosing the appropriate version for each characteristic.

1. Which SNMP version authenticates the source of management messages?
   - Version 2
   - Version 3
   - Both
2. Which SNMP version provides services for security models?
   - Version 2
   - Version 3
   - Both
3. Which SNMP version does not provide encrypted management messages?
   - Version 2
   - Version 3
   - Both
4. Which SNMP version is supported by Cisco IOS software?
   - Version 2
   - Version 3
   - Both
5. Which SNMP version includes expanded error codes with types?
   - Version 2
   - Version 3
   - Both
6. Which SNMP version uses community-based forms of security?
   - Version 2
   - Version 3
   - Both
7. Which SNMP version is used for interoperability and includes message integrity reporting?
   - Version 2
   - Version 3
   - Both

Check | Show Me | Reset

TEXT

Community Strings

For SNMP to operate, the NMS must have access to the MIB. To ensure that access requests are valid, some form of authentication must be in place.

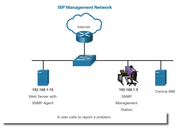
SNMPv1 and SNMPv2c use community strings that control access to the MIB. Community strings are plaintext passwords. SNMP community strings authenticate access to MIB objects.

There are two types of community strings:

- **Read-only (ro)** – This type provides access to the MIB variables, but does not allow these variables to be changed, only read. Because security is minimal in version 2, many vendors default to read-only community strings.
- **Read-write (rw)** – This type provides read and write access to all objects in the MIB.

To view or set MIB variables, the user must specify the appropriate community string for read or write access.

Click Play to see an animation about how SNMP operates with the community string.



Note: Plaintext passwords are not considered a security mechanism. This is because plaintext passwords are highly vulnerable to man-in-the-middle attacks, in which they are compromised through the capture of packets.

TEXT

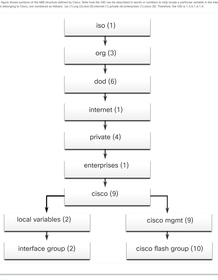
MIB Object ID

The MIB organizes variables hierarchically. MIB variables enable the management software to monitor and control the network device. Formally, the MIB defines each variable as an object ID (OID). OIDs uniquely identify managed objects in the MIB hierarchy. The MIB organizes the OIDs based on RFC standards into a hierarchy of OIDs, usually shown as a tree.

The MIB tree for any given device includes some branches with variables common to many networking devices and some branches with variables specific to that device or device type.

RFCs define some common public variables. Most devices implement these MIB variables. In addition, networking equipment vendors, like Cisco, can define their own private branches of the tree to accommodate new variables for their own networking devices.

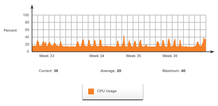
The figure shows portions of the MIB structure defined by Cisco. Note how the OID can be described in words or numbers to help locate a particular variable in the tree. OIDs belonging to Cisco, are numbered as follows: iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Therefore, the OID is 1.3.6.1.4.1.9.



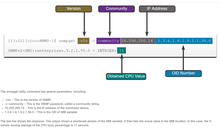
TEXT

SNMP Polling Scenario

SNMP can be used to observe CPU utilization over a period of time by polling devices. CPU statistics can then be compiled on the NMS and graphed. This creates a visual image of the CPU utilization for the network administrator to analyze. In the figure, Week 33 CPU utilization averages this timeline, notifications are sent. The figure illustrates 5 minute samples of hourly CPU utilization over the period of a few weeks.



The data is retrieved via the snmpget utility, based on the NMS. Using the snmpget utility, you can manually retrieve real-time data, or have the NMS run a report. This report would give you a product of time that you could use the data to plot trends. The example shows the data that the SNMP retrieves. The command syntax, the IP address of the network device to query, and the OID number are set. The figure demonstrates the use of the freeware snmpget utility, which allows quick retrieval of information from the MIB.



The snmpget utility command has several parameters, including:

- -v2c – This is the version of SNMP.
- -c community – This is the SNMP password, called a community string.
- 209.165.200.224 – This is the IP address of the network device.
- .1.3.6.1.4.1.9.9.109.1.1.1.1.5.9.1.3.1.0 – This is the OID of MIB variable.

The last line shows the response. The output shows a shortened version of the MIB variable. It then lists the actual value in the MIB location. In this case, the 5-minute moving average of the CPU busy percentage is 1 percent.

TEXT

SNMP Object Navigator

The snmpget utility gives some insight into the basic mechanics of how SNMP works. However, working with long MIB variable names like 1.3.6.1.4.1.9.2.1.58.0 can be problematic for the average user. More commonly, the network administrator will use a network management product with an easy to use GUI, which makes the extra effort to learn the OID numbers unnecessary.

Search for "Cisco SNMP Object Navigator tool" to find the Cisco tool that allows a network administrator to research details about a particular OID. The figure displays an example of using the navigator to research the OID for **ciscoFlashFileSystemTable**.

The figure displays an example of using the Cisco SNMP navigator to research the OID information for the ciscoFlashFileSystemTable. The figure is a screenshot of the SNMP Object Navigator ciscoFlashFileSystemTable OID. The navigator displays the OID, the object name, the object name the OID is receive object details. Output is provided below the tool box and gives the object information. The output on the screenshot shows the ciscoFlashFileSystemTable OID is 1.3.6.1.4.1.9.9.10.1.1.4.1.1 and the object name is ciscoFlashFileSystemTable. The MIB with a link to view supporting images and text is the description, this variable contains a private cisco table which contains the square only file system was last restarted.

TEXT

Lab - Research Network Monitoring Software

In this lab, you will complete the following objectives:

- Part 1: Survey Your Understanding of Network Monitoring
- Part 2: Research Network Monitoring Tools
- Part 3: Select a Network Monitoring Tool

Research Network Monitoring Software