Lab 9: Simple Network Management Protocol

Student Name: .....
Student No: .....

Objectives:

- ✓ To understand and practice Simple Network Management Protocol on GNS3.

Content:

I. Introduction to Simple Network Management Protocol

"Building a working network is important but monitoring its health is as important as building it."

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

1. Understand SNMP

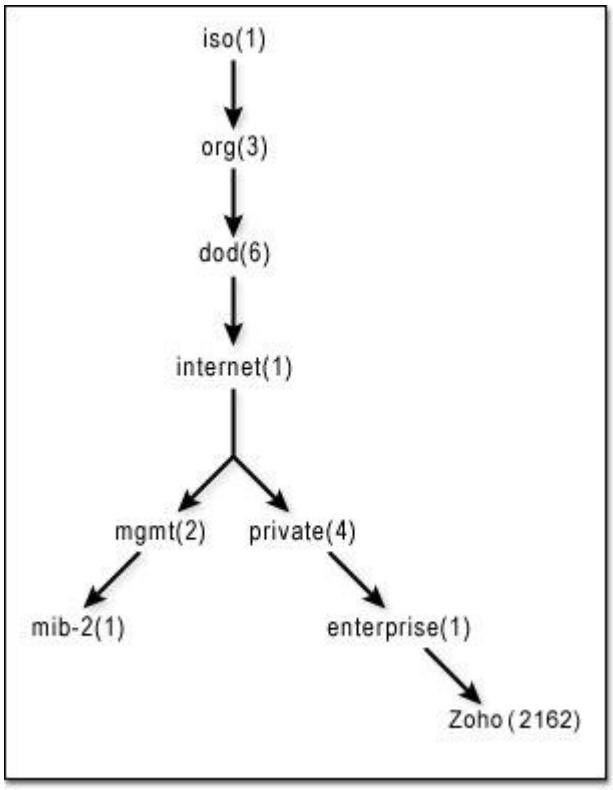
SNMP consists of 3 items:

- SMNP Manager (sometimes called Network Management System – NMS): a software runs on the device of the network administrator (in most case, a computer) to monitor the network.
- SNMP Agent: a software runs on network devices that we want to monitor (router, switch, server…)
- Management Information Base (MIB): is the collection of managed objects. This component makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP

Manager can ask the Agent (and the Agent can understand them). MIB is commonly shared between the Agent and Manager.

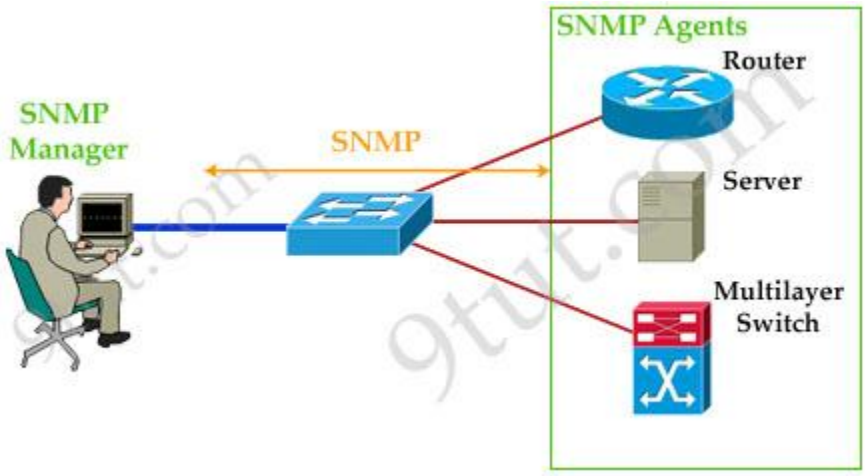
There are a lot of syntaxes defined for defining the MIB, but the purpose of the MIB is simple. For example, if a company wants to build an application and wants the application to be remotely managed, then while building the application itself, the architects of the application or the device will write a MIB which will have information, such as what are the variables that should be published outside (to the Manager), what is the use of each variable, what each value in the variable represents, and so on.

Each variable is assigned a unique identifier in SNMP that is called an object identifier (OID). Object identifier is a unique ID (like registration numbers), but the uniqueness is maintained all over the world. The format of OID is a sequence of numbers with dots in between. There are two roots for object identifiers, they are iso (which is .1) and ccit (which starts with .0). Most object identifiers start with .1.3.6.1 (where 1 = iso, 3 = org, 6 = dod, 1 = internet). From internet, there are two branches, mgmt and private.



All standard MIBs reside under mgmt (.1.3.6.1.2) in this diagram - for example, MIB II (.1.3.6.1.2.1). The distinction between the standard and private MIBs is that of control over the object definitions (that is, defining the variables). Standard MIBs are those that have been approved by the Internet Activities Board (IAB). MIBs defined unilaterally by equipment and software vendors are initially defined as private MIBs under private.enterprises. A branch within the private.enterprises sub-tree is allocated to each vendor that registers for an enterprises object identifier. In the above picture, zoho has got the enterprise OID as 2162. So all the variables we define for our device or application should fall under .1.3.6.1.4.1.2162 (.iso.org.dod.internet.private.enterprise.zoho). Till the

enterprise number (like 2162), the uniqueness is maintained by the committee, after this the uniqueness should be maintained by each enterprise.



For example, in the topology above you want to monitor a router, a server and a Multilayer Switch. You can run SNMP Agent on all of them. Then on a PC you install a SMNP Manager software to receive monitoring information. SNMP is the protocol running between the Manager and Agent. SNMP communication between Manager and Agent takes place in form of messages. The monitoring process must be done via a MIB which is a standardized database and it contains parameters/objects to describe these networking devices (like IP addresses, interfaces, CPU utilization, …). Therefore the monitoring process now becomes the process of GET and SET the information from the MIB.

2. SNMP Versions

SNMP has multiple versions but there are three main versions: SNMP version 1, SNMP version 2c, SNMP version 3.

SNMPv1 is the original version and is very legacy so it should not be used in our network. SNMPv2c updated the original protocol and offered some enhancements. One of the noticeable enhancement is the introduction of INFORM and GETBULK messages.

Both SNMPv1 and v2 did not focus much on security and they provide security based on **community string** only. Community string is really just a clear text password (without encryption). Any data sent in clear text over a network is vulnerable to packet sniffing and interception. There are two types of community strings in SNMPv2c:

- **Read-only (RO)**: gives read-only access to the MIB objects which is safer and preferred to other method.
- **Read-write (RW)**: gives read and write access to the MIB objects. This method allows SNMP Manager to change the configuration of the managed router/switch so be careful with this type.

The community string defined on the SNMP Manager must match one of the community strings on the Agents in order for the Manager to access the Agents.

SNMPv3 provides significant enhancements to address the security weaknesses existing in the earlier versions. The concept of community string does not exist in this version. SNMPv3 provides a far more secure communication using entities, users and groups

Note: Although SNMPv3 offers better security but SNMPv2c however is still more common

3. SNMP Messages

SNMP Messages are used to communicate between the SNMP Manager and Agents. SNMPv1 supports five basic SNMP messages:

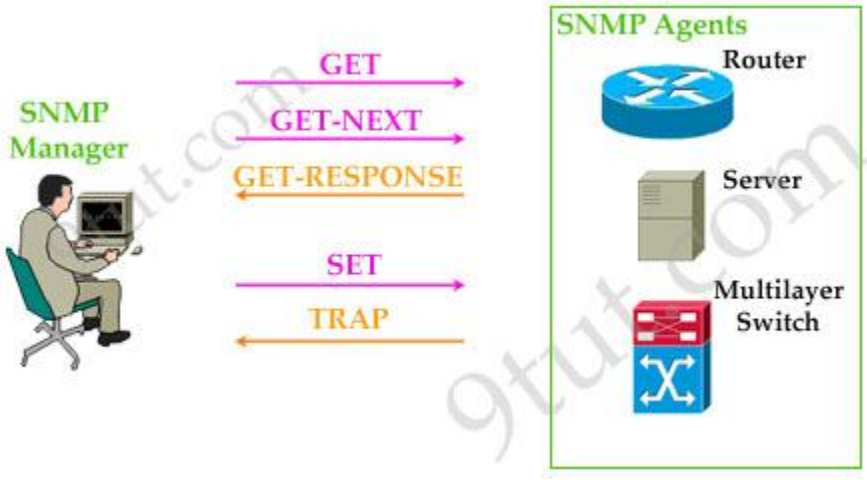
- SNMP GET
- SNMP GET-NEXT
- SNMP GET-RESPONSE
- SNMP SET
- SNMP TRAP

In general, the GET messages are sent by the SNMP Manager to retrieve information from the SNMP Agents while the SET messages are used by the SNMP Manager to modify or assign the value to the SNMP Agents.

Note: GET-NEXT retrieves the value of the next object in the MIB.

The GET-RESPONSE message is used by the SNMP Agents to reply to GET and GET-NEXT messages.

Unlike GET or SET messages, TRAP messages are initiated from the SNMP Agents to inform the SNMP Manager on the occurrence of an event. For example, suppose you want to be alarmed when the CPU usage of your server goes above 80%. But it would be very annoying if the administrator has to actively use the GET message to check the CPU usage from time to time. In this case, the TRAP message is very suitable for that purpose because the administrator would only be informed from the CPU itself when that event occurs. The figure below shows the direction of SNMP messages:



From SNMPv2c, two new messages were added: INFORM and GETBULK.

INFORM: An disadvantage of TRAP message is unreliable. SNMP communicates via UDP so it is unreliable because when the SNMP Agents send TRAP message to the SNMP Manager it cannot know if its messages arrive to the SNMP Manager. To amend this problem, a new type of message, called INFORM, was introduced from SNMPv2. With INFORM message, the SNMP Manager can now acknowledge that the message has been received at its end with an SNMP response protocol data unit (PDU). If the sender never receives a response, the INFORM can be sent again. Thus, INFORMs are more likely to reach their intended destination.

GETBULK: The GETBULK operation efficiently retrieve large blocks of data, such as multiple rows in a table. GETBULK fills a response message with as much of the requested data as will fit.

Note: There is no new message types on SNMPv3 compared to SNMPv2c.

4. SNMP Configuration

This part will go through a simple SNMP configuration of SNMPv2c as it is still the most popular SNMP version being used these days.

a. Configure a community string

```
Router(config)#snmp-server community <community name> ro
```

The ro stands for read-only method.

b. Configure the IP address of a host receiver (SNMP Manager) for SNMPv2c TRAPs or INFORMs

```
Router(config)#snmp-server host 10.10.10.12 version 2c <community name>
```

c. Enable the SNMP Traps

```
Router(config)#snmp-server enable traps
```

If we don’t want to enable all trap messages we can specify which traps we want to be notified. For example, if you only want to receive traps about link up/down notification type then use this command instead:

```
Router(config)#snmp-server enable traps link cisco
```

Of course we have to configure an SNMP Manager on a computer with these community strings so that they can communicate.

II. Practice

Lab steps:

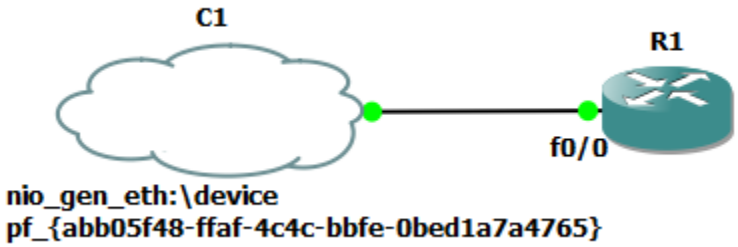
1. Open GNS3 with administrator privilege. (right click on GNS3 icon, choose Run as administrator).

2. Create the topology as follows:

   a. Drag the Cloud to the main Workspace. Under NIO Ethernet tab, choose the interface that is being used to connect your computer to the Internet. (The wired Interface is better if possible) and click "Add" to create the Ethernet Interface for the Cloud.

   b. Drag c2600 Router to the main Workspace (Other types of router can also be used for this lab).

   c. Connect two devices.



   d. If your computer is connecting to the Internet using Wired Interface, configure interface f0/0 of R1 to obtain an IP address via DHCP. Otherwise, manually configure the IP address for R1's f0/0 interface. Assume f0/0 interface of R1 is allocated the IP address of 172.28.13.200

3. Install an SNMP management program.

   a. Download and install the PowerSNMP Free Manager by Dart Communications from the following URL: http://www.dart.com/snmp-free-manager.aspx

   This executable file of the program is also delivered together with this document.

   b. Launch the PowerSNMP Free Manager program.

   c. Click No if prompted to discover available SNMP agents. You will discover SNMP agents after configuring SNMP on R1. PowerSNMP Free Manager supports SNMP version 1, 2, and 3. This lab uses SNMPv2.

   d. In the pop-up Configuration window (if no pop-up window appear, go to Tools > Configuration), set the local IP address to listen on 172.28.13.100 (assume that your computer is using this IP address) and click OK .

   Note: If prompted to discover available SNMP agents, click No and continue to next part of the lab.

4. Configure an SNMP agent.

a. On R1, enter the following commands from the global configuration mode to configure the router as an SNMP agent. In line 1 below, the SNMP community string is lab9, with read-only privileges. In lines 2 and 3, the SNMP manager location and contact commands provide descriptive contact information. Line 4 specifies the IP address of the host that will receive SNMP notifications, the SNMP version, and the community string. Line 5 enables all default SNMP traps.

```
R1(config)# snmp-server community lab9 ro
R1(config)# snmp-server location netlab_B1
R1(config)# snmp-server contact netlab_admin
R1(config)# snmp-server host 172.28.13.100 version 2c lab9
R1(config)# snmp-server enable traps
```

b. At this point, you may notice that the PowerSNMP Free Manager is receiving notifications from R1. If it is not, you can try to force a SNMP notification to be sent by entering a copy run start command on R1. Continue to the next step if it is unsuccessful

5. Discover SNMP agents.

a. From the PowerSNMP Free Manager on PC-A, open the Discover > SNMP Agents window. Enter the IP address 172.28.13.255 (the broadcast IP address in the same range with IP address of your computer and R1's f0/0 interface). In the same window, click Properties and set the Community to lab9 and the SNMP Version to Two, and then click OK. Now you can click Find to discover all SNMP agents on the 172.28.13.0 network. The PowerSNMP Free Manager should find R1 at 172.28.13.200. Click the checkbox and then Add to add R1 as an SNMP agent

b. In the PowerSNMP Free Manager, R1 is added to the list of available SNMPv2 agents.

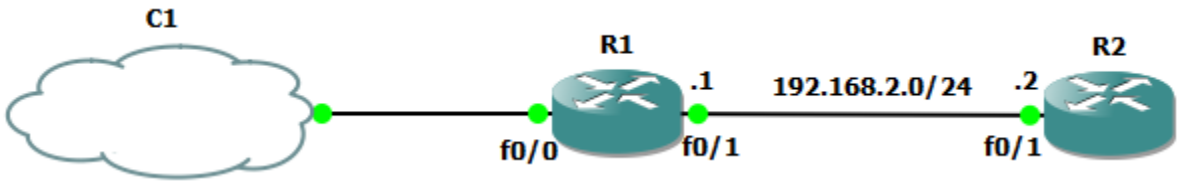
Next, you will force SNMP notifications to be sent to the SNMP manager located at PC-A. You will then convert the received OID codes to names to learn the nature of the messages. The MIB/OID codes can be easily converted using the Cisco SNMP Object Navigator located at http://www.cisco.com.

6. Clear current SNMP messages.

In the PowerSNMP Free Manager, right-click the Traps window and select Clear to clear the SNMP messages.

7. Generate an SNMP trap and notification.

Drag c2600 Router to the main Workspace, and configure f0/1 interface of R1 and R2 as follows:



Accessing global configuration mode and enable an interface will generate an SNMP trap notification to be sent to the SNMP Manager at your computer. Notice the Enterprise/OID code numbers that are visible in the traps window

8. Decode SNMP MIB/OID messages.

   From a computer with Internet access, open a web browser and go to http://www.cisco.com

   a. Using the search tool at the top of the window, search for SNMP Object Navigator.

   b. Choose SNMP Object Navigator MIB Download MIBs OID OIDs from the results.

   c. Navigate to the MIB Locator page by clicking the SNMP Object Navigator.

   d. Using the SNMP Object Navigator page, decode the OID code number from the PowerSNMP Free Manager generated in step 7. Enter the OID code number and click Translate to see their corresponding message translations

Note: another useful lab on SNMP can be found at
http://resources.intenseschool.com/network-management-labs-in-gns3-part-1/

Reference

http://www.9tut.com/simple-network-management-protocol-snmp-tutorial

http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol

http://www.webnms.com/cagent/help/technology_used/c_snmp_overview.html

https://courses.cs.ut.ee/MTAT.08.004/2014_spring/uploads/Main/38_2.pdf