Network Management System (NMS)
Using SNMP Protocol

1 INTRODUCTION

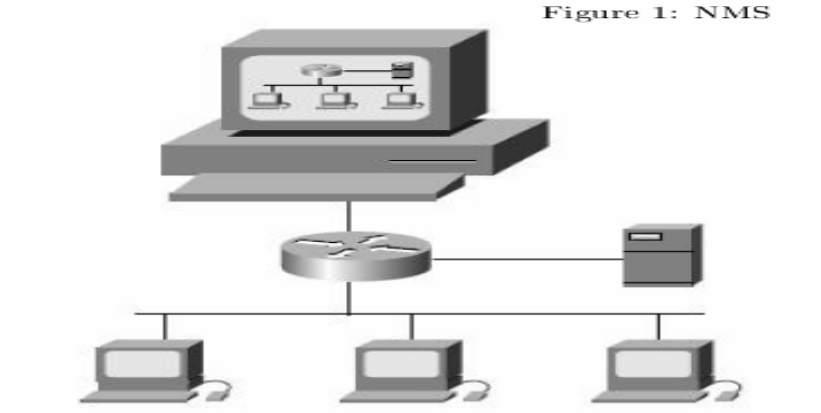
In today's complex network of routers, switches, and servers, it can seem like a daunting task to manage all the devices on your network and make sure they're not only up and running but also performing optimally. This is where the Simple Network Management Protocol (SNMP) can help. SNMP was introduced in 1988 to meet the growing need for a standard for managing Internet Protocol (IP) devices. SNMP provides its users with a "simple" set of operations that allows these devices to be managed remotely. This experiment is aimed toward system administrators who would like to begin using SNMP to manage their servers or routers.

2 SNMP DESCRIPTIONS

SNMP defines a client/server relationship. The client program (called the network manager) makes virtual connections to a server program (called the SNMP agent), which executes on a remote network device, and serves information to the manager regarding the device’s status. The database, controlled by the SNMP agent, is referred to as the SNMP Management Information Base (MIB), and is a standard set of statistical and control values. SNMP additionally allows the extension of these standard values with values specific to a particular agent through the use of private MIBs. Directives, issued by the network manager client to an SNMP agent, consist of the identifiers of SNMP variables (referred to as MIB object identifiers or MIB variables) along with instructions to either get the value for the identifier, or set the identifier to a new value. Through the use of private MIB variables, SNMP agents can be tailored for a myriad of specific devices, such as network bridges, gateways, and routers. The definitions of MIB variables supported by a particular agent are incorporated in descriptor files, written in Abstract Syntax Notation (ASN.1) format, made available to network management client programs so that they can become aware of MIB variables and their usage.

the fig. below shows how can we use the SNMP in managing our network .

Figure 1: NMS



3 SNMP VERSIONS

Three versions of SNMP exist: SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) and SNMP version3 (SNMPv3). These versions have a number of features in common, but SNMPv2 and SNMPv3 offers enhancements, such as additional protocol operations. Standardization of yet another version of SNMP—SNMP Version 4 (SNMPv4)—is pending. This chapter provides descriptions of the SNMPv1, SNMPv2, and SNMPv3 protocol operations.

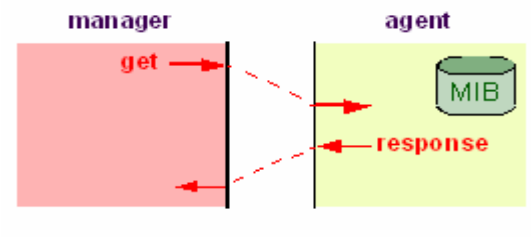
4 SNMP OPERATION

SNMP provide us with different operation which facilitate our managing and controlling over our network.

The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap.

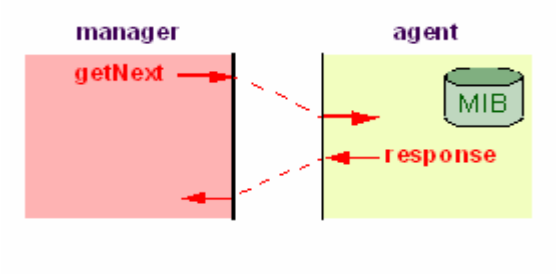
4.1 GET REQUEST :

Specific values can be fetched via the “get” request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device. as shown in the fig. below



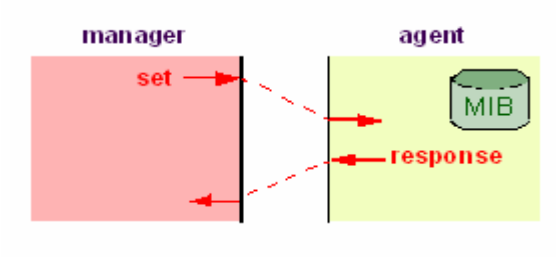
4.2 GET NEXT REQUEST:

The SNMP standard permits network managers to “walk” through all SNMP values of a device (via the “get-next” request) to determine all names and values that an operant device supports. This is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a “get-next”, and repeating this operation until an error is encountered (indicating that all MIB object names have been “walked”.)



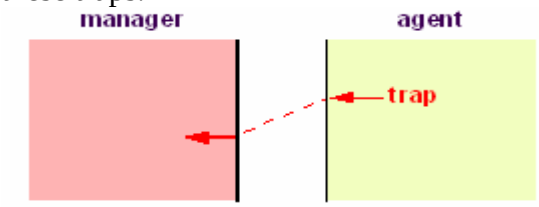
4.3 SET REQUEST:

The SNMP standard provides a method of effecting an action associated with a device (via the “set” request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. This provides a way of configuring and controlling network devices via SNMP.



4.4 TRAP MESSAGE:

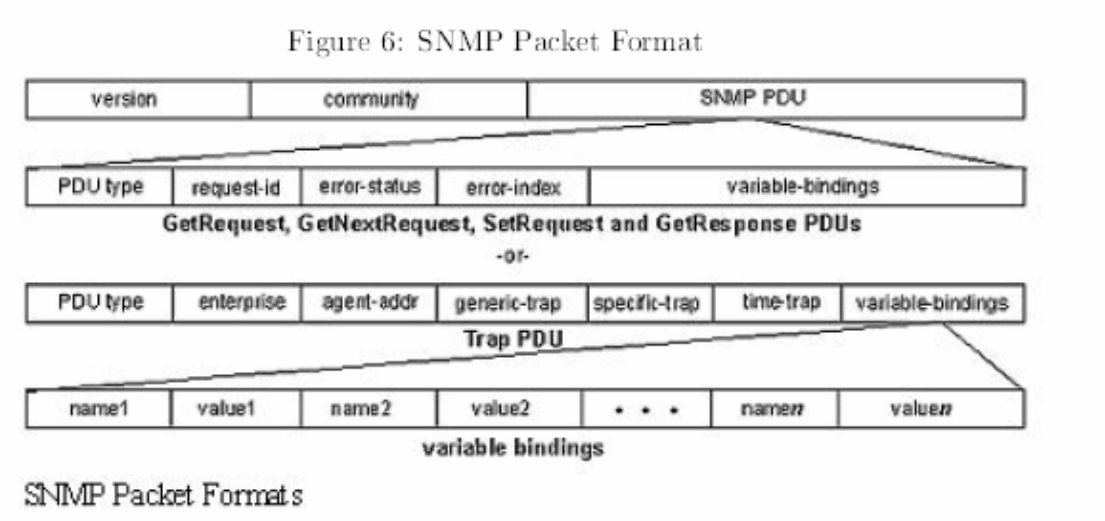
The SNMP standard furnishes a mechanism by which devices can “reach out” to a network manager on their own (via the “trap” message) to notify the manager of a problem with the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.



5 SNMP PACKET FORMATS

The image below shows the SNMP packet formats. Each variable binding contains an identifier, a type and a value (if a Set or response). The agent checks each identifier against its MIB to determine whether the object is managed and changeable (if processing a Set). The manager uses its MIB to display the readable name of the variable and sometimes interpret its value.

Figure 6: SNMP Packet Format



SNMP Packet Formats

6 OBJECTIVES:

Configure the simple Network Management Protocol over Cisco routers. Background: Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. Optionally, you can specify one or more of the following characteristics associated with the string:

• An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

• A MIB view, which defines the subset of all MIB objects accessible to the given community.

• Read and write or read-only permission for the MIB objects accessible to the community.

7 APPARATUS REQUIRED:

The following resources will be required:

- Cisco 1700 Router
- 3 Straight through Cables.
- PC with MIB Browser software Installed.
- PC with snifter Software Installed.

8 EXPERIMENTAL PROCEDURES

Notes:

1)
the SNMP use two ports:

• port ``161" for the set and get functions

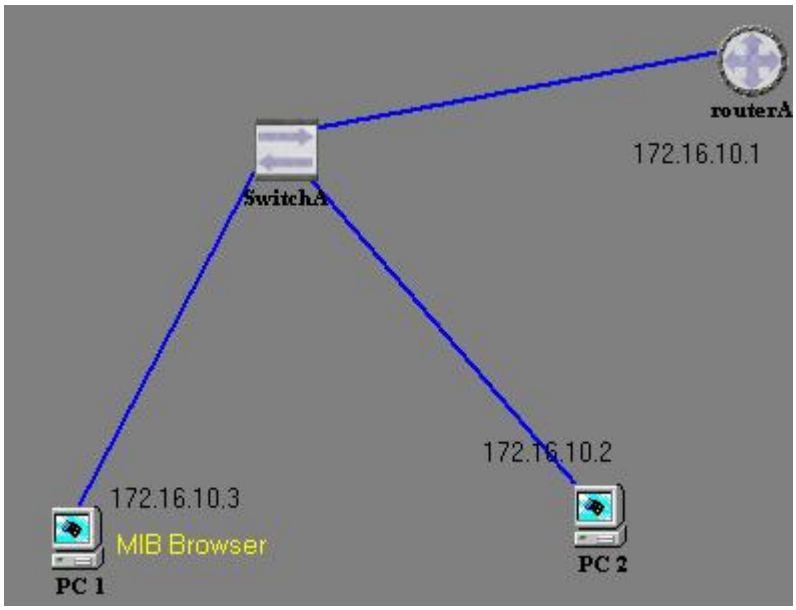
• port ``162" for the trap function

so the first step is to turn off the firewall or we can handle it with opening these two ports

2)
To learn how to install the SNMP services see the appendix

8.1 :

Build the following Network



8.2 :

Enable and configure Router IP address for Fast Ethernet interface

8.3 :

Enable And Configure SNMP Agent on Cisco Router.

Explanation:

Instructions are provided here for Use an SNMP community string to define the relationship between the SNMP manager and the agent.

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the SNMP-server community global configuration command. To remove the specified community string, use the no form of this command.

By default, an SNMP community string permits read-only access to all objects.

Examples:

The following example assigns the string samer to SNMP allowing read-only access and specifies that IP access list 4 can use the community string:

Router(config)# snmp-server community samer ro 4

The following example assigns the string ``ccna" to SNMP allowing read-write access to the objects in the restricted view:

Router(config)# snmp-server community ccna view restricted rw

The following example removes the community ccosamana :

Router(config)# no snmp-server community ccosamana

The following example disables all versions of SNMP:

Router(config)# no snmp-server

8.4 :

• Configure the PC IP address to be in the same network, and install Management and monitoring tools from add/remove windows components.

• Configure SNMP Manger on PC to connect Cisco Router SNMP Agent.

Explanation: Instructions are provided here for Use an SNMP MIB browser how to connect Router Agent . Ensure that SolrWinds Tool Bar is started. Choose from tool bar MIB Browser and start the program called MIB Browser. Provide the IP address or host name of your Router.

8.5 :

As mentioned before, the community is a kind of security authentication that the SNMPv1 provide, So let us now feel how it works and how to set it.

• providing a wrong community, and noticing what is the response of that

• providing the right community.

8.6 :ADDING THE COMMUNITY IN THE AGENT

to let you NMS communicate with any host, you must configure the agent community in order to make it as a security authontication between both sides.

adding a community string in your PC agent following these steps:

• strat -> run -> services.msc

• choose SNMP Services.

• choose Security tap.

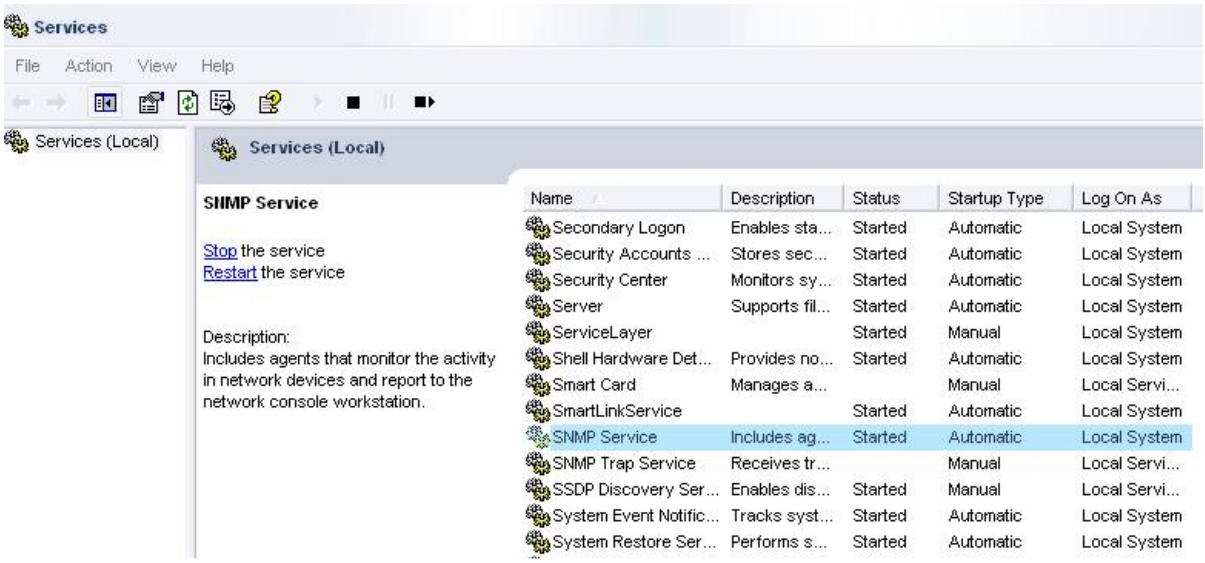
• Press add to add the new community choosing the authontication type of it (read only, read and write, ... etc)

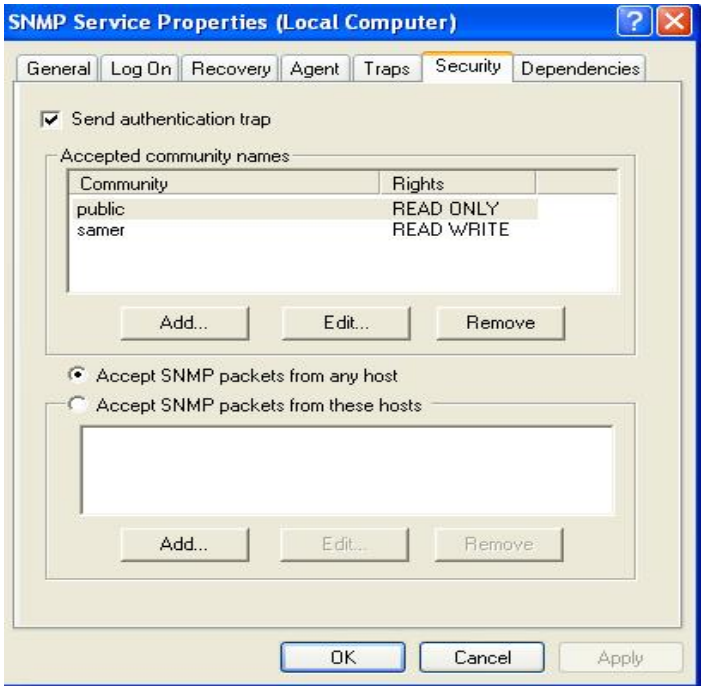
I.e :

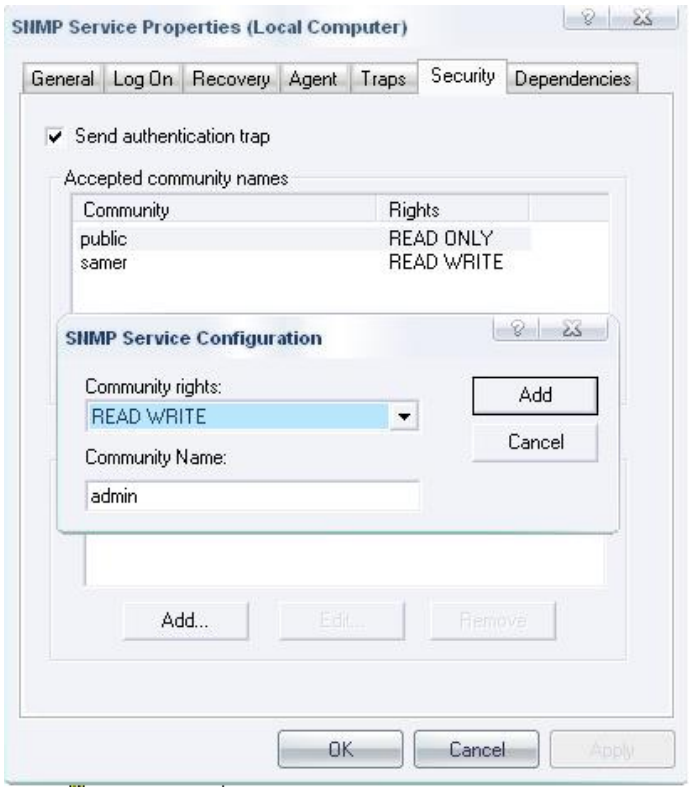
• Read Only : this community allowing the NMS to read without allowing it to creat change.

• Read Write: this community allowing the NMS to read and write.

And the figures below show how to do it step by step:

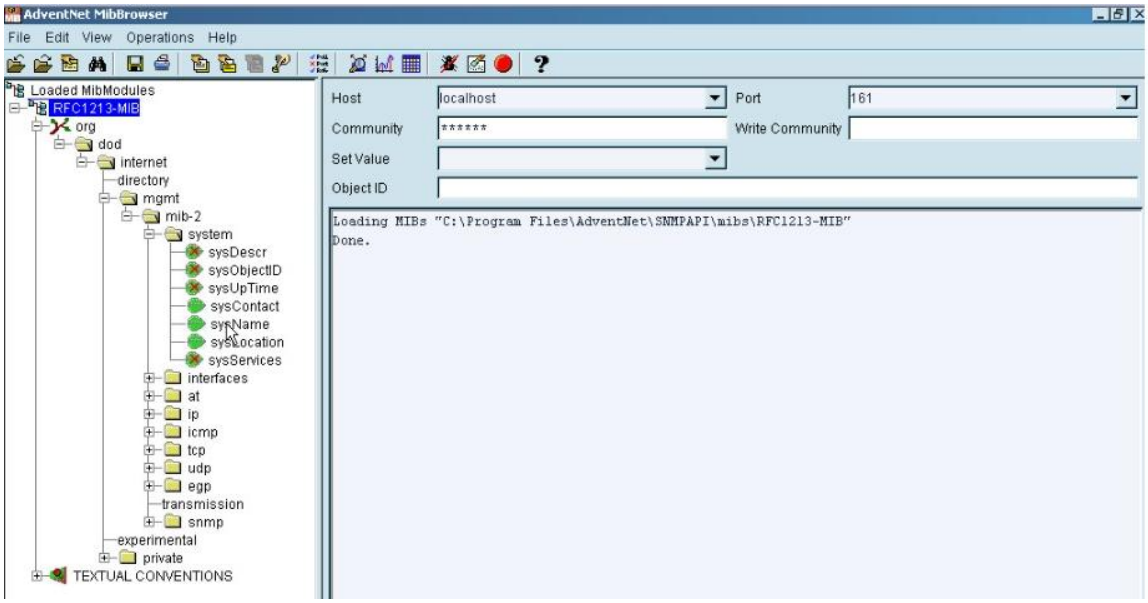



SNMP Service Properties (Local Computer)
General
Log On
Recovery
Agent
Traps
Security
Dependencies
Send authentication trap
Accepted community names
Community
Rights
public
READ ONLY
samer
READ WRITE
Add...
Edit...
Remove
Accept SNMP packets from any host
Accept SNMP packets from these hosts
Add...
Edit...
Remove
OK
Cancel
Apply


SNMP Service Properties (Local Computer)
General
Log On
Recovery
Agent
Traps
Security
Dependencies
Send authentication trap
Accepted community names
Community
Rights
public
READ ONLY
samer
READ WRITE
SNMP Service Configuration
Community rights:
READ WRITE
Add
Cancel
Community Name:
admin
Add...
Edit...
Remove
OK
Cancel
Apply

8.7 : SNMP OPERATIONS

SET OPERATION



we can see now how can we use this function to let us set the computer name for example

first we have to go to the services (start->run-> services.msc) and choosing the SNMP right click , then go to the security tap then set your agent to accept packets from host (specific host) or from any host.

now in the MIB browser we can choose the system name object ID as shown in the fig above

give the host of PC2

assign the port 161 for this function

write the right community that you used.

enter the new name that you like.

then choose set

here if you gave the right host and community the new name will take place instead of the old one.

GET OPERATION

like what we did above we can get the name of the PC3 from our NMS .

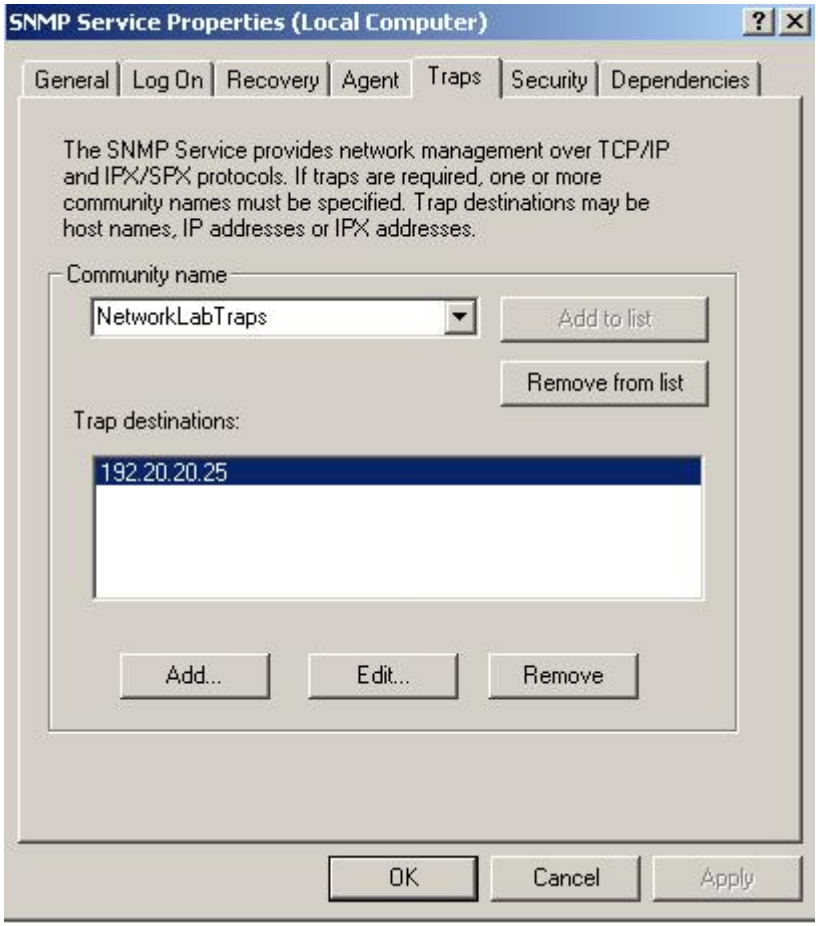
as what we did before, entering the right community , the ip address of the host and the object ID

then choose the get function

and the same for the router if we want to set or get any object.

TRAP OPERATION

To use the trap service, first, you have to to add the IP address of the NMS to the trap destination in the agent, as shown:



As shown in the figure, you must specify the community for traps. In the figure, the community is: NetworkLabTraps. This community is used also by the NMS to authenticate SNMP trap packets received on port 162. Note that the community is case sensitive like a password.

TRAP SCENARIO:

1. Go to the 'Trap Viewer' in the MIB-browser. Add the community 'NetworkLabTraps' with port '162'.

2. Press 'Start' to listen for traps with specified community.

3. Try to perform a GET operation on 'sysName' object in the MIB-II with the correct community. What is the result?

4. Change the community to anything other than that configured by the SNMP agent. And repeat the above step. What is the result? What does the Trap Viewer show?

To see details about traps in the trap viewer, select the trap and then press on 'Show Details'. In the scenario above, the the trap sent to the NMS has information indicating 'AuthenticationFailure'.

8.8 : USE THE PC WITH SNIFFER SOFTWARE(ETHERREAL) TO CAPTURE SNMP TRAFFIC

Start ethereal software and go Capture Menu and configure it with appreciate parameters and start capturing SNMP traffic pass between MIB Browser and SNMP agent.

NOTE: make sure you are capturing from the right NIC. Repeat the step connecting SNMP manager and SNMP agent after connection successful stop capture and search for the community string and write it down

8.9 ENABLE AND CONFIGURE SNMP TRAP ON CISCO ROUTER AND MANAGEMENT STATION.

The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers. Routers can send notifications to SNMP managers when particular events occur. For example, an agent router might send a message to a manager when the agent router experiences an error condition. o Configure Cisco router to Send traps Messages. To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the snmp-server enable traps global configuration command. To disable all available SNMP notifications, use the no form of this command. This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command. If you do not enter an snmp-server enable traps command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one snmp-server enable traps command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate snmp-server enable traps command for each notification type and notification option. The snmp-server enable traps command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.

Example*:* The following example enables the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

Router(config)# snmp-server enable traps

Router(config)# snmp-server host 10.1.1.1 public

Router(config)# snmp-server host myhost.cisco.com public

• Configure and enable PC to Receive trap Messages. This can be done from the trap viewer as mentioned before.

• Start SolarWinds SNMP Traps Receiver Program form Start Menu

• On the router make some changes so a trap to be send to the SNMP trap receiver.

• Configure router to enable serial port.

• Configure router to disable the same serial port.

• Try to use SNMP trap editor to send a trap from one PC to another which have SNMP trap Receiver.