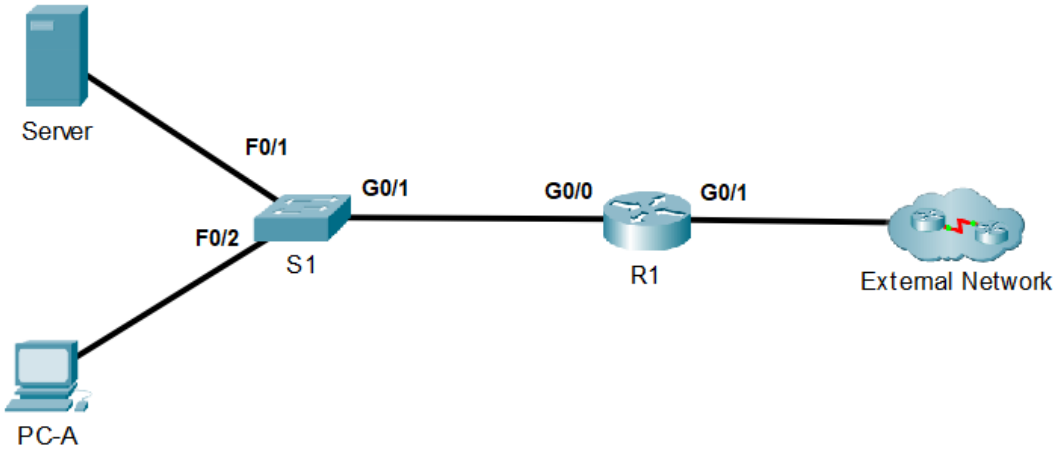
Networking Academy

Shaun Lim

Lab 6.3 Using Network Management Tools (SNMP) – PT

This activity comes with an accompanying Packet Tracer file with a partially configured network. Make sure to download the Packet Tracer file from the Animospace assignment page.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	209.165.200.2	255.255.255.252	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.4	255.255.255.0	192.168.10.1
Server	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

Configure an SNMPv2 Manager and Agent

Background / Scenario

Network management is an essential task of a network administrator once a network is deployed and operational. It involves regularly monitoring device operations and making the necessary configuration changes in response to various network scenarios. To reduce the administrative overhead of performing network management, several tools are available. These include device discovery tools, logging, and centralized management. In this lab, you will configure and explore the capabilities of a widely used network management tool and protocols: SNMP.

Instructions: Configure an SNMPv2 Manager and Agent

Simple Network Management Protocol (SNMP) is an IETF standard which can be used to both monitor and control clients on the network. SNMP can be used to get and set variables related to the status and configuration of network hosts like routers and switches, as well as network client computers. The SNMP manager can poll SNMP agents for data, or data can be automatically sent to the SNMP manager by configuring traps on the SNMP agents.

In Part 4, R1 will be configured as an SNMP agent with the PC host acting as SNMP manager using its built in Network Management System.

Step 1: Configure R1 as an SNMP Agent

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 ciscolab, with read-only privileges. On a real device, it is highly recommended that an ACL be used to limit access via SNMP to legitimate network managers only. SNMP trapping may also be configured for automated reporting of device status changes; however, due to Packet Tracer feature limitations, these additional configurations will not be performed.

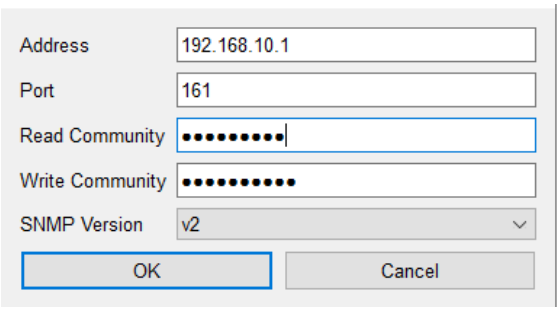
```
R1(config)# snmp-server community ciscoread ro
R1(config)# snmp-server community ciscowrite rw
```

Step 1: Configure SNMP manager access to the SNMPv2 agent.

a. On the PC Host Desktop, open the MIB Browser

b. Click on Advanced...

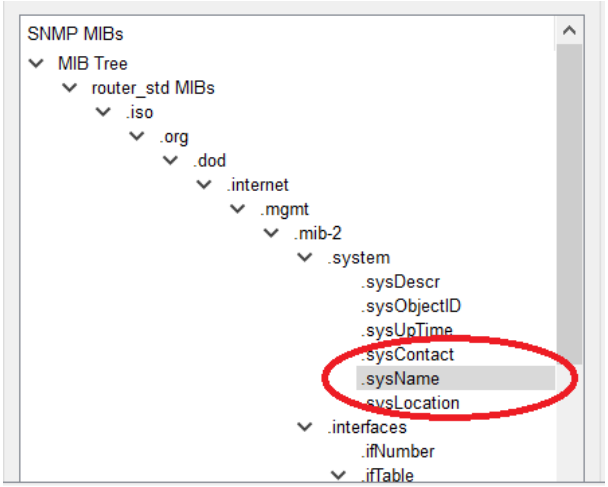
c. Enter the SNMPv2 settings that were configured on R1. Click **OK** to continue.



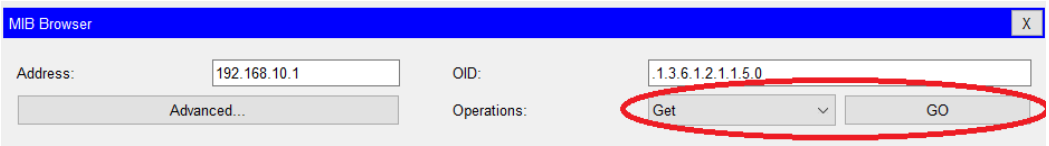
SNMP Parameters	Settings
Address	192.168.10.1
Read Community	ciscoread
Write Community	ciscowrite
SNMP Version	V2

Step 2: Query for MIB object values using the GET Request.

a. In the MIB Tree panel of the browser (left panel), expand the Router_std MIBs tree and select the object **.iso.org.dod.internet.mgmt.mib-2.system.sysName** You may exand the panel to to full screen and drag the edge of the left pane to easily see the node names as you go further down the tree.



b. Set the Operation to **Get** and click on **Go** to get the value of the selected MIB object



What was the result of the query?

Name/OID is 1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysName.0)
Value is R1
Type is OctetString

c. Visit the Cisco SNMP Object Navigator (https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en)

Accessing the page will require you to login using your NetAcad account .

d. Copy the numeric OID (do not include the last '.0') to the query box and click on **Translate.** This will retrieve details about the specific MIB object.

What does the OID represent according to the resulting description?

The OID provides human-readable names in order to easily identify and label network devices. The OID will be represented if the name of the device is unknown. Otherwise, it will remain empty.

Object	sysName
OID	1.3.6.1.2.1.1.5
Type	DisplayString
Permission	read-write
Status	current
MIB	SNMPv2-MIB ; - View Supporting Images
Description	"An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string."

What permission are available for the object?

Read-write

e. Go back to the MIB Browser in Packet Tracer. Select the object **.iso.org.dod.internet.mgmt.mib-2.system.interfaces.ifTable.ifEntry.ifDescr** then perform a **GET** request again.

What were the results and how many entries were returned this time?

There were 3 entries instead of 1.

Name/OID	Value	Type
1.3.6.1.2.1.2.2.1.2.1	Vlan1	OctetString
1.3.6.1.2.1.2.2.1.2.2	GigabitEthernet0/0	OctetString
1.3.6.1.2.1.2.2.1.2.3	GigabitEthernet0/1	OctetString

f. Take note of the OID number of the results of the last query. They should all have identical IDs except for the last digit. Since this particular object has multiple entries, each entry is assigned its own index as shown below.

Result Table

Name/OID	Value
.1.3.6.1.2.1.2.2.1.2.1 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.if...	Vlan1
.1.3.6.1.2.1.2.2.1.2.2 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.if...	GigabitEthernet0/0
.1.3.6.1.2.1.2.2.1.2.3 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.if...	GigabitEthernet0/1
.1.3.6.1.2.1.2.2.1.2.4 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.if...	Serial0/0/0
.1.3.6.1.2.1.2.2.1.2.5 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.if...	Serial0/0/1

Based on the output of the MIB browser, what index is assigned to G0/1?	3 (1.3.6.1.2.1.2.2.1.2.3)

Step 3: Change MIB object values using the SET Request.

a. Try looking for the OID that represents the interface administrative status of G0/1. Hint: This is also a multiple entry object similar to the interface description. The last digit used for the status of a specific interface will be the same index assigned to the interface when retrieving its description.

What is the numeric OID?	7 (1.3.6.1.2.1.2.2.1.7)

b. Query the Cisco online Object Navigator for this OID. Again, do not include the last '.x' of the OID.

What are the permissions, data type and possible values for this OID?

Permissions	Read-write
Type	Integer
Values	1 : up 2 : down 3 : testing

c. We will now attempt to shutdown the G0/1 interface of R1 using SNMP. In the MIB Browser, change the operation to **Set**. This will bring up a dialog box to input values. Enter the following then click **OK**

OID: (Use the OID determined in Step 3a.)

Datatype: (Copy the type dertermined in Step 3b)

Value: (Copy the value for 'down' in Step 3b)

d. In the MIB Browser, click on **Go** and observe the effect to R1.

What changes happened to the status of R1?

Its status became down. (Line protocol on Interface GigabitEthernet0/1, changed state to down)

Reflection Question

Why is it preferable to solely use read-only access when working with SNMPv2?

When utilizing Simple Network Management Protocol version 2 (SNMPv2), it is typically recommended to restrict access to read-only activities only because these actions enable network monitoring and querying network devices without having to worry about unintentionally changing important settings. Additionally, it improves security by lowering the possible consequences of unwanted modifications, and additionally, read-only access guarantees that network administrators get access to useful data regarding the performance, configuration, and status of devices without worrying about potential issues that may arise because of write operations.