

## Module 4 Lab 4: SNMP Operations Using a MIB Browser (Using a Manager on the Network)

---

(NETLAB+)

### SNMP Operations Using a MIB Browser (Using a Manager on the Network)

**Objective:** To become familiar with SNMP operations on multiple routers in a network and using a MIB Browser on the PC to discover information about the network.

**Overview:** As you work through the lab, you will answer a total of 10 questions in your Canvas online classroom. You will notice statements such as 'ANSWER QUESTION #' and QUESTION # [screenshot] at the end of steps within the lab.

- Steps 2–5 and 8–10 have questions.
- Step 10 have a question to include screenshots.

### START HERE

#### Instructions

Cisco routers and switches contain SNMP agents that can respond to standard SNMP operations. A NMS can query a Cisco device for information via an SNMP GET operation, or it can tell the device to change some setting or take some actions, via a SET operation. In this lab, you will learn how to perform SNMP operations in a network. The PC connected to the R2 LAN in the lower left corner is the manager or NMS. R1, R2, and R3 are agents that can report data to the NMS.

**Step 1.** Schedule NetLab using the information provided by the instructor (remembering that you had to change the password the first time you logged in). Open Cisco Packet Tracer using the icon on the Windows 10 desktop computer within NetLab. Use the **File** menu option to open the **PT\_SNMP\_OperationsUsingMIB\_Browser\_Network** file noting that you may have to expand the file name section to see the file. The topology should resemble Figure 1. The OSPF routing protocol has been installed on the routers. All devices are addressed except for PC1 and PC2.

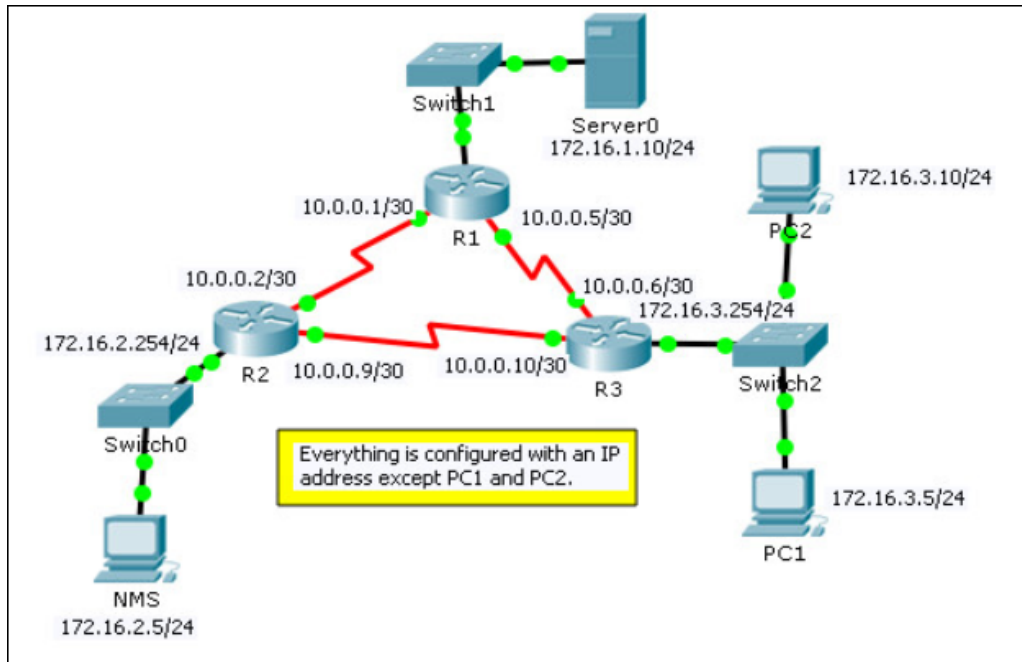


Figure 1.

**Step 2.** Configure PC1 and PC2 with an IP address, subnet mask, and default gateway. Refer to a previous lab (that could be in a previous module) if you do not remember how to do this. The IP addressing used for the networks are shown in the following table: **ANSWER QUESTIONS 1 AND**

**2**

Device	Interface	IP Address
R1	FastEthernet0/0	172.16.1.254/24
	Serial0/0/0	10.0.0.1/30
	Serial0/0/1	10.0.0.5/30
R2	FastEthernet0/0	172.16.2.254/24
	Serial0/0/0	10.0.0.2/30
	Serial0/0/1	10.0.0.9/30
R3	FastEthernet0/0	172.16.3.254/24
	Serial0/0/0	10.0.0.6/30
	Serial0/0/1	10.0.0.10/30
PC-NMS	FastEthernet	172.16.2.5/24
PC1	FastEthernet	172.16.3.5/24
PC2	FastEthernet	172.16.3.10/24
Server0	FastEthernet	172.16.1.10/24

**Step 3.** Verify that PC1 has connectivity its default gateway. Click on **PC1 > Desktop** tab > **Command Prompt** > use the **ping 172.16.3.254** command to see if you can get to PC1's default gateway, the R3 router. If you get four (4) request time out messages, return to Step 2. Your IP addressing information is not correct. **DO NOT PROCEED** until you receive the following message: "Reply from 172.16.3.254: bytes=32 time=1ms TTL=255." Note that the time may be 0ms on the second, third, and fourth replies. **ANSWER**

**QUESTION 3.**

**Step 4.** Verify that PC2 has connectivity to the server on the R1 LAN (172.16.1.10). Also verify that PC2 has connectivity to the PC serving as the SNMP manager (172.16.2.5) that collects the data from the agents. Do not proceed if you get a request timed out message on either test. If you get a request timed out message for all four replies (two or three request timed out messages are normal due to ARP), your IP addressing is wrong and you should return to step 2. **ANSWER QUESTION 4.**

**Step 5.** Access the R1 router by clicking on it once > **CLI** tab. Name the router and enable the SNMP service of agent on R1 using the following commands. Note that the ro parameter allows read-only (GET) SNMP access and the rw parameter allows read-write (GET/SET) SNMP access. Also, verify that R1 has connectivity to the NMS manager using the ping command.

```
Router> enable
```

```
Router# configure t
```

```
Router(config)# hostname R1
```

```
R1(config)# snmp-server community public ro
```

```
R1(config)# snmp-server community private rw
```

```
R1(config)# end
```

```
R1# ping 172.16.2.5
```

**ANSWER QUESTION 5.**

**Step 6.** Enable the SNMP service of agent R2 using the same commands as R1 (except don't do the hostname command—you can tell from the prompt that R2 has already had this command applied).

**Step 7.** Enable the SNMP service of agent R3 using the same commands as R1.

**Step 8.** Click once on the PC serving as the NMS manager > **Desktop** tab > **MIB Browser** > **Advanced** button > specify the community strings for R2's address **172.16.2.254** > Read Community is **public** > Write Community is **private** > **OK**. Navigate the MIB tree using the **router\_std MIBs** section to navigate to the **mib-2** section. Remember that you might need to expand the Packet Tracer window, then expand the NMS MIB Browser window, and finally expand the room for the left window within the MIB Browser by clicking on the lines between the two windows in the MIB Browser. When the double lines appear, click and drag the left window to the right to expand. **ANSWER QUESTIONS 6 and 7.**

**Step 9.** Change the MIB Browser on the NMS (using the Advanced button again) to pull information from router R3. You will be required to put an IP address of R3 and the same community information that matches R3. **ANSWER QUESTIONS 8 and 9.**

**Step 10.** Companies frequently have more than one manager in case the PC or server acting as the manager goes down. Configure PC1 or PC2 as the manager. Use the MIB Browser to access router R1. Use the SET command to change the System Contact information through the MIB Browser.

**QUESTION 10 [screenshot]**