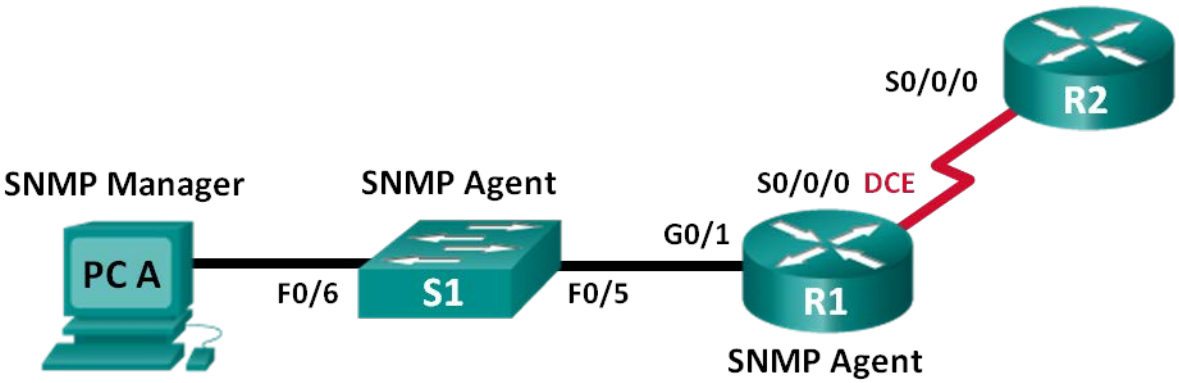
Lab – Configuring SNMP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure an SNMPv2 Manager and Agent

Part 3: Configure an SNMPv3 Manager and Agent

Background / Scenario

Simple Network Management Protocol (SNMP) is a network management protocol and 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 this lab, you will download, install, and configure SNMP management software on PC-A. You will also configure a Cisco router and Cisco switch as SNMP agents. After capturing SNMP notification messages from the SNMP agent, you will convert the MIB/Object ID codes to learn the details of the messages using the Cisco SNMP Object Navigator.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is

shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Note: The **snmp-server** commands in this lab will cause the Cisco 2960 switch to issue a warning message when saving the configuration file to NVRAM. To avoid this warning message verify that the switch is using the **lanbase-routing** template. The IOS template is controlled by the Switch Database Manager (SDM). When changing the preferred template, the new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **lanbase-routing** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end
S1# reload
```

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS, Release 15.4(3) universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows with terminal emulation program, such as Tera Term, SNMP manager, such as SNMP MIB Browser by ManageEngine, and Wireshark)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology
- SNMP Management Software (SNMP MIB Browser by ManageEngine)

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the devices with basic settings.

Step 1: Cable the network as shown in the topology.

Step 2: Configure the PC host.

Step 3: Initialize and reload the switch and routers as necessary.

Step 4: Configure basic settings for the routers and switch.

a. Disable DNS lookup.

b. Configure device names as shown in the topology.

c. Configure IP addresses as shown in the Addressing Table. (Do not configure or enable the VLAN 1 interface on S1 at this time.)

d. Assign **cisco** as the console and vty password and enable login.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Configure **logging synchronous** to prevent console messages from interrupting command entry.

g. Verify successful connectivity between PC-A and R1 and between the routers by issuing the **ping** command.

h. Copy the running configuration to the startup configuration.

Part 2: Configure SNMPv2 Manager and Agent

In Part 2, SNMP management software will be installed and configured on PC-A, and R1 and S1 will be configured as SNMP agents.

Step 1: Install an SNMP management program.

a. Download and install the SNMP MIB Browser by ManageEngine from the following URL: https://www.manageengine.com/products/mibbrowser-free-tool/download.html. You will be asked to provide an email address to download the software.

b. Launch the ManageEngine MibBrowser program.

1) If you receive an error message regarding the failure to load MIBs. Navigate to the MibBrowser Free Tool folder:

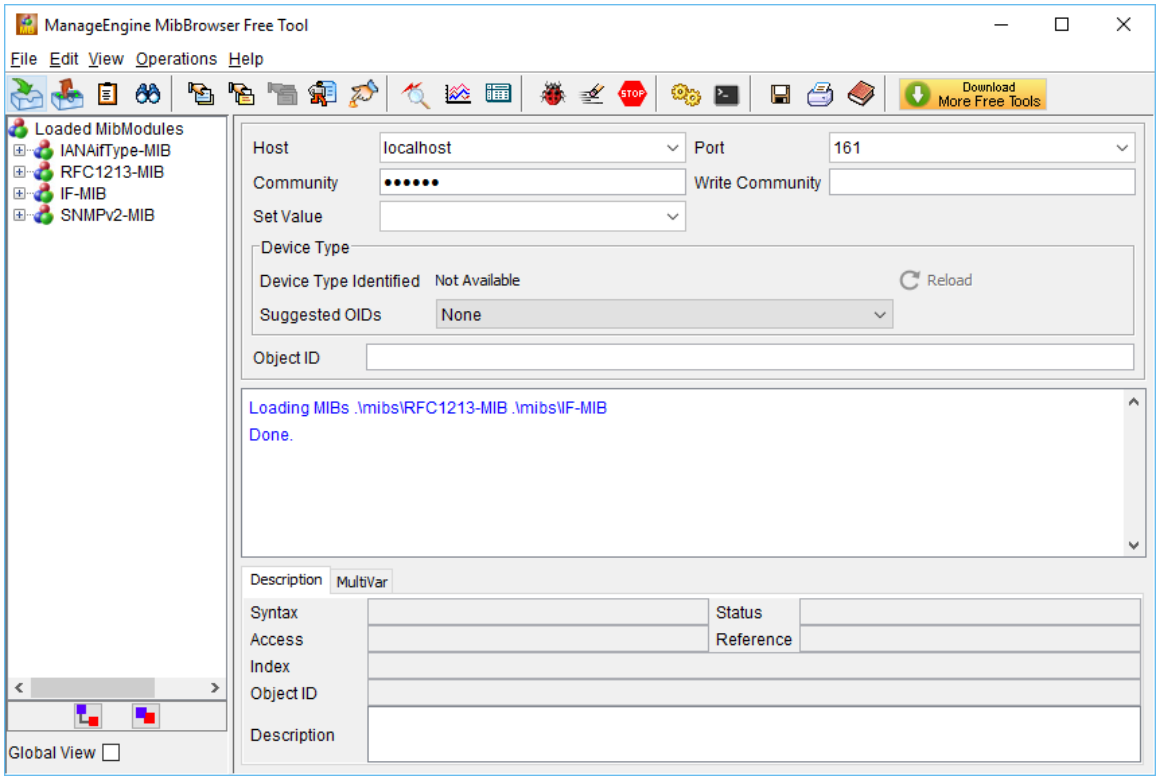
32bit: C:\Program Files (x86)\ManageEngine\MibBrowser Free Tool

64bit: C:\Program Files\ManageEngine\MibBrowser Free Tool

2) Right-click the **mibs** folder, Properties, and select the **Security** tab. Click **Edit**. Select **Users**. Check the **Modify** under **Allow** column. Click **OK** to change the permission.

3) Repeat the previous step with the **conf** folder.

4) Launch the ManageEngine MibBrowser program again.



Step 2: Configure a SNMPv2 agent.

On S1, enter the following commands from the global configuration mode to configure the switch as an SNMP agent. In line 1 below, the SNMP community string is **ciscolab**, with read-only privileges, and the named access list SNMP_ACL defines which hosts are allowed to get SNMP information from S1. 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, and lines 6 and 7 create the named access list, to control which hosts are permitted to get SNMP information from the switch.

```
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server location Company_HQ
S1(config)# snmp-server contact admin@company.com
S1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
S1(config)# snmp-server enable traps
S1(config)# ip access-list standard SNMP_ACL
S1(config-std-nacl)# permit 192.168.1.3
```

Step 3: Verify the SNMPv2 settings.

Use the **show** commands to verify the SNMPv2 settings.

```
S1# show snmp
Chassis: FCQ1628Y5MG
Contact: admin@company.com
Location: Company_HQ
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 192.168.1.3.162, 0/10, 0 sent, 0 dropped.
SNMP agent enabled

S1# show snmp community

Community name: ciscolab
Community Index: ciscolab
```

```
Community SecurityName: ciscolab
storage-type: nonvolatile        active access-list: SNMP_ACL
<output omitted>
```

What is the configured SNMP community?

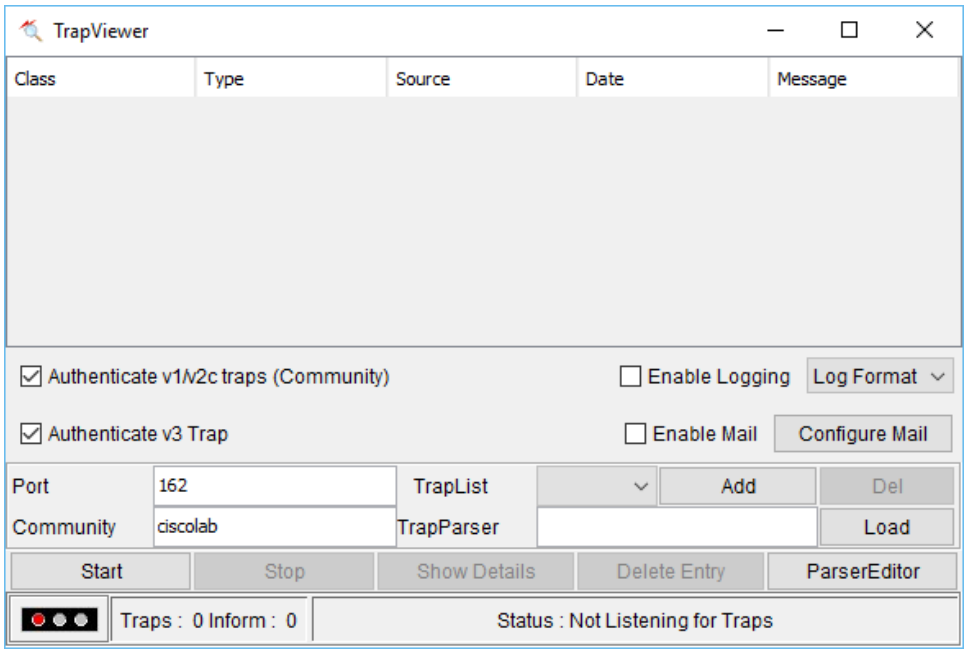
Step 4: Enable SNMP trap.

In this step, you will start the SNMP trap and observe the messages when you configure and enable SVI on VLAN 1 for S1.

a. In the MibBrowser, click **Edit** > **Settings**. Verify that **v2c** is selected as the SNMP Version. Click **OK** to continue.

b. Click **Trap Viewer UI** ( ).

c. Verify **162** is the Port number and configure **ciscolab** as the Community.



d. Click **Start** after you have verified the settings. The TrapList field displays **162:ciscolab**.

e. To generate SNMP messages, configure and enable SVI on S1. Use the IP address **192.168.1.2 /24** for VLAN 1 and disable and enable the interface.

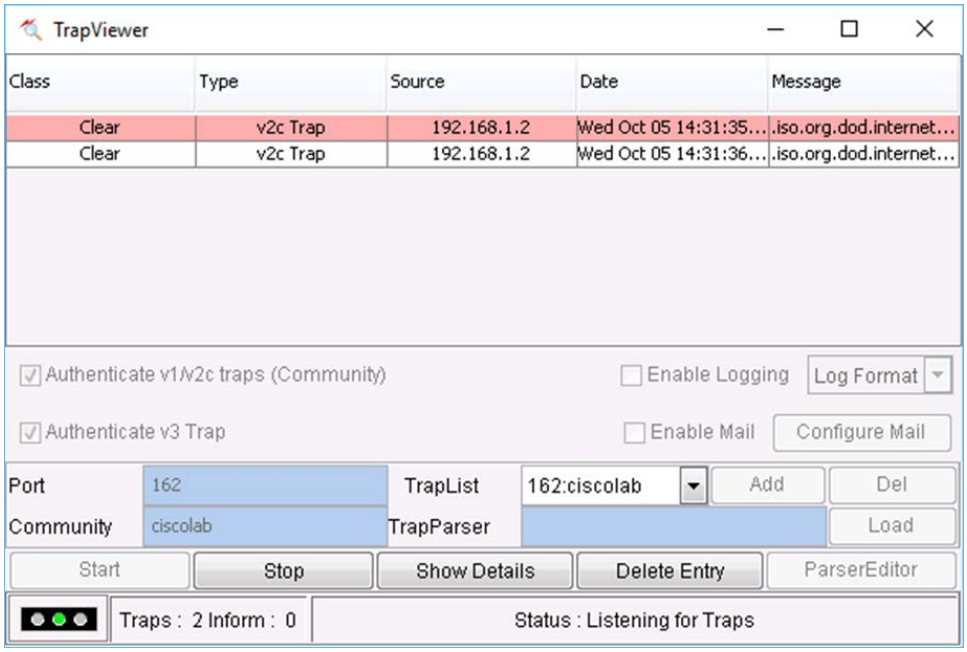
f. Enter the **show snmp** command to verify the SNMP messages were sent.

```
S1# show snmp
Chassis: FCQ1628Y5MG
Contact: admin@company.com
Location: Company_HQ
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
```

```
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
        0 Input queue packet drops (Maximum queue size 1000)
    2 SNMP packets output
        0 Too big errors (Maximum packet size 1500)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        2 Trap PDUs
    SNMP global trap: enabled

    SNMP logging: enabled
        Logging to 192.168.1.3.162, 0/10, 2 sent, 0 dropped.
    SNMP agent enabled
    SNMP agent enabled
```

g. Navigate to the **TrapViewer**. View the messages that have been trapped by MibBrowser. To see the details of each message, click **Show Details**.



Part 3: Configure SNMPv3 Manager and Agent

Step 1: Configure a SNMPv3 agent on R1.

On R1, enter the following commands from the global configuration mode to configure the router as an SNMP agent. In lines 1 – 3 below, a standard ACL named PERMIT-ADMIN permits only the hosts of the network 192.168.1.0 /24 to access the SNMP agent running on R1. Line 4 configures an SNMP view, SNMP-RO, and

it includes the iso tree from the MIB. In line 5, an SNMP group is configured with the name ADMIN, is set to SNMPv3 with authentication and encryption required, and only allows access limit to hosts permitted in the PERMIT-ADMIN ACL. Line 5 defines a user named USER1 with the group ADMIN. Authentication is set to use SHA with the password cisco12345 and encryption is set for AES 128 with cisco54321 as the configured password.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user USER1 ADMIN v3 auth sha cisco12345 pri aes 128
cisco54321
R1(config)#
*Aug  5 02:52:50.715: Configuring snmpv3 USM user, persisting
snmpEngineBoots. Please Wait...
```

Step 2: Verify a SNMPv3 configuration on R1.

Use the **show** commands to verify the SNMPv3 settings.

```
R1# show run | include snmp
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included

R1# show snmp user

User name: USER1
Engine ID: 800000090300D48CB5CEA0C0
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN
```

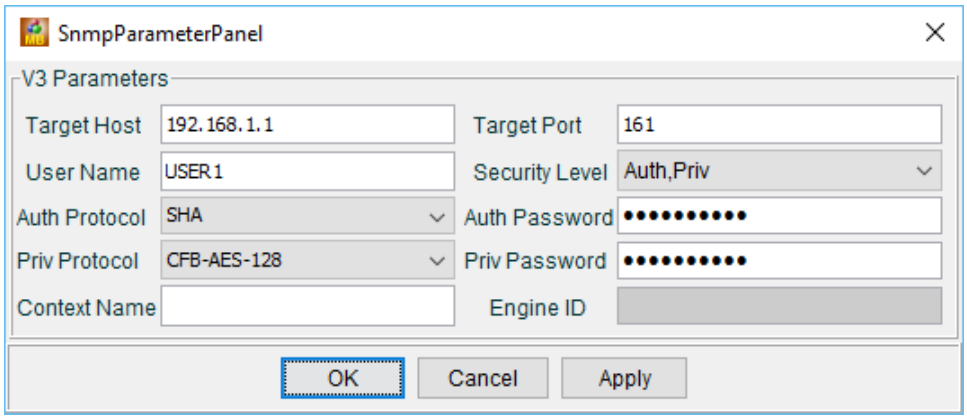
Step 3: Configure SNMP manager access to the SNMPv3 agent.

a. Navigate to PC-A Open **Wireshark**. Start a live capture on the appropriate interface.

b. Enter **snmp** in the Filter field.

c. In the MibBrowser, click **Edit** > **Settings**. Select **v3** for SNMP Version. Then click **Add**.

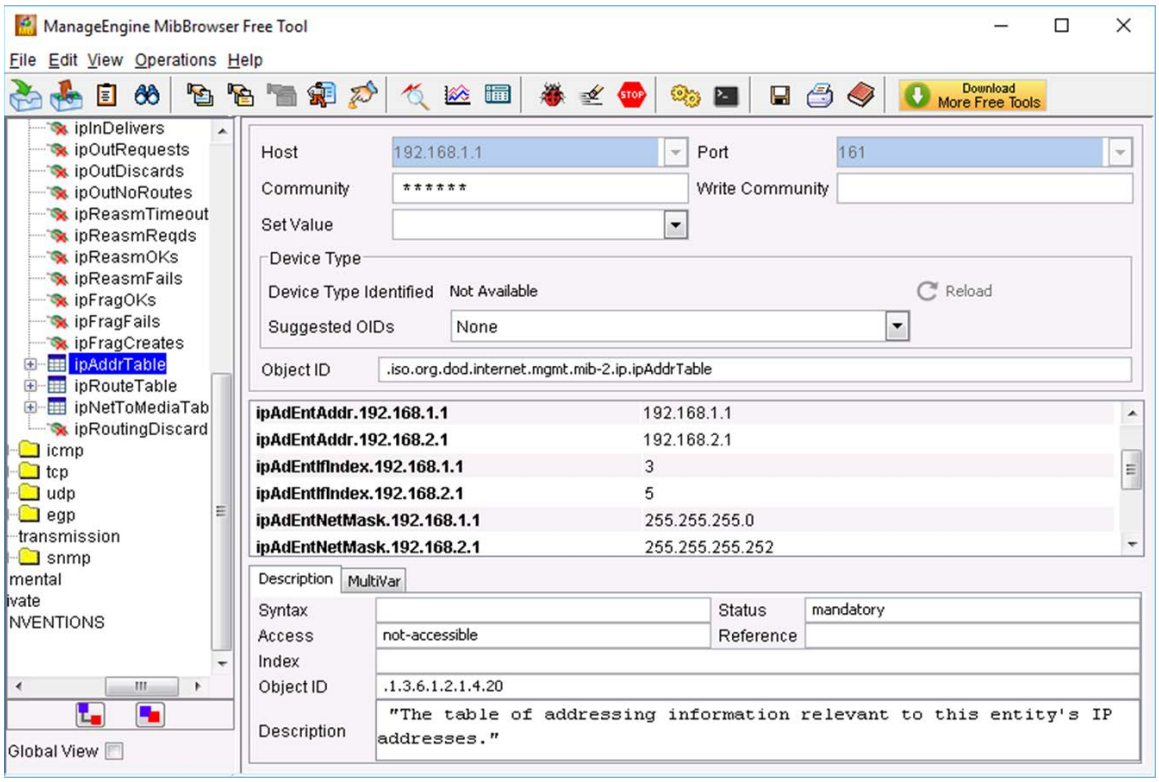
d. Enter the SNMPv3 settings that were configured on R1. Click **OK** to continue.



SNMPv3 Parameters	Settings
Target Host	192.168.1.1
User Name	USER1
Auth Protocol	SHA
Priv Protocol	CFB-AES-128
Target Port	161
Security Level	Auth,Priv
Auth Password	cisco12345
Priv Password	cisco54321

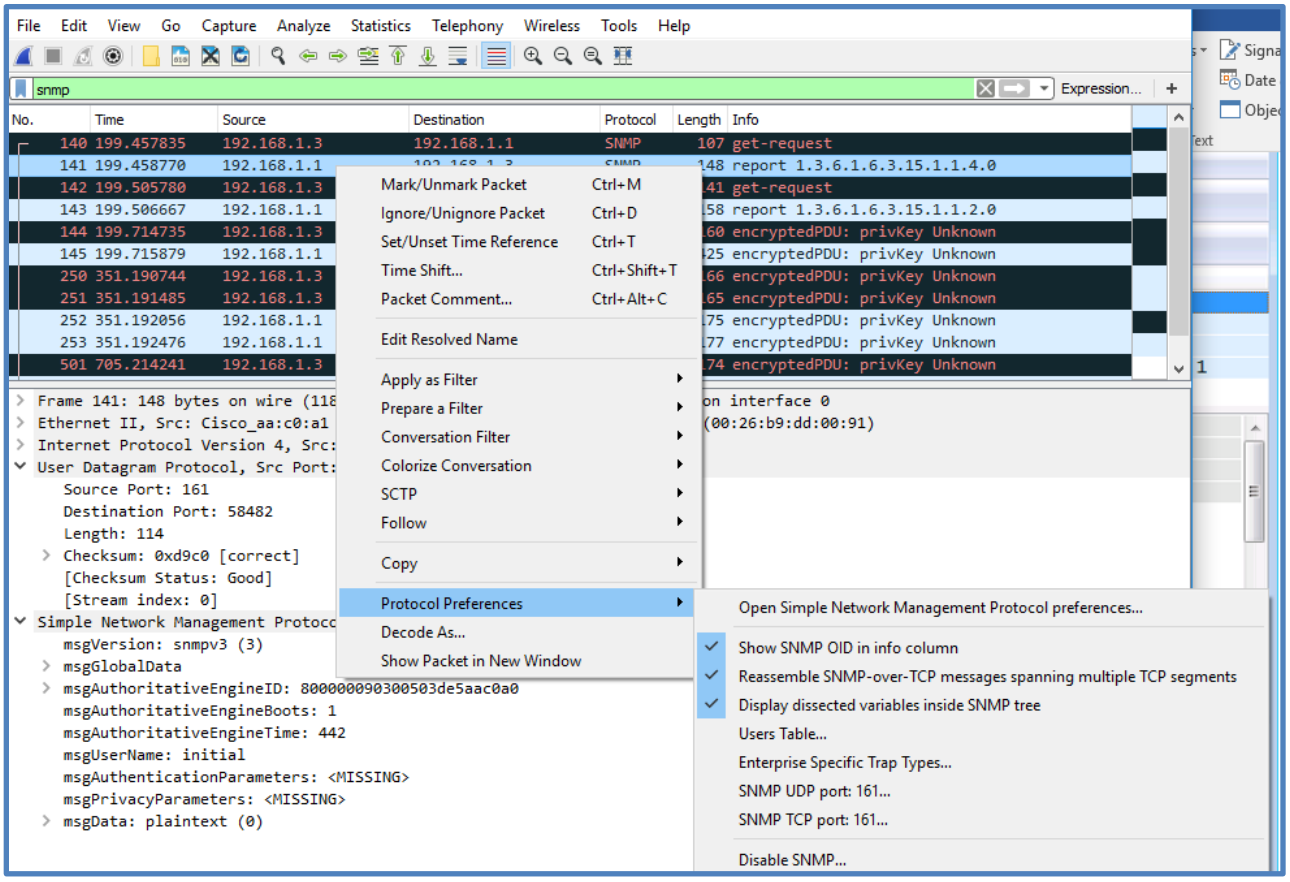
e. Click **Edit** > **Find Node**. Enter **ipAddrTable** in the Find What field and click **Close**. Verify **ipAddrTable** is selected in the left panel and **.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable** is listed in the ObjectID field.

f. Click **Operation** > **GET** to get all the objects under the select MIB object, **ipAddrTable** in this instance.

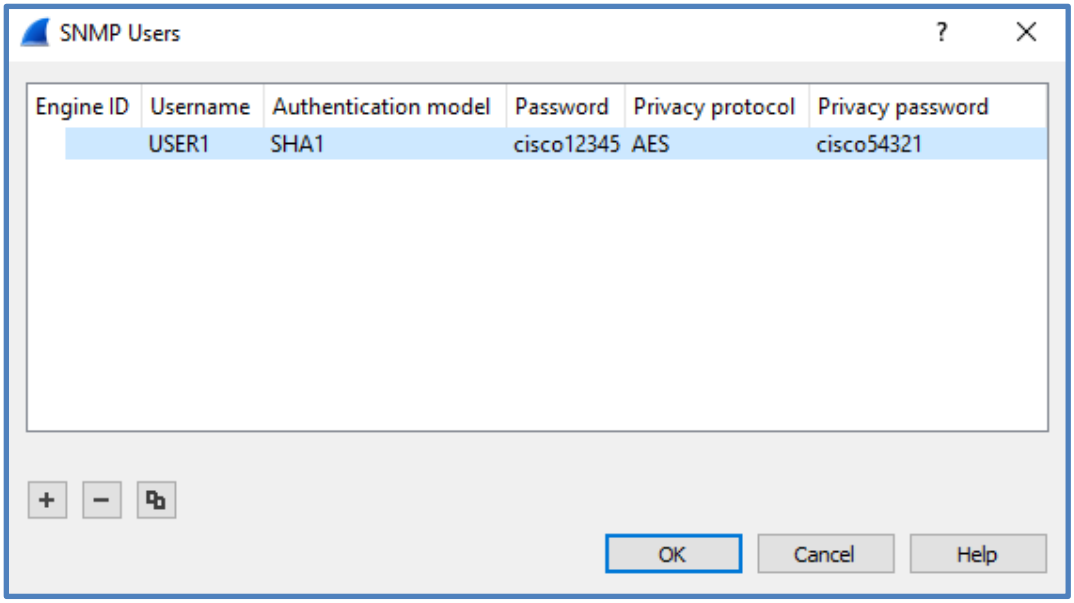


g. Navigate back to the Wireshark screen. Stop the live capture.

h. In the Results panel, right-click one of the results. Select **Protocol Preferences > Open Simple Network Management Protocol Preferences**.

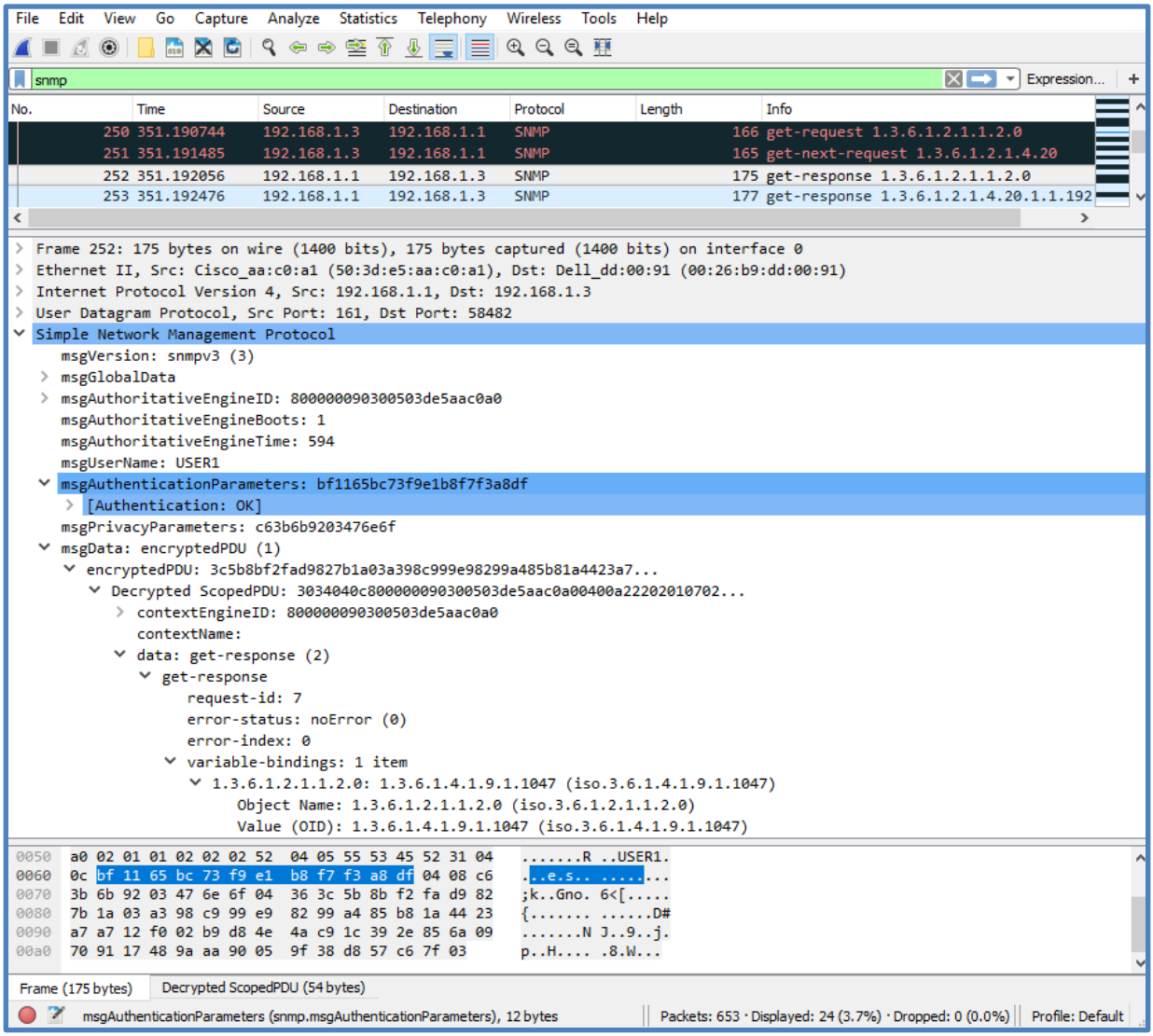


i. Click **Edit** for the Users Table. Click **New** and enter user information in Step 1. Click **OK**.



j. Click **OK** to accept the user information. Click **OK** again to exit the Wireshark Preferences window.

k. Select one of the lines. Expand the SNMP result and view the decrypted messages.



Step 4: Review your results.

What are the IP addresses configured on R1 in the SNMPv3 results?

Compare the Wireshark decrypted SNMP packets and MIB Browser results. Record your observations.

Reflection

1. What are some of the potential benefits of monitoring a network with SNMP?

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

3. What are the benefits of using SNMPv3 over SNMPv2?

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.