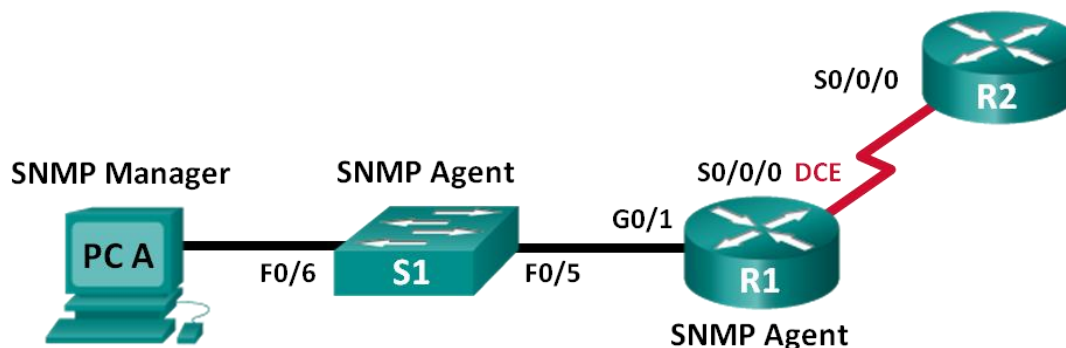


Lab – Configuring SNMP

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 SNMP Manager and Agents

Part 3: Convert OID Codes with the Cisco SNMP Object Navigator

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 15.2(4)M3 (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 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- 1 PC (Windows 7, Vista, or XP with Internet access)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology
- SNMP Management Software (PowerSNMP Free Manager by Dart Communications, or SolarWinds Kiwi Syslog Server, Evaluation Version with 30 Day Trial)

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.

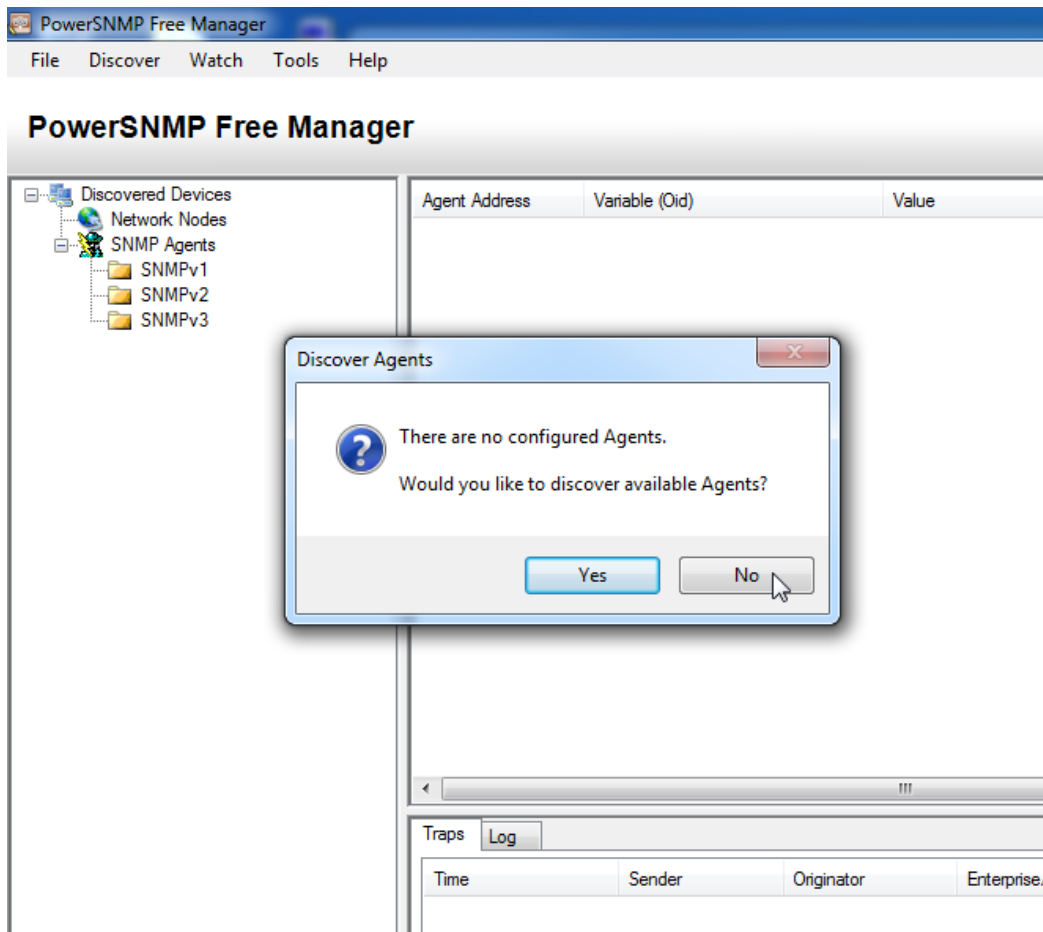
- Disable DNS lookup.
- Configure device names as shown in the topology.
- Configure IP addresses as shown in the Addressing Table. (Do not configure the S0/0/0 interface on R1 at this time.)
- Assign **cisco** as the console and vty password and enable login.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Verify successful connectivity between the LAN devices by issuing the ping command.
- Copy the running configuration to the startup configuration.

Part 2: Configure SNMP Manager and Agents

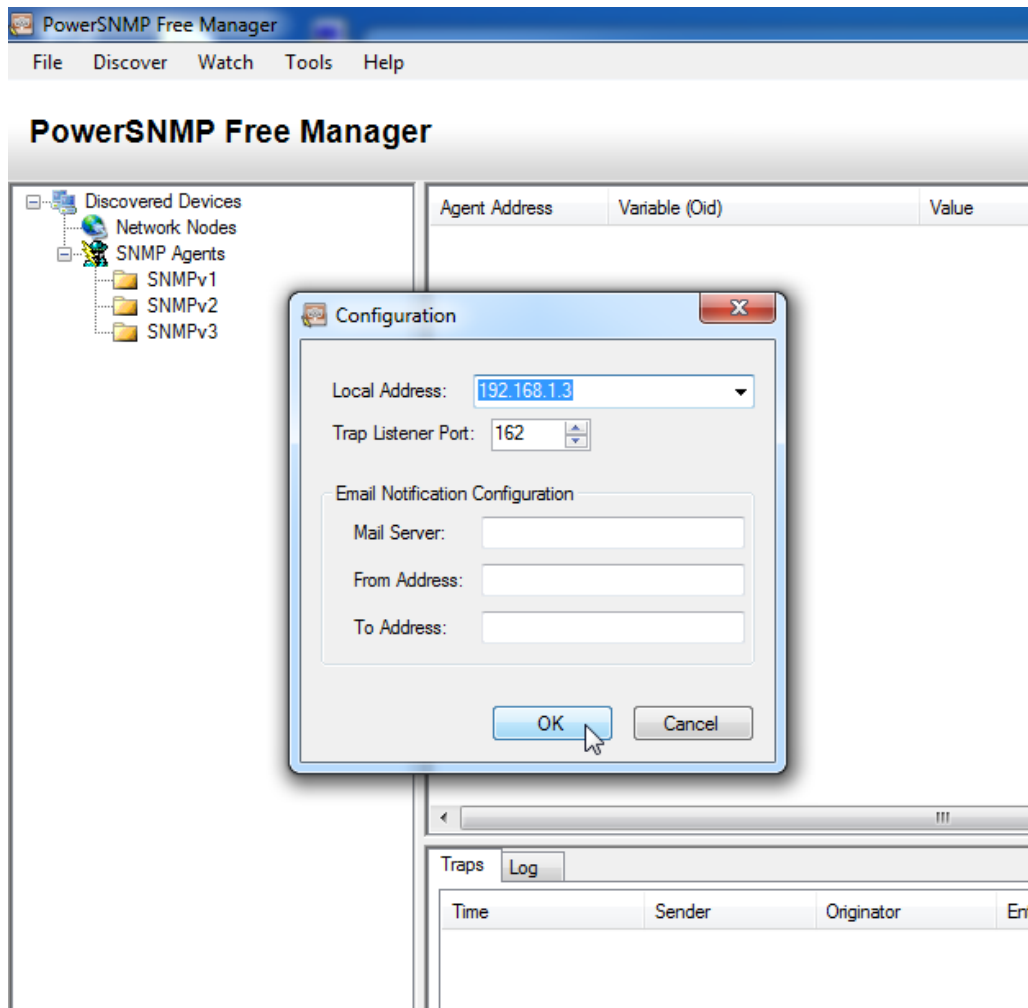
In Part 2, SNMP management software will be installed and configured on PC-A, and R1 and S1 will be configured as SNMP agents.

Step 1: Install an SNMP management program.

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



- In the pop-up Configuration window (if no pop-up window appear, go to Tools > Configuration), set the local IP address to listen on 192.168.1.3 and click **OK**.



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

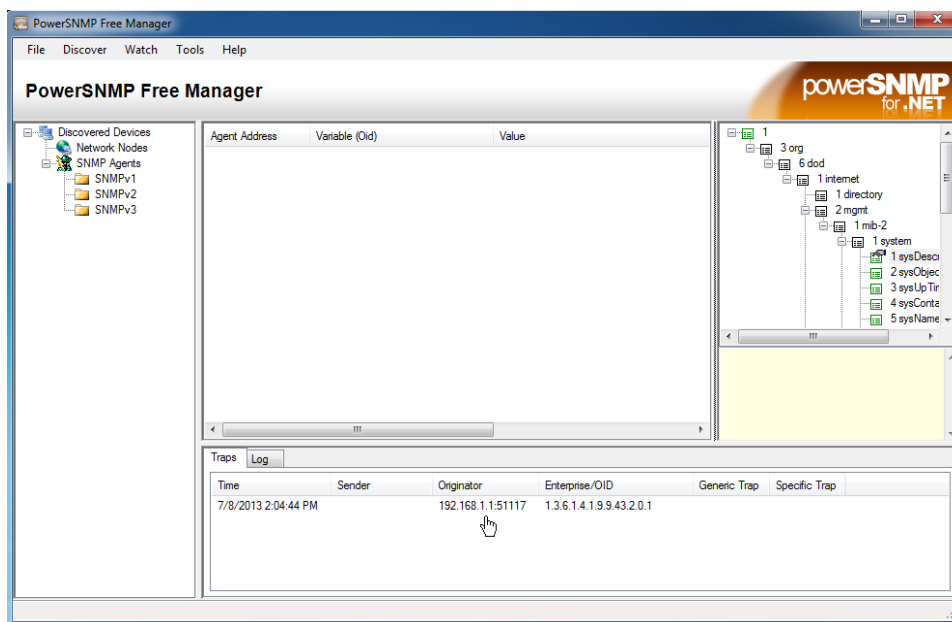
Step 2: Configure an SNMP agent.

- 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 **ciscolab**, with read-only privileges, and the named access list **SNMP_ACL** defines which hosts are allowed to get SNMP information from R1. 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 router.

```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

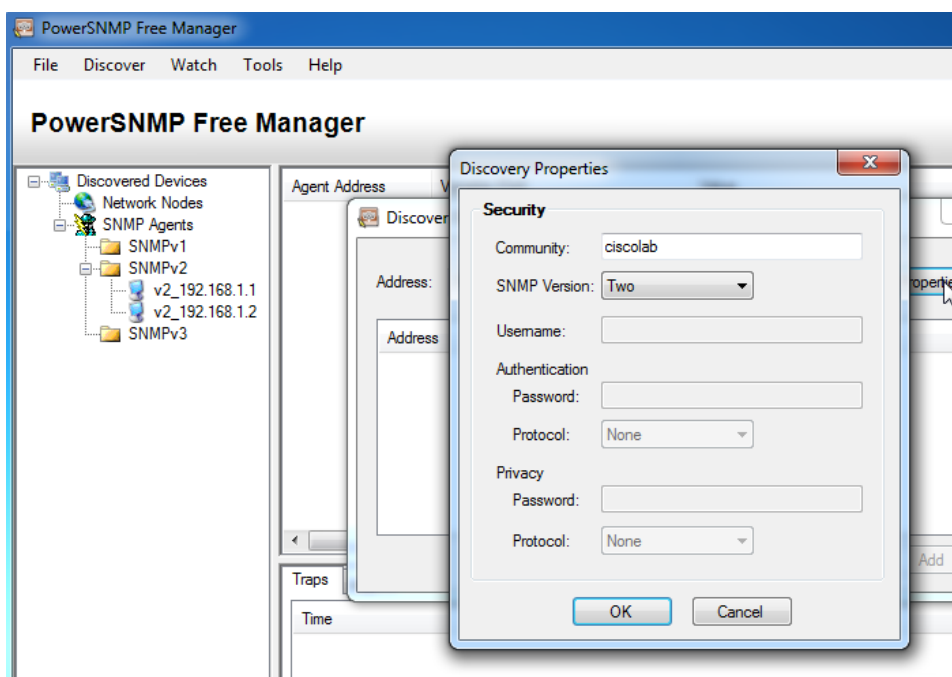
Lab – Configuring SNMP

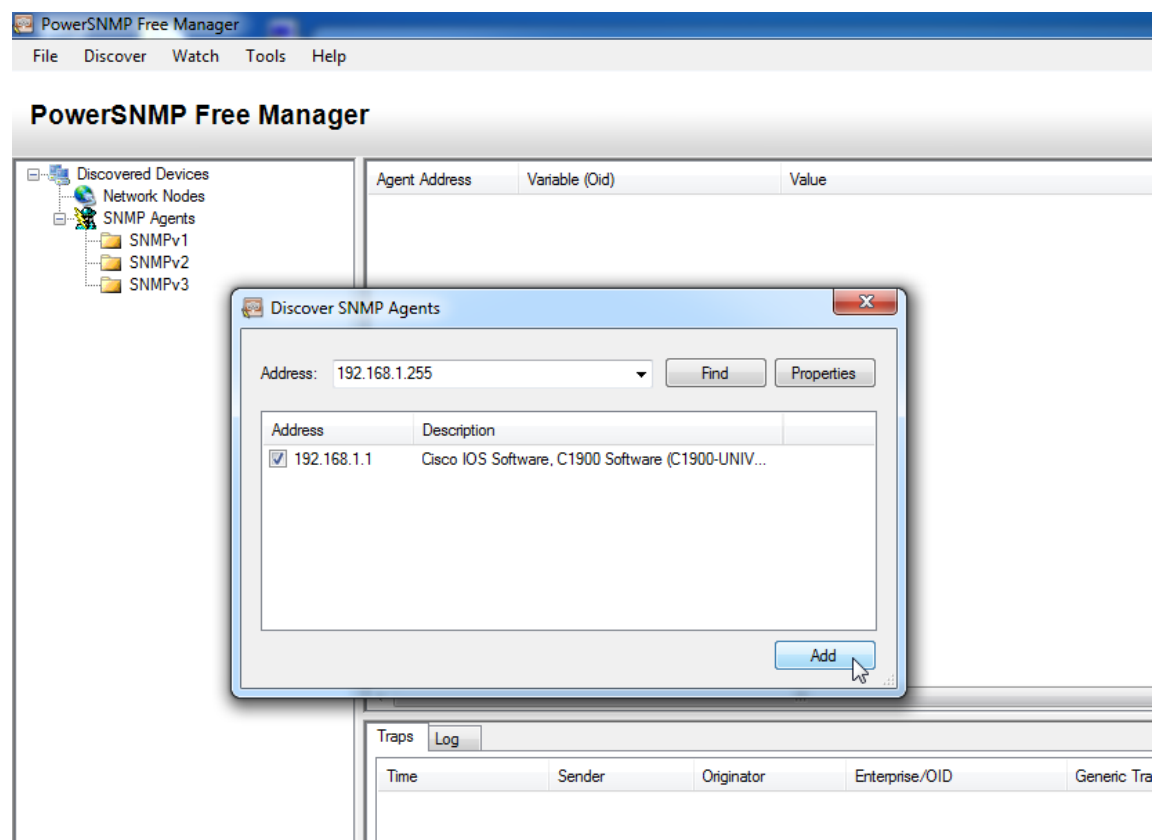
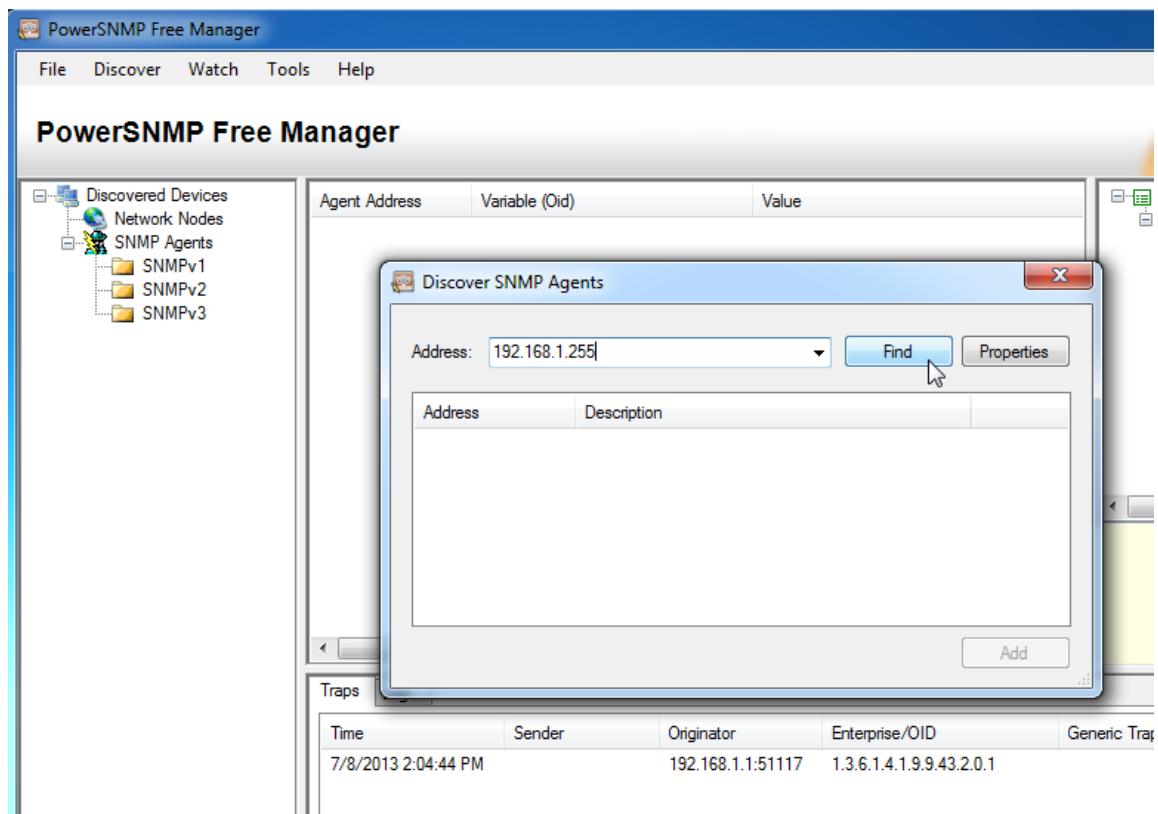
- b. At this point, you may notice that the PowerSNMP Free Manager is receiving notifications from R1. If it is not, you can try to force a SNMP notification to be sent by entering a **copy run start** command on R1. Continue to the next step if it is unsuccessful.



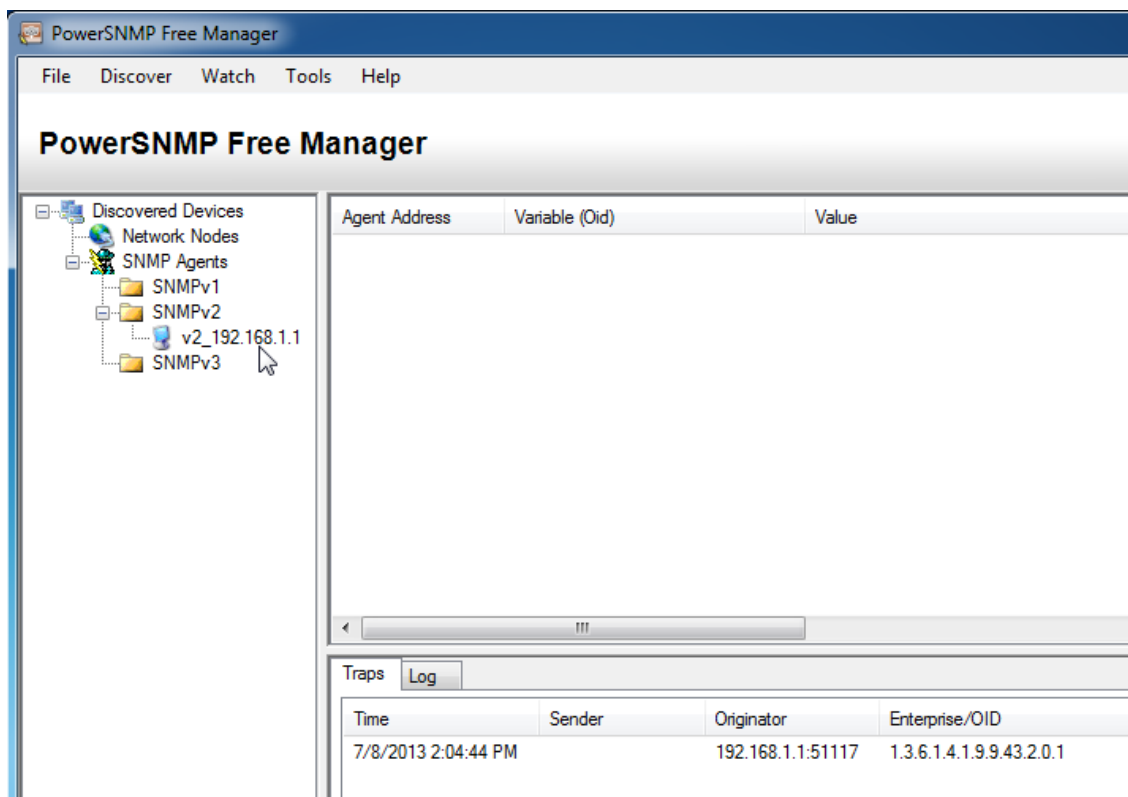
Step 3: Discover SNMP agents.

- a. From the PowerSNMP Free Manager on PC-A, open the **Discover > SNMP Agents** window. Enter the IP address **192.168.1.255**. In the same window, click **Properties** and set the Community to **cisco1ab** and the SNMP Version to **Two**, and then click **OK**. Now you can click **Find** to discover all SNMP agents on the 192.168.1.0 network. The PowerSNMP Free Manager should find R1 at 192.168.1.1. 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.



- c. Configure S1 as an SNMP agent. You can use the same **snmp-server** commands that you used to configure R1.
- d. After S1 is configured, SNMP notifications from 192.168.1.2 display in the Traps window of the PowerSNMP Free Manager. In the PowerSNMP Free Manager, add S1 as an SNMP agent using the same process that you used to discover R1.

Part 3: Convert OID Codes with the Cisco SNMP Object Navigator

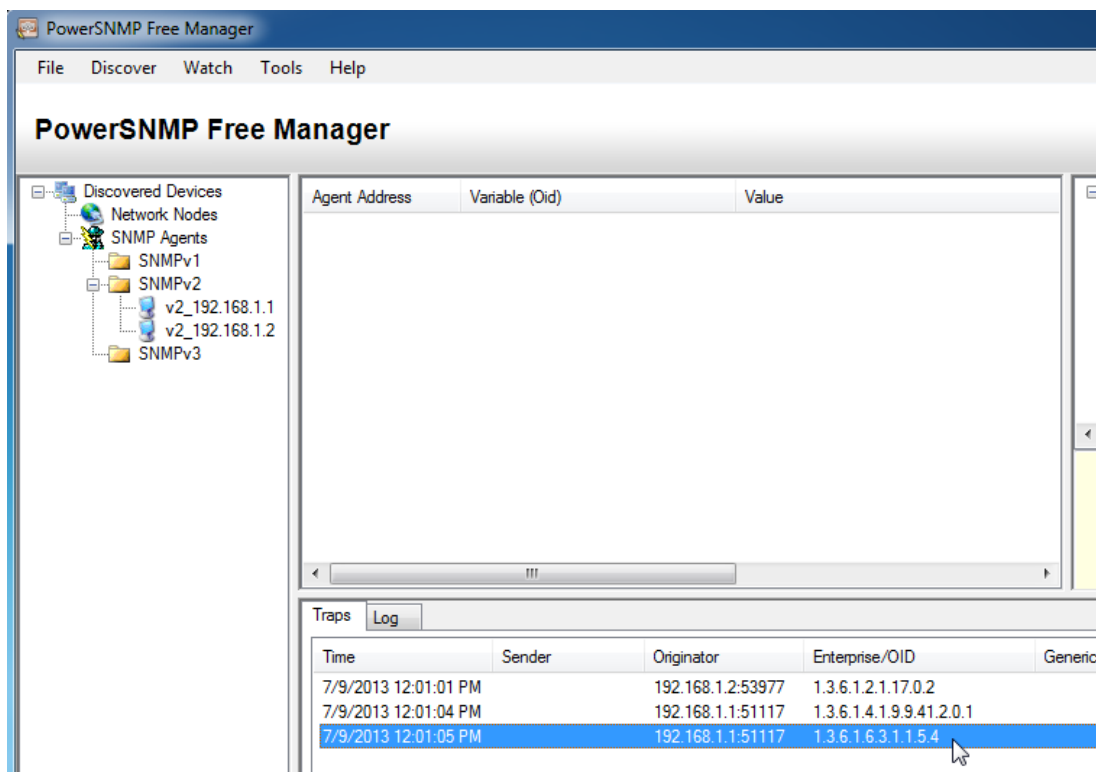
In Part 3, you will force SNMP notifications to be sent to the SNMP manager located at PC-A. You will then convert the received OID codes to names to learn the nature of the messages. The MIB/OID codes can be easily converted using the Cisco SNMP Object Navigator located at <http://www.cisco.com>.

Step 1: Clear current SNMP messages.

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

Step 2: Generate an SNMP trap and notification.

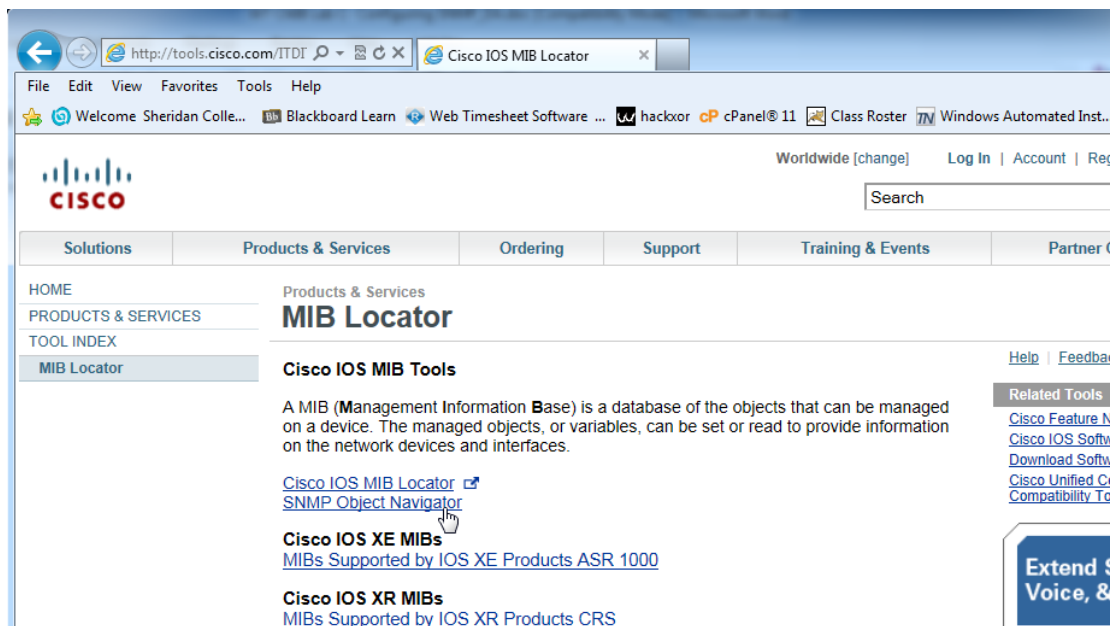
On R1, configure the S0/0/0 interface according to the Addressing Table at the beginning of this lab. Accessing global configuration mode and enable an interface to generate an SNMP trap notification to be sent to the SNMP Manager at PC-A. Notice the Enterprise/OID code numbers that are visible in the traps window.



Step 3: Decode SNMP MIB/OID messages.

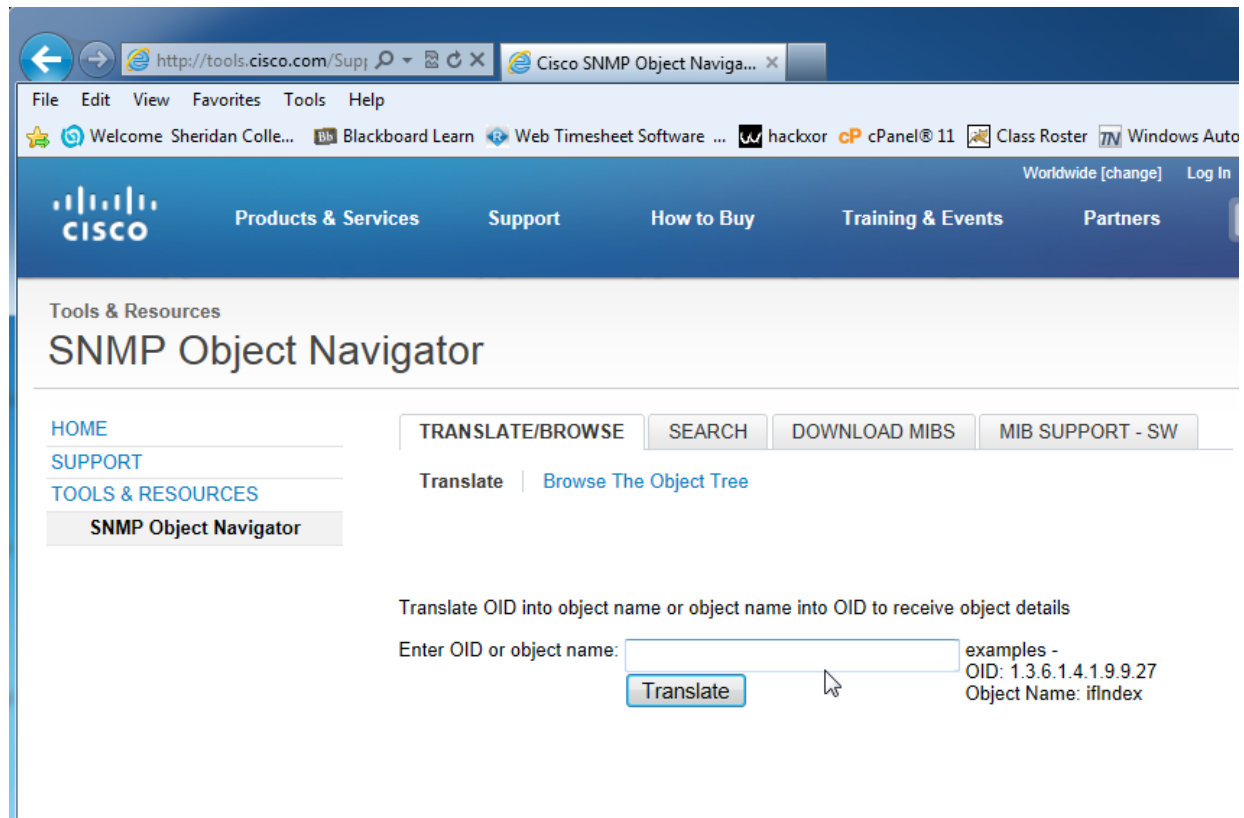
From a computer with Internet access, open a web browser and go to <http://www.cisco.com>.

- Using the search tool at the top of the window, search for **SNMP Object Navigator**.
- Choose **SNMP Object Navigator MIB Download MIBs OID OIDs** from the results.
- Navigate to the **MIB Locator** page. Click the **SNMP Object Navigator**.



Lab – Configuring SNMP

- d. Using the **SNMP Object Navigator** page, decode the OID code number from the PowerSNMP Free Manager generated in Part 3, Step 2. Enter the OID code number and click **Translate**.



- e. Record the OID code numbers and their corresponding message translations below.

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?

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) |
| <p>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.</p> | | | | |