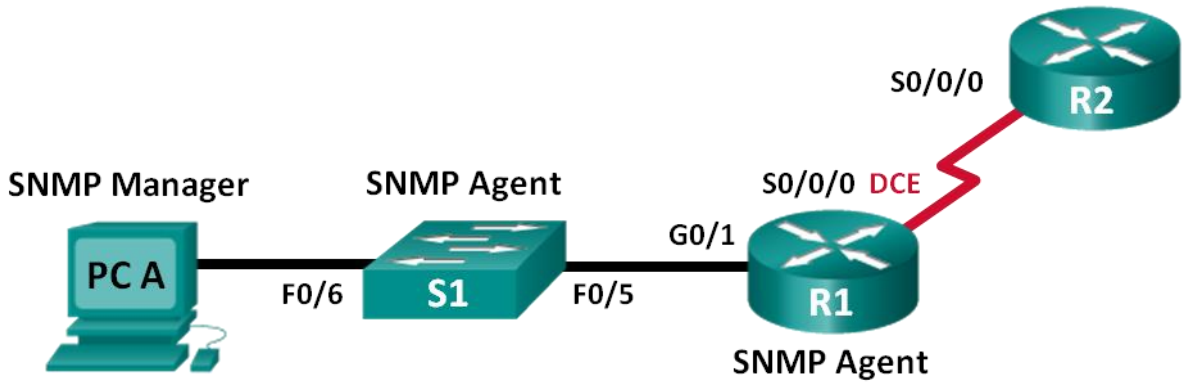
Lab – Configuring SNMP (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

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.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

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.

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 the S0/0/0 interface on R1 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 the LAN devices by issuing the ping command.

h. Copy the running configuration to the startup configuration.

Part 2: Configure SNMP Manager and Agents

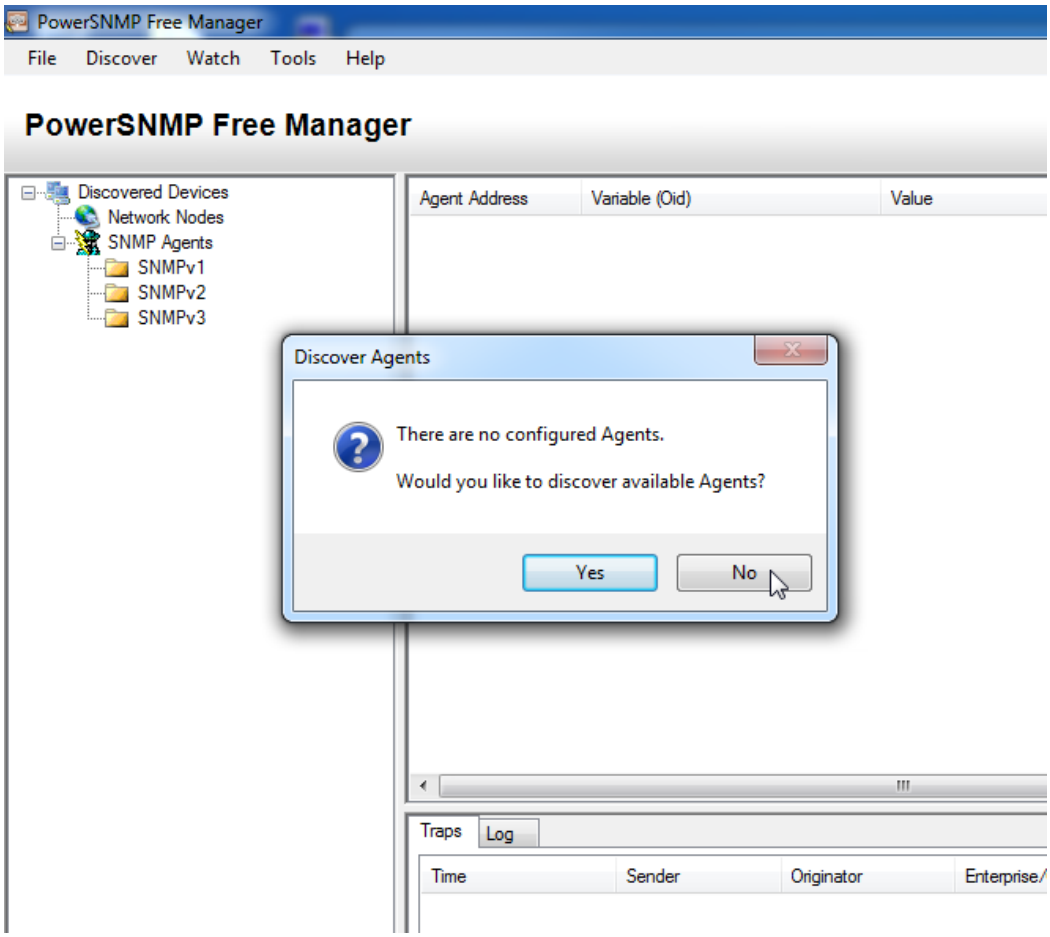
In Part 2, SNMP management software will be installed and configured on PC-A, and R1 and S1 will be configured as SNMP agents.

Step 1: Install an SNMP management program.

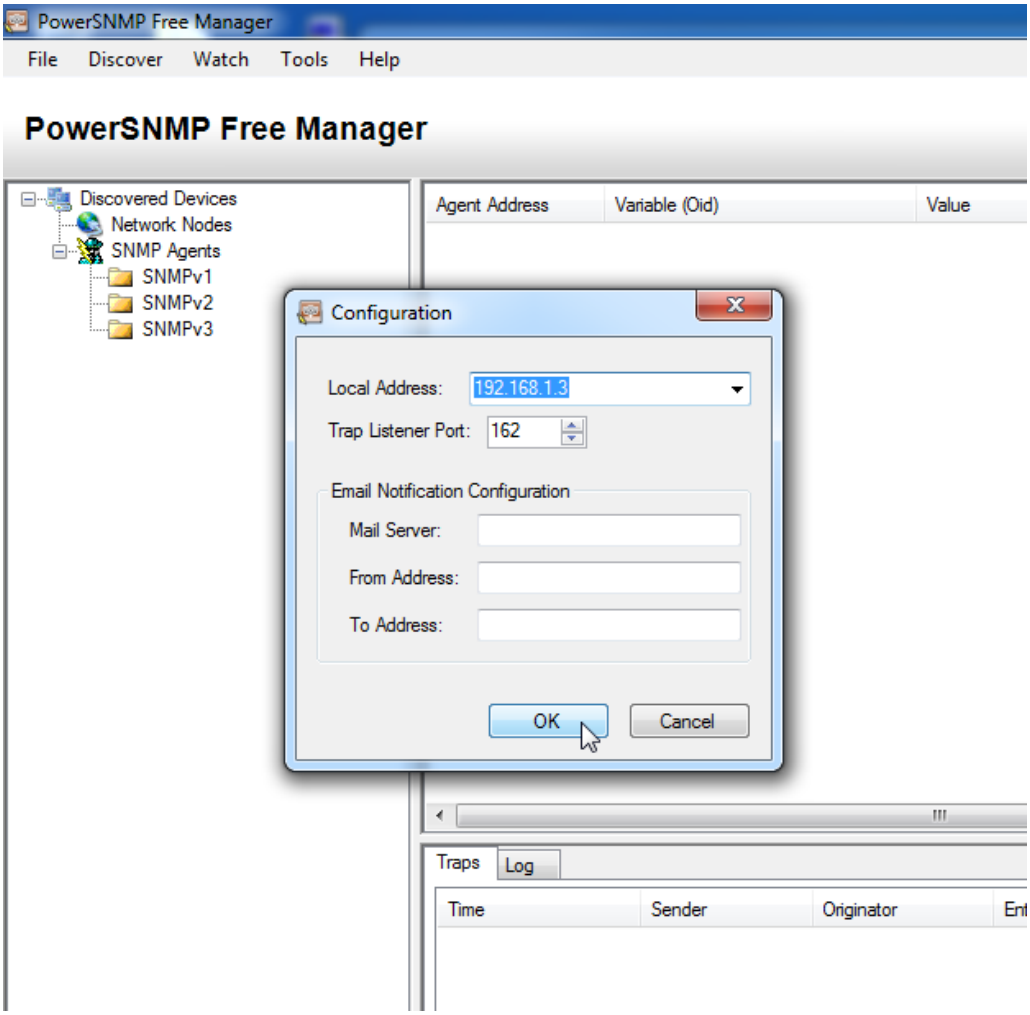
a. Download and install the PowerSNMP Free Manager by Dart Communications from the following URL: http://www.dart.com/snmp-free-manager.aspx.

b. Launch the PowerSNMP Free Manager program.

c. 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.



d. 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**.



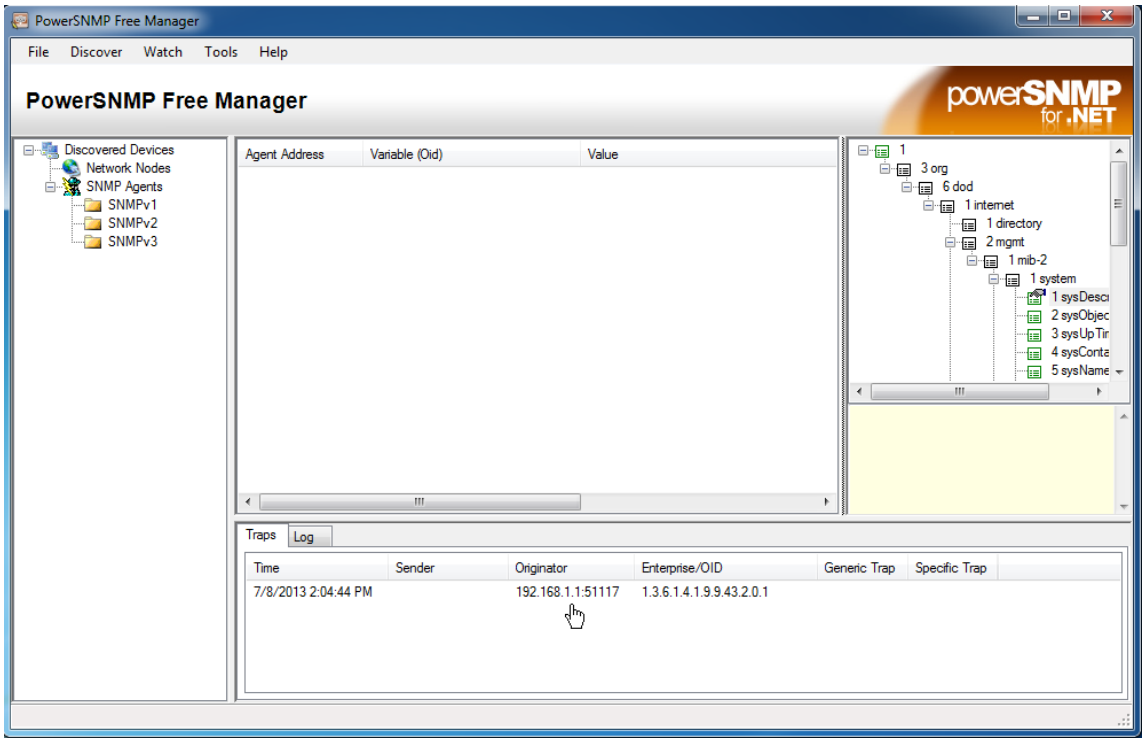
Note: If prompted to discover available SNMP agents, click **No** and continue to next part of the lab.

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.

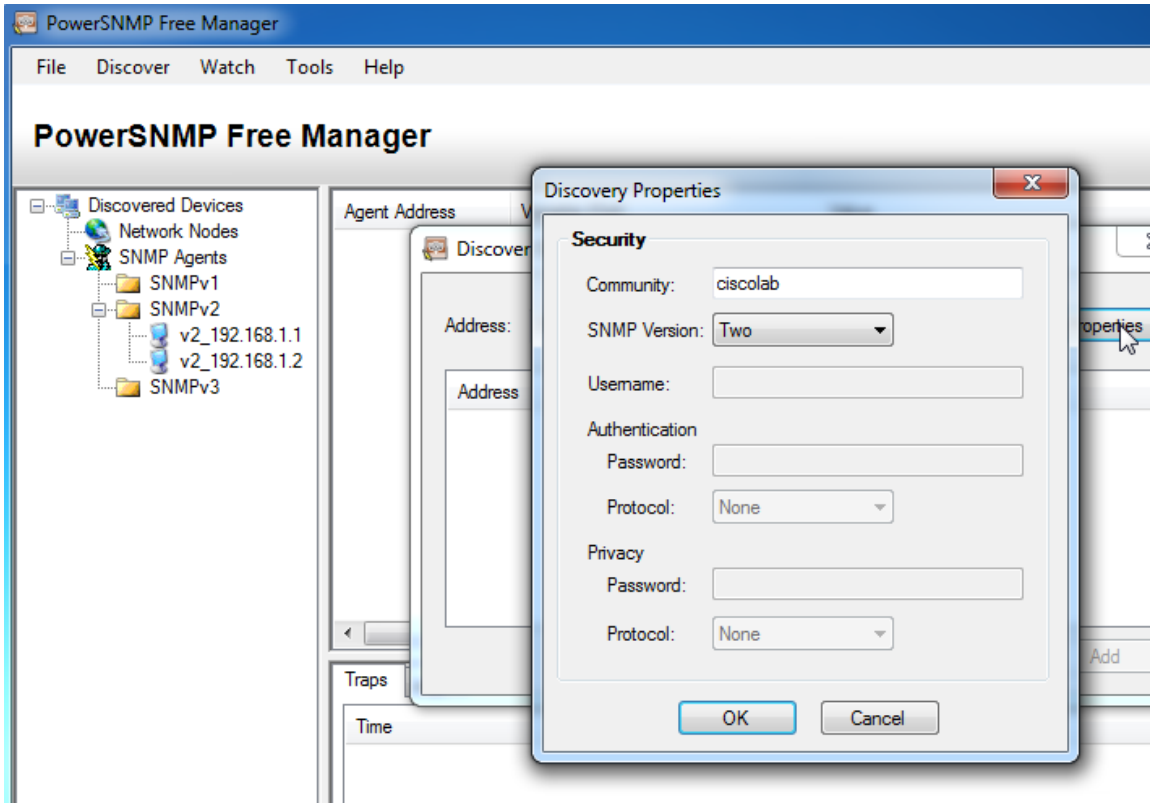
```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)#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

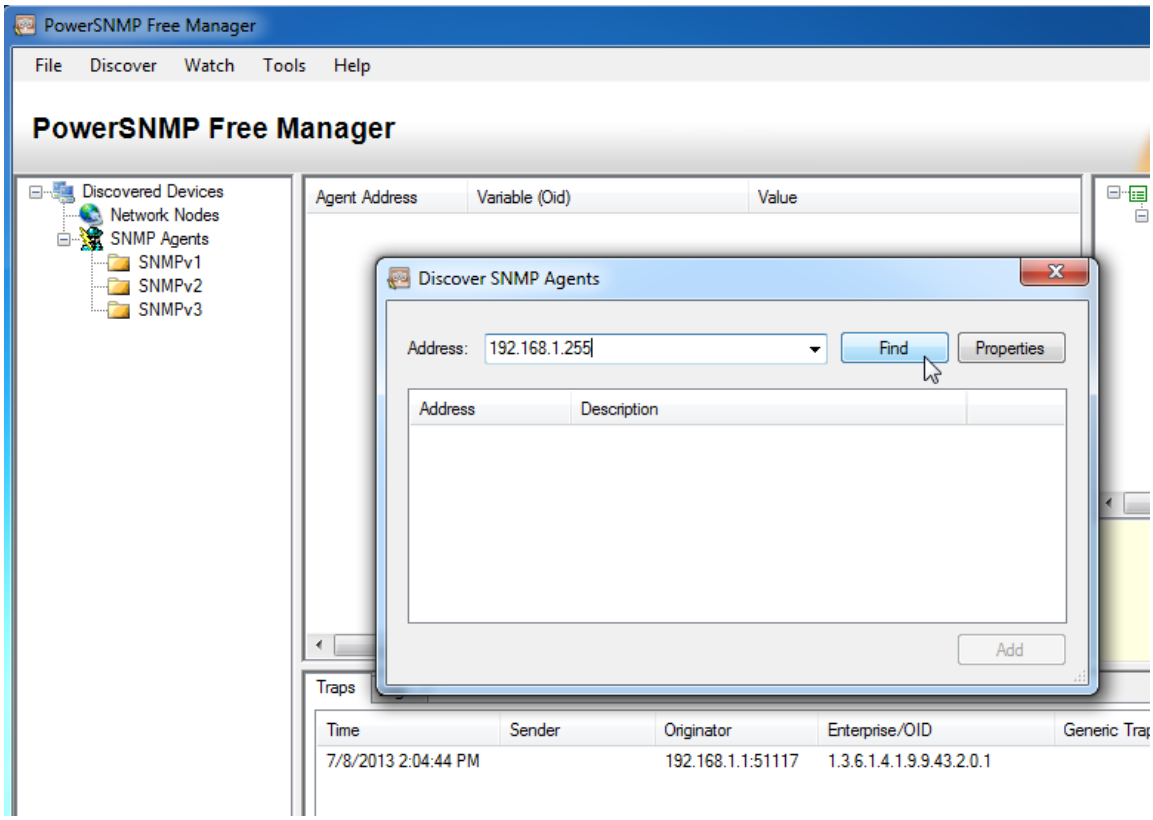
b. At this point, you may notice that the PowerSNMP Free Manager is receiving notifications from R1. If it is not, you can try to force a SNMP notification to be sent by entering a **copy run start** command on R1. Continue to the next step if it is unsuccessful.

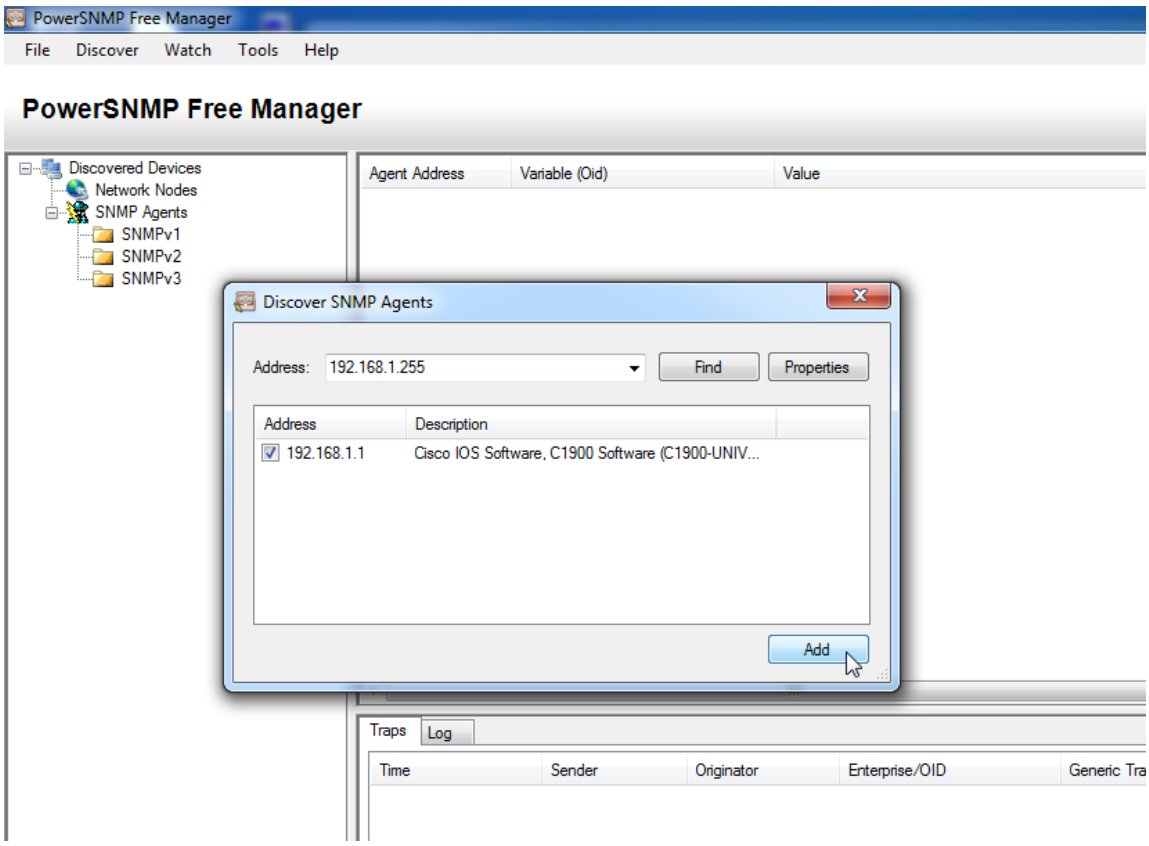


Step 3: Discover SNMP agents.

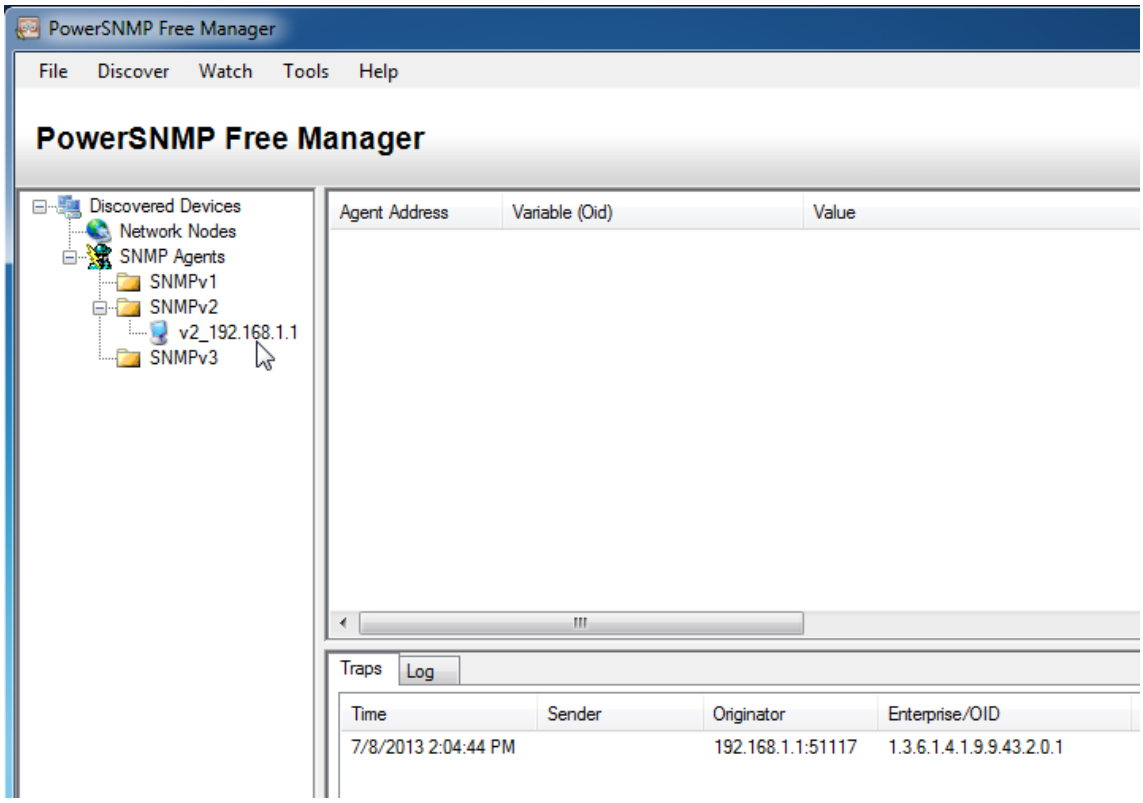
a. From the PowerSNMP Free Manager on PC-A, open the **Discover > SNMP Agents** window. Enter the IP address **192.168.1.255**. In the same window, click **Properties** and set the Community to **ciscolab** and the SNMP Version to **Two**, and then click **OK**. Now you can click **Find** to discover 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.

```
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server location snmp_manager
S1(config)# snmp-server contact ciscolab_admin
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
```

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.

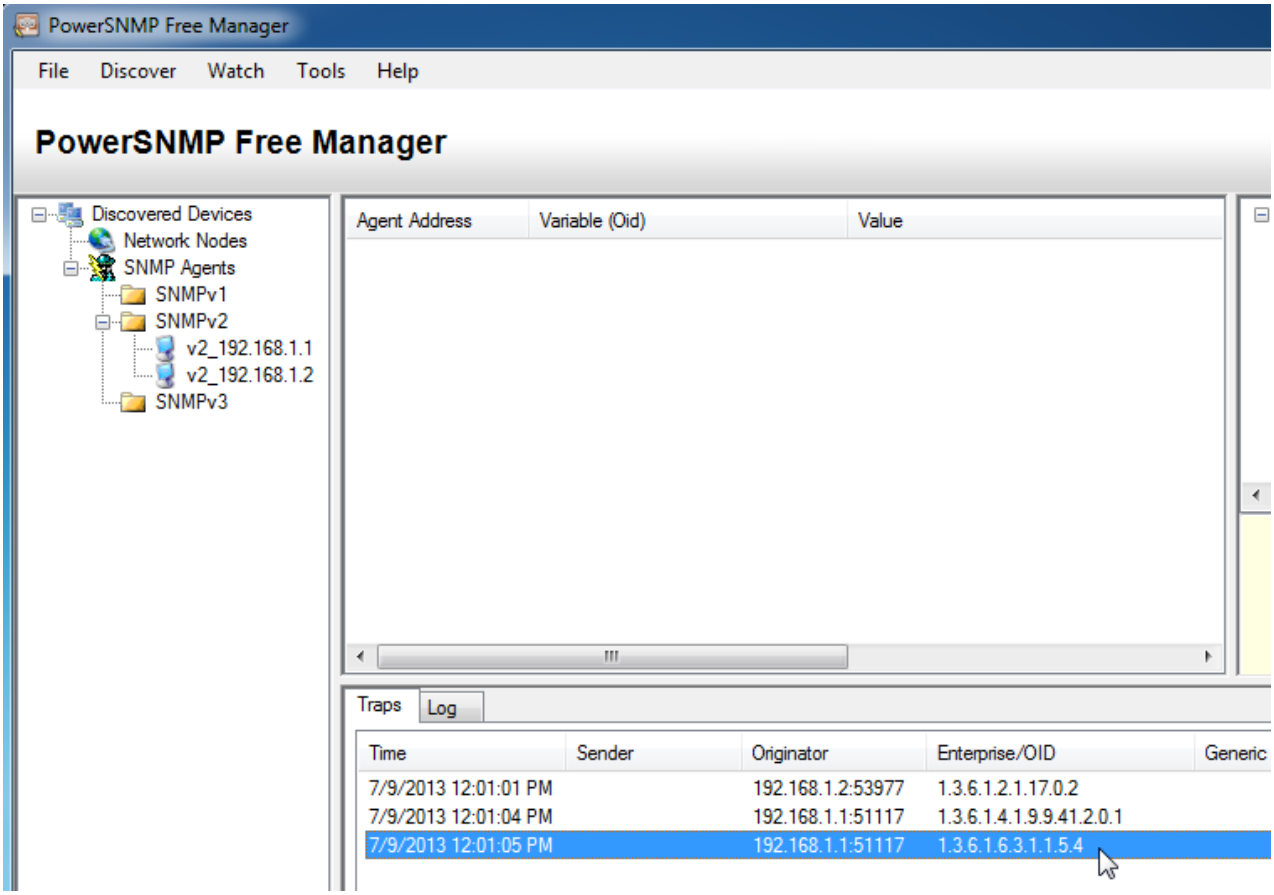
Step 1: Clear current SNMP messages.

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.

```
R1(config)# interface s0/0/0
R1(config)# ip address 192.168.2.1 255.255.255.252
R1(config)# clock rate 128000
R1(config)# no shutdown
```



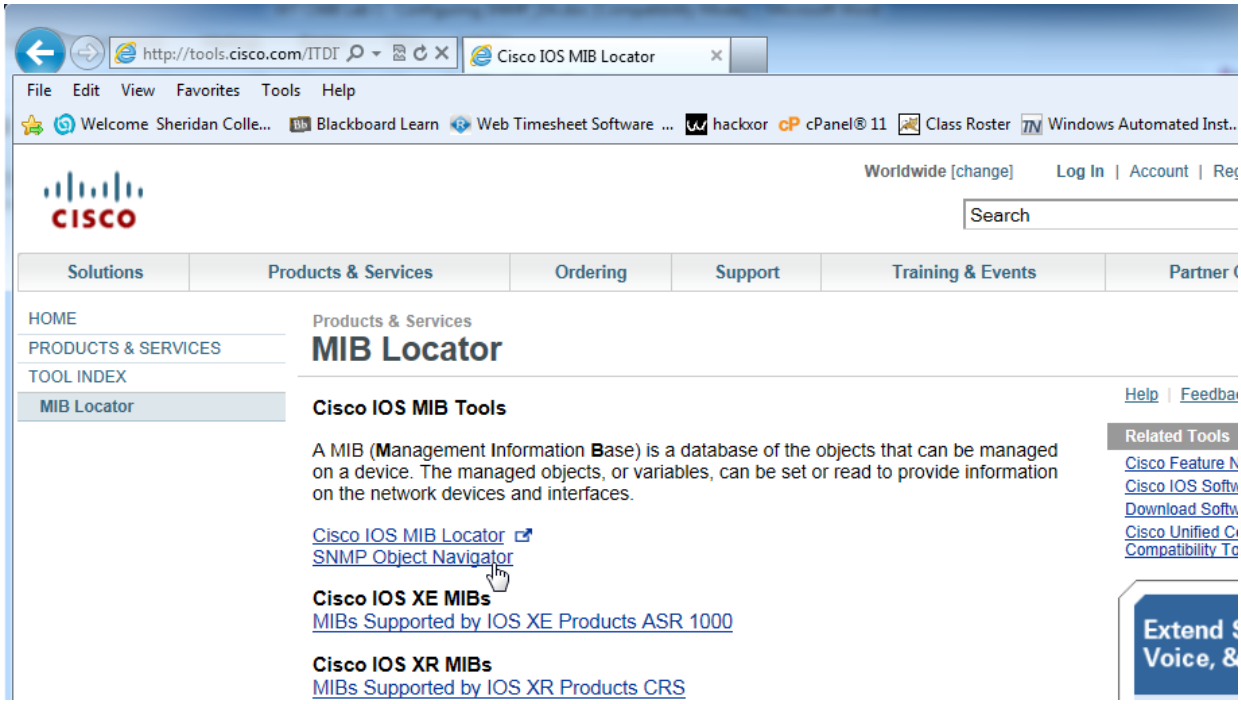
Step 3: Decode SNMP MIB/OID messages.

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

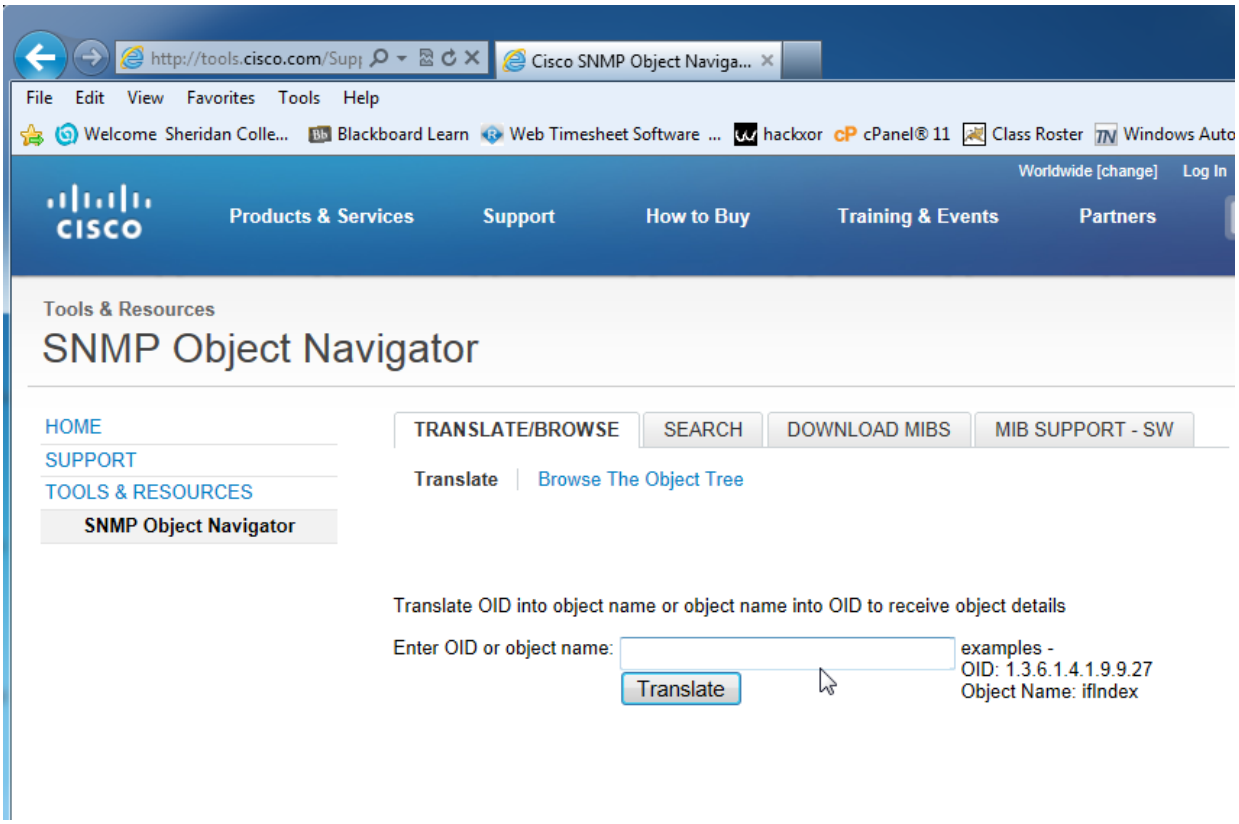
a. Using the search tool at the top of the window, search for **SNMP Object Navigator**.

b. Choose **SNMP Object Navigator MIB Download MIBs OID OIDs** from the results.

c. Navigate to the **MIB Locator** page. Click the **SNMP Object Navigator**.



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.

_____

_____

_____

_____

_____

For example, the description for OID 1.3.6.1.6.3.1.1.5.4 is a linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

Reflection

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

   _____

   _____

   Answers will vary, but students may point to the ability of SNMP as an open and cross platform protocol to work with many different devices including host computers on the network. SNMP benefits a network administrator whose job it is to monitor the status and configuration of network hosts across the entire network.

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

   _____

   _____

   Because SNMPv2 supports only unencrypted community strings, using read-write access would be a greater security risk.

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.

Device Configs

Router R1

```
R1#show run
Building configuration...

Current configuration : 5969 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
```

```
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
!
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
```

```
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps c3g
snmp-server enable traps entity-sensor threshold
snmp-server enable traps adslline
snmp-server enable traps vdsl2line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp cbgp2
snmp-server enable traps isis
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-
change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
```

```
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps waas
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps firewall serverstatus
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.1.3 version 2c ciscolab
!
control-plane
!
line con 0
```

```
 password cisco
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R2

```
R2#show run
Building configuration...

Current configuration : 1251 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
```

```
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#show run
Building configuration...

Current configuration : 4618 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
```

```
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps cluster
```

```
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-
guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet police
snmp-server enable traps fru-ctrl
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps ipsla
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.1.3 version 2c ciscolab
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```