Práctica de laboratorio: Configuración de SNMP

Topología

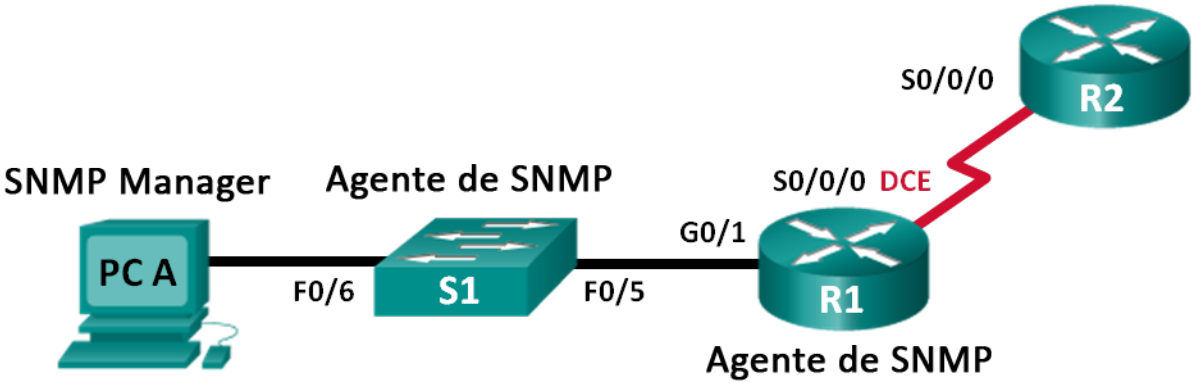


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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

Objetivos

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Configurar un administrador de SNMP y agentes SNMP

Parte 3: Convertir los códigos OID con Cisco SNMP Object Navigator

Información básica/situación

El protocolo simple de administración de red (SNMP) es un protocolo de administración de red y un estándar IETF que se puede utilizar para controlar a los clientes en la red. SNMP puede utilizarse para obtener y establecer variables relacionadas con el estado y la configuración de los hosts de red como los routers y los switches, así como los equipos cliente de red. El administrador de SNMP puede sondear a los agentes SNMP para obtener datos, o los datos se pueden enviar automáticamente al administrador de SNMP mediante la configuración de traps en los agentes SNMP.

En esta práctica de laboratorio, descargará, instalará y configurará software de administración SNMP en la PC-A. También configurará un router Cisco y un switch Cisco como agentes SNMP. Después de capturar mensajes de notificación SNMP del agente SNMP, convertirá los códigos MIB y de ID de objeto para conocer los detalles de los mensajes mediante Cisco SNMP Object Navigator.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: en esta práctica de laboratorio, los comandos **snmp-server** harán que el switch Cisco 2960 emita un mensaje de advertencia al guardar el archivo de configuración en la NVRAM. Para evitar este mensaje de advertencia, verifique que el switch utilice la plantilla **lanbase- routing**. Switch Database Manager (SDM) controla la plantilla del IOS. Cuando se cambia la plantilla preferida, la nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Utilice los siguientes comandos para asignar la plantilla **lanbase-routing** como plantilla predeterminada en SDM.

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

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- 1 computadora (Windows 7, Vista o XP, con acceso a Internet)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología
- Software de administración SNMP (PowerSNMP Free Manager de Dart Communications, o servidor de syslog Kiwi de SolarWinds, versión de evaluación con prueba de 30 días)

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los dispositivos con los parámetros básicos.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Configurar el equipo host.

Paso 3: Inicializar y volver a cargar el switch y los routers, según sea necesario.

Paso 4: Configurar los parámetros básicos para los routers y el switch.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

c. Configure las direcciones IP, según se muestran en la tabla de direccionamiento. (No configure la interfaz S0/0/0 en R1 en este momento).

d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

f. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

g. Verifique que la conectividad entre los dispositivos LAN sea correcta mediante la emisión del comando ping.

h. Copie la configuración en ejecución en la configuración de inicio

Parte 2: Configurar el administrador de SNMP y los agentes SNMP

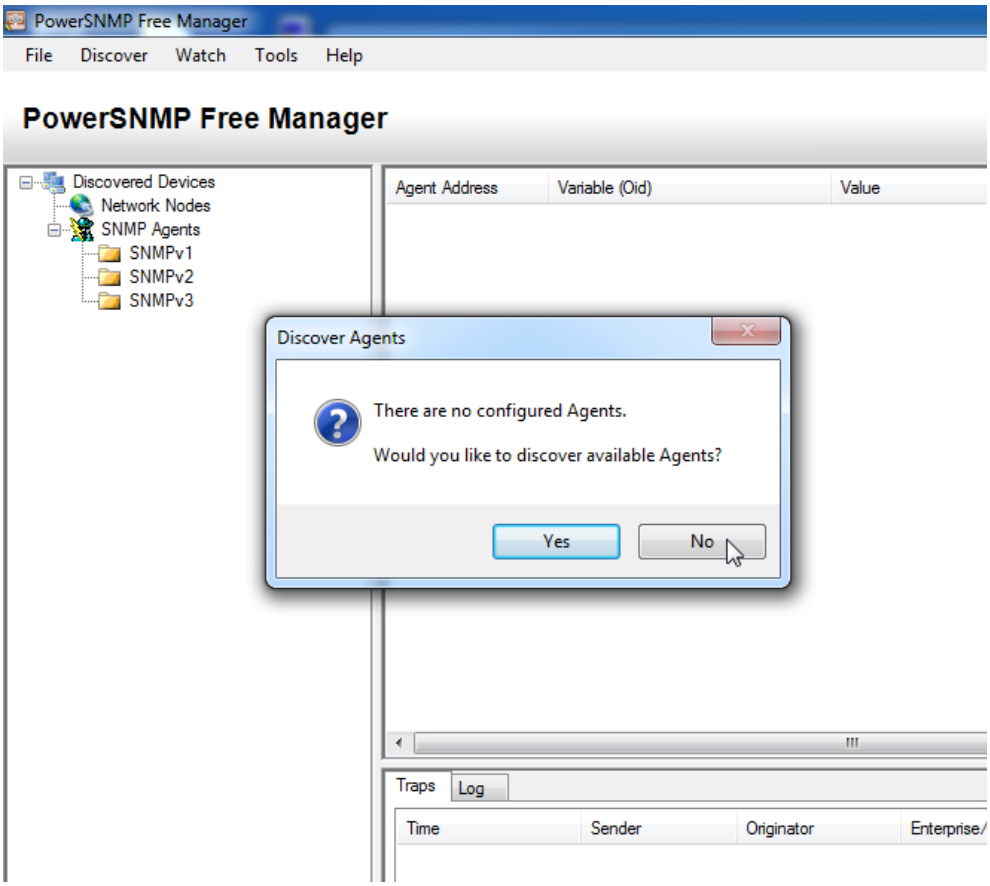
En la parte 2, se instalará y se configurará el software de administración SNMP en la PC-A, y se configurará el R1 y el S1 como agentes SNMP.

Paso 1: Instalar un programa de administración SNMP.

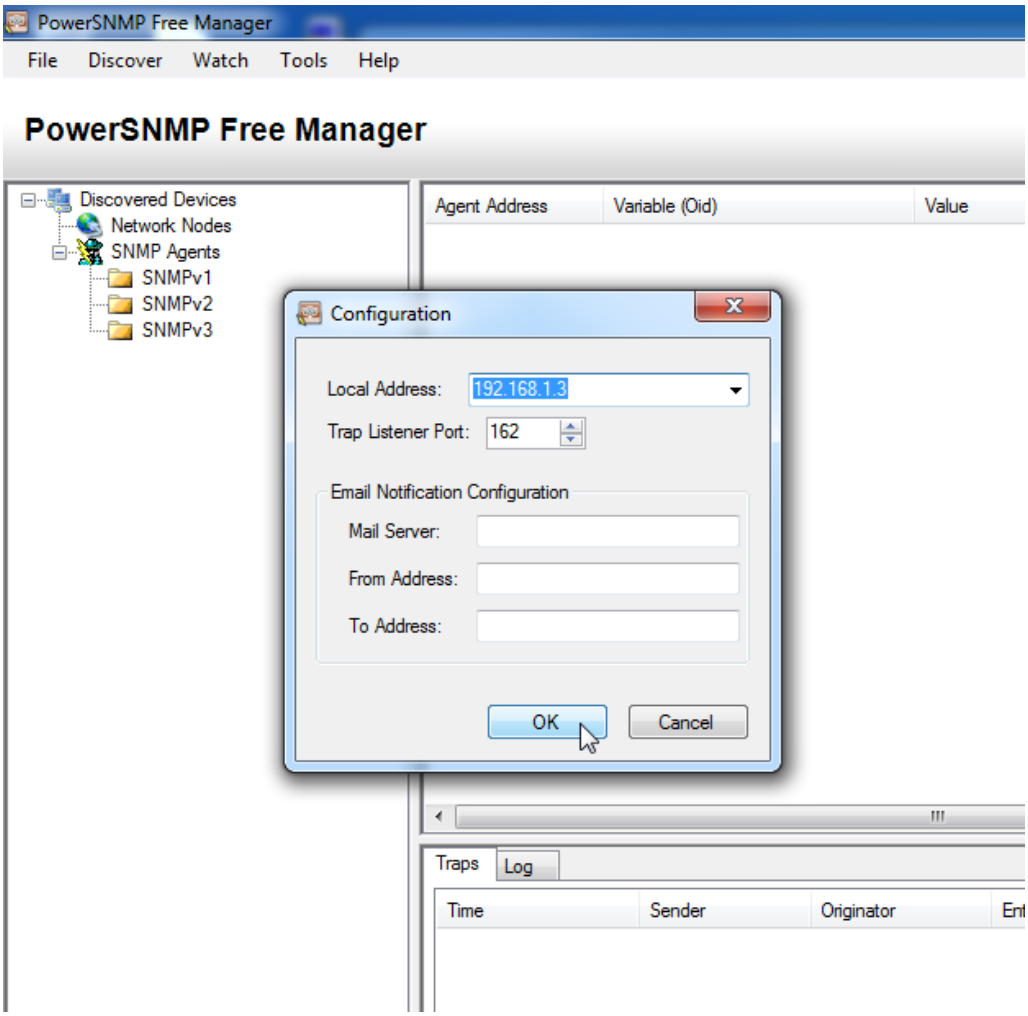
a. Descargue e instale PowerSNMP Free Manager de Dart Communications del siguiente URL: http://www.dart.com/snmp-free-manager.aspx.

b. Inicie el programa PowerSNMP Free Manager.

c. Haga clic en **No** si se le pide que detecte los agentes SNMP disponibles. Detectará los agentes SNMP después de configurar SNMP en el R1. PowerSNMP Free Manager admite SNMP versión 1, 2 y 3. En esta práctica de laboratorio, se utiliza SNMPv2.



d. En la ventana emergente Configuration (Configuración) establezca la dirección IP local para escuchar en 192.168.1.3 y haga clic en **OK** (Aceptar); si no aparece ninguna ventana emergente, vaya a Tools > Configuration (Herramientas > Configuración).



Nota: si se le pide que detecte los agentes SNMP disponibles, haga clic en **No** y continúe con la siguiente parte de la práctica de laboratorio.

Paso 2: Configurar un agente SNMP.

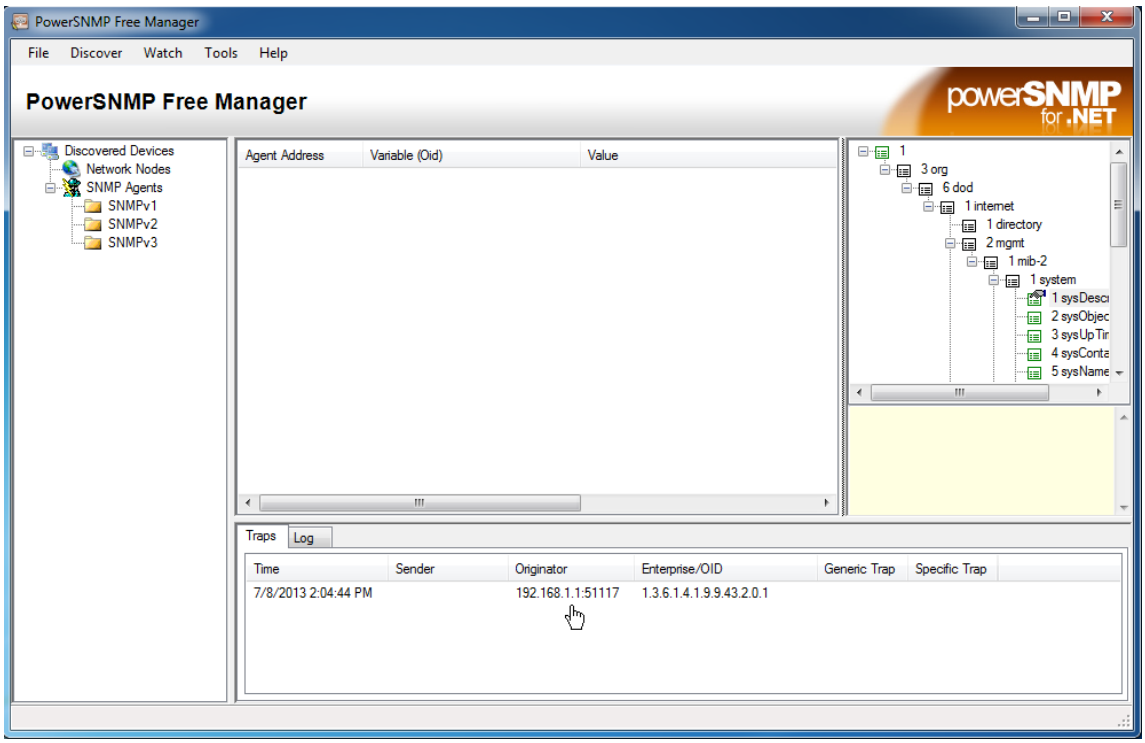
a. En el R1, introduzca los siguientes comandos del modo de configuración global para configurar el router como agente SNMP. En la línea 1 a continuación, la cadena de comunidad SNMP es **ciscolab**, con privilegios de solo lectura, y la lista de acceso con nombre SNMP_ACL define qué hosts tienen permitido obtener la información de SNMP del R1. En las líneas 2 y 3, los comandos de ubicación y contacto del administrador de SNMP proporcionan información descriptiva de contacto. La línea 4 especifica la dirección IP del host que recibirá notificaciones SNMP, la versión de SNMP y la cadena de comunidad. La línea 5 habilita todas las traps de SNMP predeterminadas, y las líneas 6 y 7 crean la lista de acceso con nombre, para controlar qué hosts tienen permitido obtener la información SNMP del 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
```



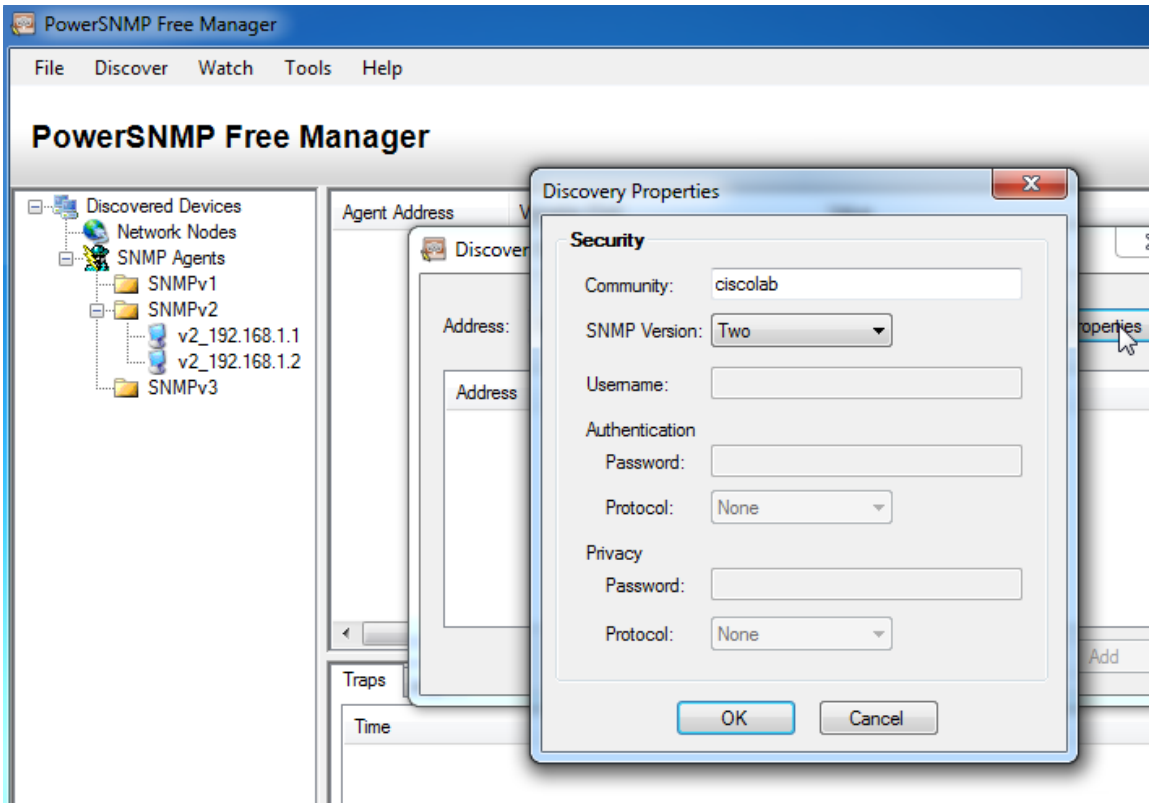
```
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

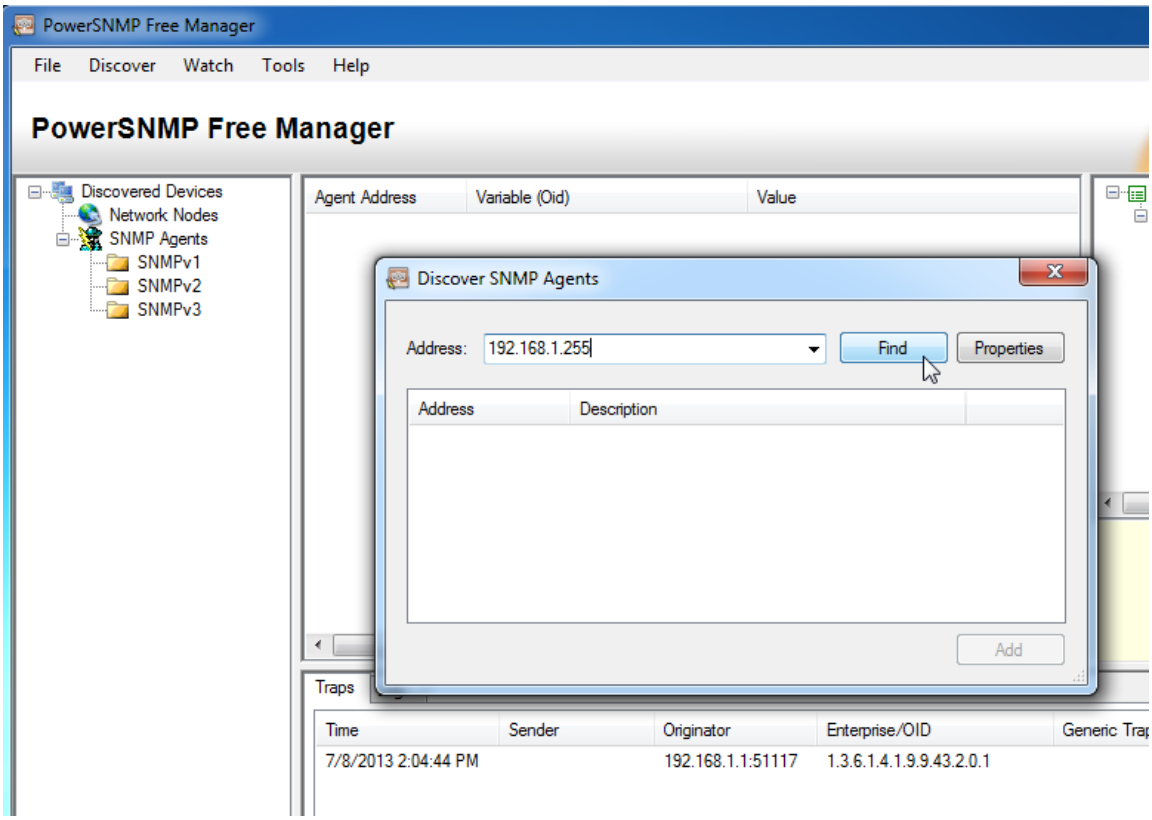
b. En este momento, puede observar que PowerSNMP Free Manager recibe notificaciones del R1. De lo contrario, puede intentar forzar que se envíe una notificación SNMP mediante la introducción del comando **copy run start** en el R1. Continúe con el siguiente paso si no se realiza correctamente.

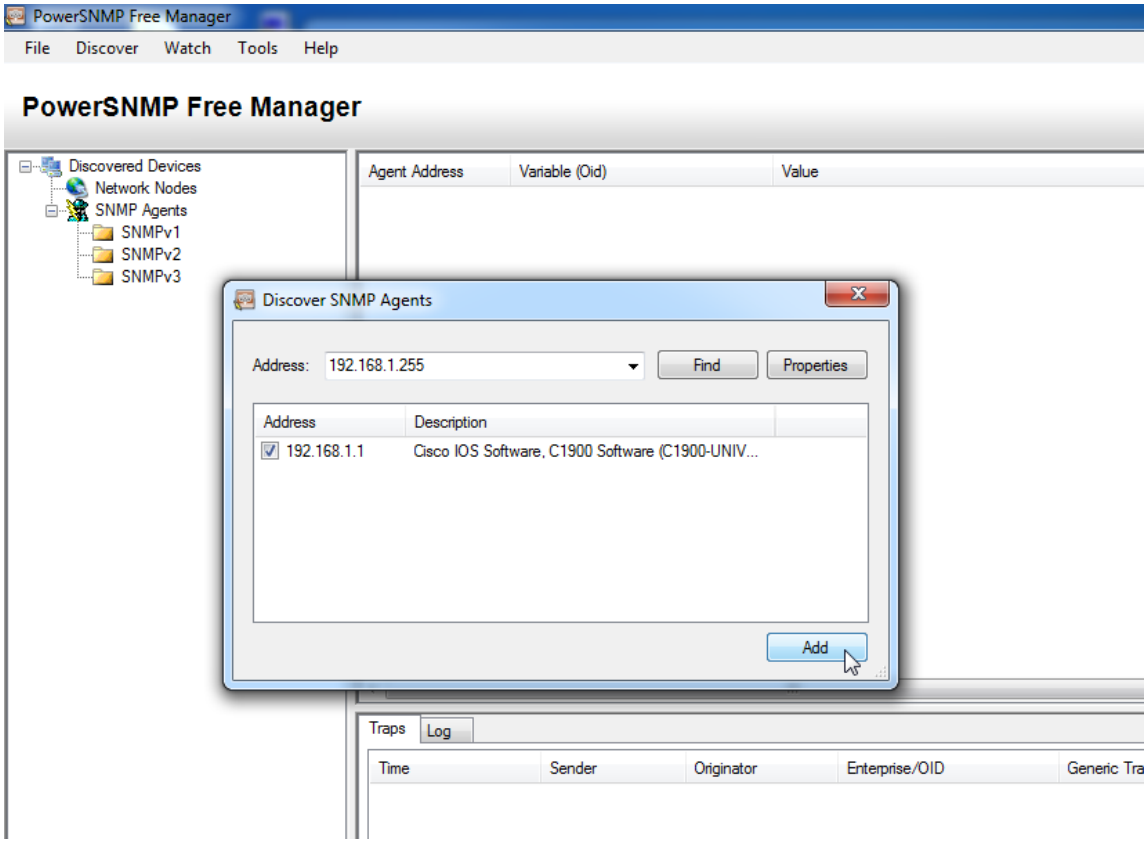


Paso 3: Detectar los agentes SNMP.

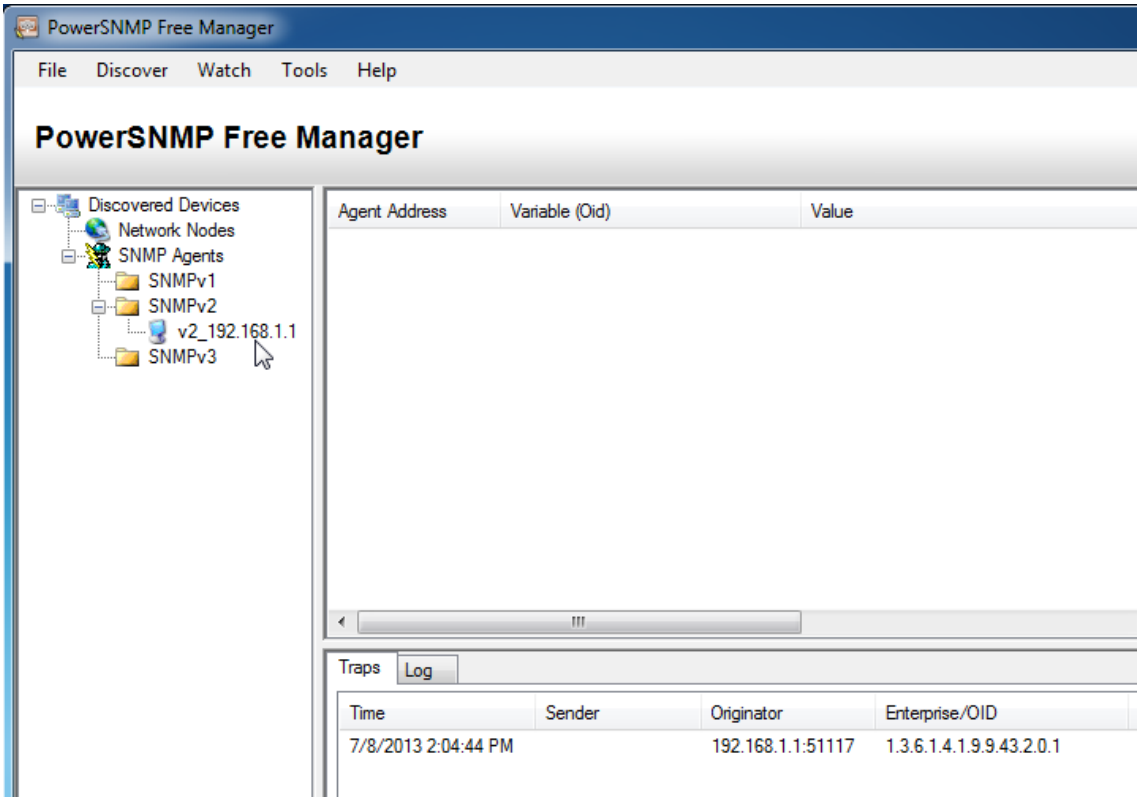
a. Desde PowerSNMP Free Manager en la PC-A, abra la ventana **Discover > SNMP Agents** (Detectar > Agentes SNMP). Introduzca la dirección IP **192.168.1.255**. En la misma ventana, haga clic en **Properties** (Propiedades) y establezca **ciscolab** en Community (Comunidad) y **Two** (Dos) en SNMP Version (Versión de SNMP); a continuación, haga clic en **OK**. Ahora puede hacer clic en **Find** (Buscar) para detectar todos los agentes SNMP en la red 192.168.1.0. PowerSNMP Free Manager debería encontrar al R1 en 192.168.1.1. Haga clic en la casilla de verificación y, a continuación, en **Add** (Agregar) para agregar al R1 como agente SNMP.







b. En PowerSNMP Free Manager, se agrega el R1 a la lista de agentes SNMPv2 disponibles.



c. Configure el S1 como agente SNMP. Puede utilizar los mismos comandos **snmp-server** que utilizó para configurar el R1.

d. Después de configurar el S1, se muestran notificaciones SNMP de 192.168.1.2 en la ventana Traps de PowerSNMP Free Manager. En PowerSNMP Free Manager, agregue el S1 como agente SNMP mediante el mismo proceso que utilizó para detectar al R1.

Parte 3: Convertir los códigos OID con Cisco SNMP Object Navigator

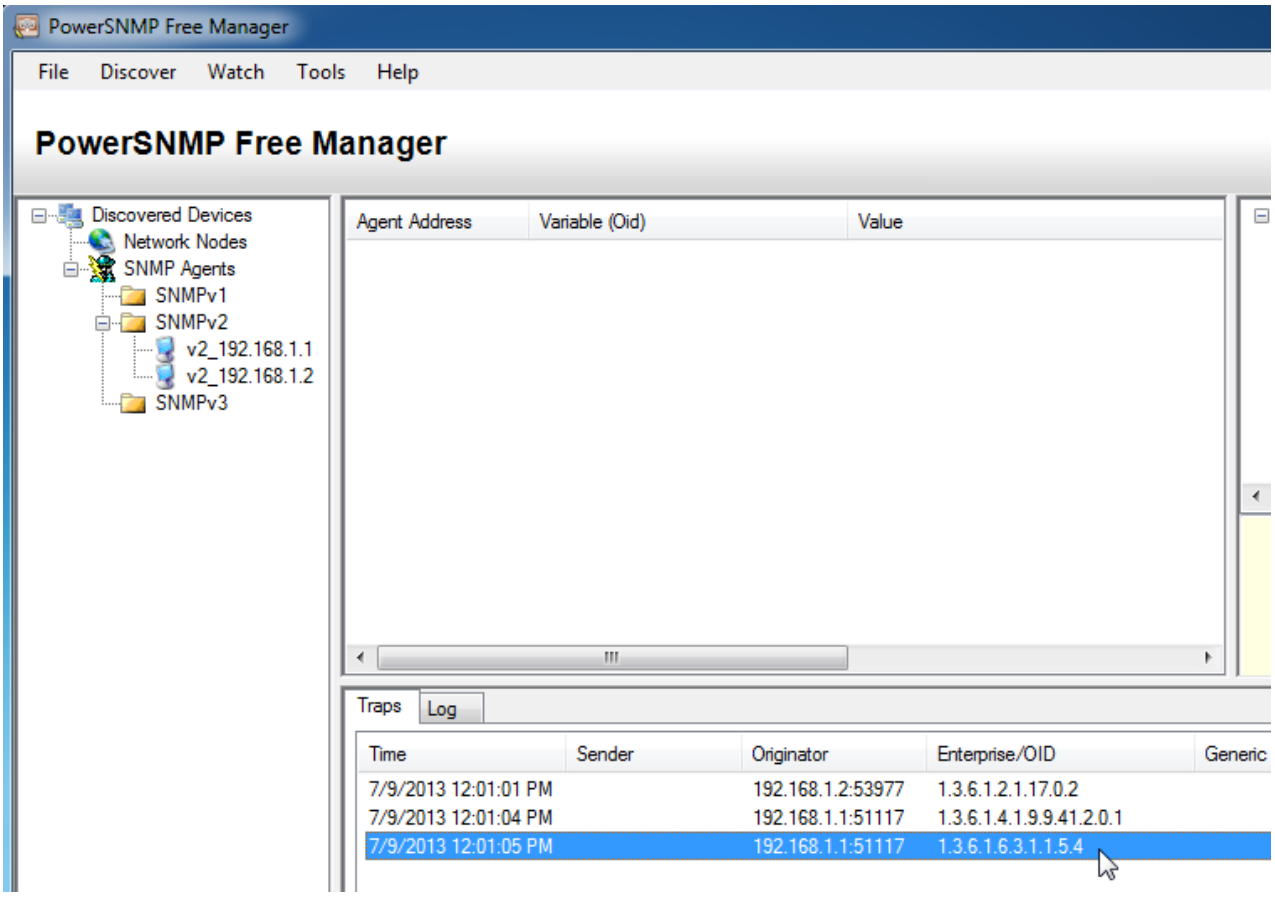
En la parte 3, forzará el envío de notificaciones SNMP al administrador de SNMP ubicado en la PC-A. A continuación, convertirá a nombres los códigos OID recibidos para descubrir la naturaleza de los mensajes. Los códigos MIB y OID se pueden convertir fácilmente mediante Cisco SNMP Object Navigator, ubicado en http://www.cisco.com.

Paso 1: Borrar los mensajes de SNMP actuales.

En PowerSNMP Free Manager, haga clic con el botón secundario en la ventana **Traps** y seleccione **Clear** (Borrar) para borrar los mensajes SNMP.

Paso 2: Generar una trap y una notificación de SNMP.

En el R1, configure la interfaz S0/0/0 según la tabla de direccionamiento que se encuentra al inicio de esta práctica de laboratorio. Acceda al modo de configuración global y habilite una interfaz para generar una notificación de trap SNMP que se envíe al administrador de SNMP en la PC-A. Observe los números de código Enterprise/OID (Empresa/OID) que se ven en la ventana de traps.



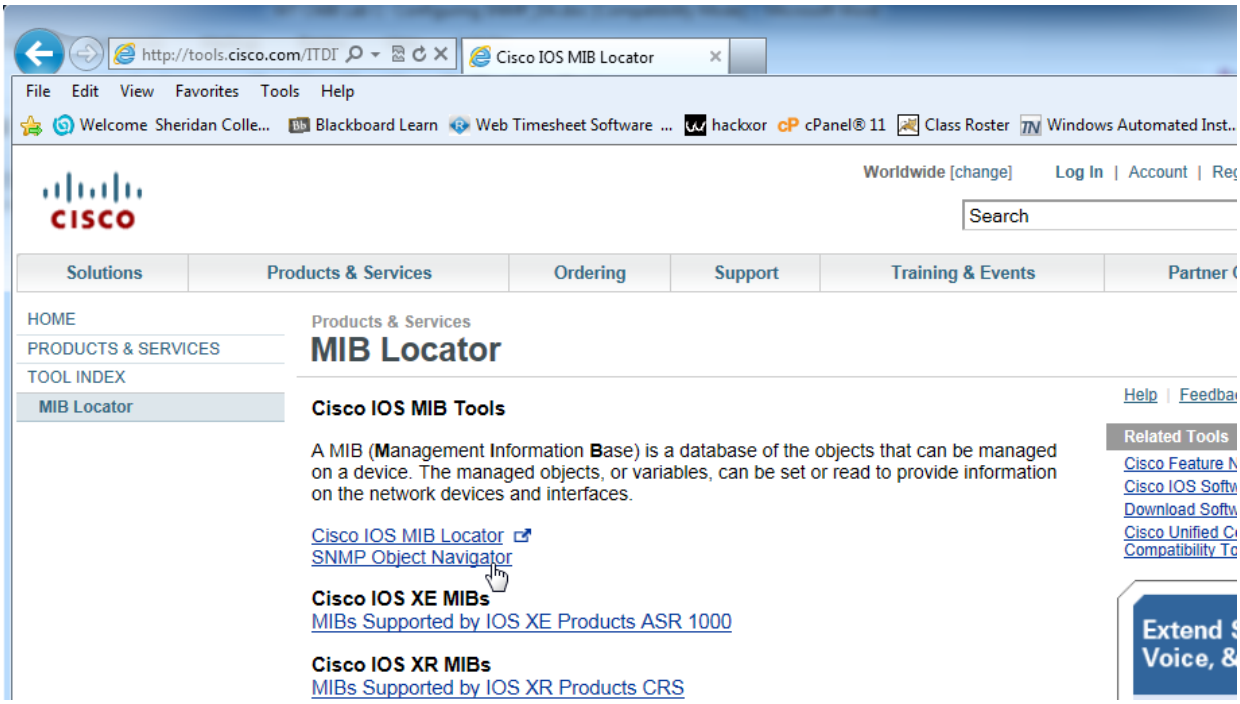
Paso 3: Decodificar los mensajes MIB y OID de SNMP.

En una computadora con acceso a Internet, abra un navegador web y vaya a http://www.cisco.com.

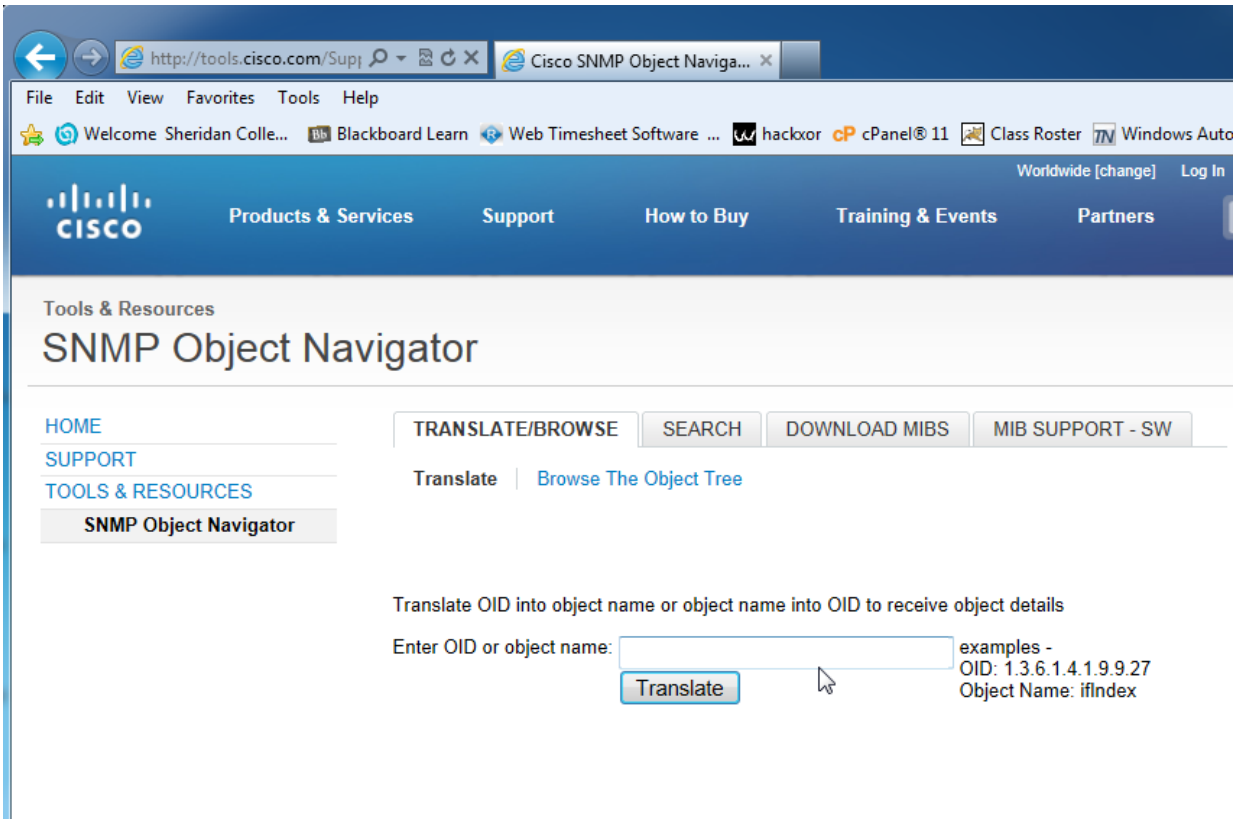
a. Mediante la herramienta de búsqueda en la parte superior de la ventana, busque **SNMP Object Navigator**.

b. Elija **SNMP Object Navigator MIB Download MIBs OID OIDs** de los resultados.

c. Navegue hasta la página **MIB Locator**. Haga clic en **SNMP Object Navigator**.



d. Mediante la página **SNMP Object Navigator**, decodifique el número de código OID de PowerSNMP Free Manager que se generó en el paso 2 de la parte 3. Introduzca el número de código OID y haga clic en **Translate** (Traducir)



e. Registre los números de código OID y las traducciones de mensaje correspondientes a continuación.

Reflexión

1. ¿Cuáles son algunos de los posibles beneficios de monitorear una red con SNMP?

2. ¿Por qué es preferible utilizar solamente acceso de solo lectura al trabajar con SNMPv2?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 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)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI de ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.