

Práctica de laboratorio: Configuración de SNMP

Topología

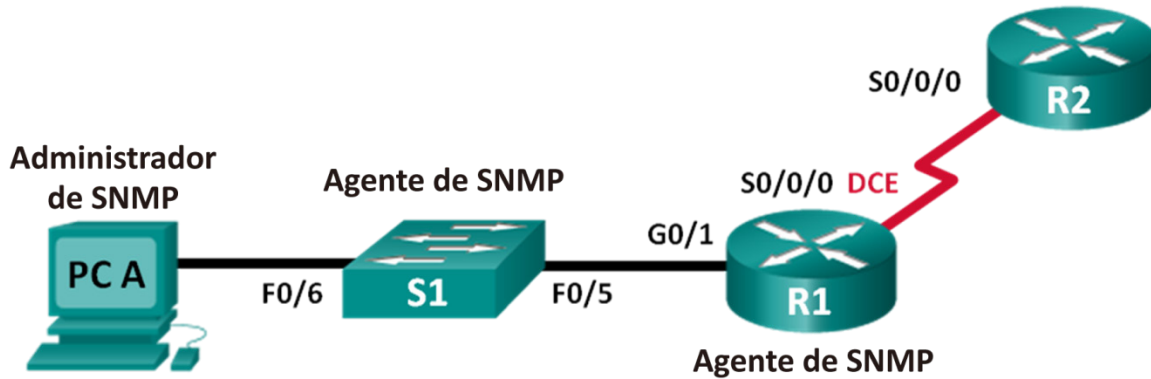


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
	S0/0/0	192.168.2.1	255.255.255.252	N/D
R2	S0/0/0	192.168.2.2	255.255.255.252	N/D
S1	VLAN 1	192.168.1.2	255.255.255.0	N/D
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: Configure un administrador SNMPv2 y un agente

Parte 3: Configure un gerente de SNMPv3 y un agente

Aspectos básicos/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 PC-A. También configurará un router Cisco y un switch Cisco como agentes de 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 usan en las actividades prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.4(3) (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, 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 al instructor.

Nota: Los comandos **snmp-server** de esta actividad de laboratorio, 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 esté usando la plantilla **lanbase-routing**. Switch Database Manager (SDM) controla la plantilla del IOS. Al cambiar la plantilla preferida, la nueva plantilla se usará después de reiniciar, incluso si no se guarda la configuración.

```
S1# show sdm prefer
```

Use los siguientes comandos para asignar la plantilla **lanbase-routing** como la plantilla de SDM predeterminada.

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

Recursos necesarios

- 2 routers (Cisco 1941 con Cisco IOS versión 15.4(3), imagen universal o equivalente)
- 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 1 PC (Windows con un programa de emulación de terminal, como Tera Term, administrador SNMP, como navegador de administración (MIB por ManageEngine, y Wireshark)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología
- Software de administración SNMP (navegador de administración (MIB por ManageEngine)

Parte 1: Armar la red y configurar los ajustes 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 de 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 ni active la interfaz VLAN 1 en S1 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.

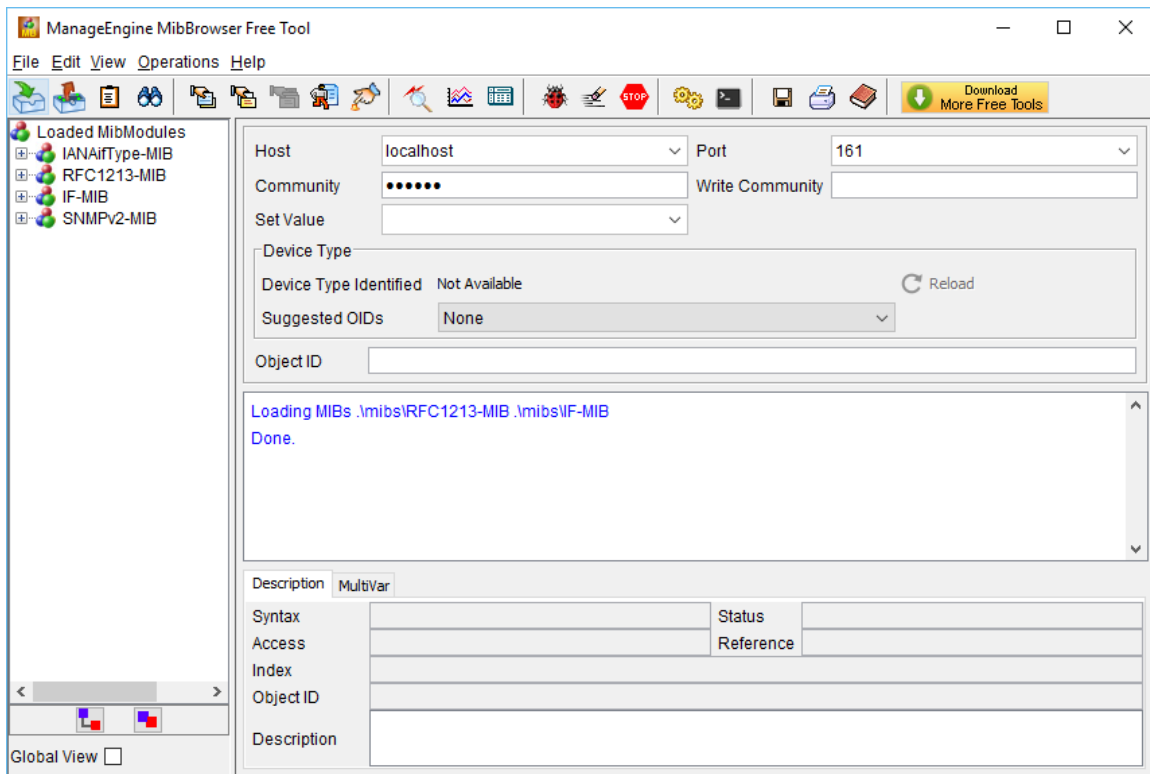
- f. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- g. Verifique la conectividad satisfactoria entre PC-A y R1 y entre los routers mediante **el comando ping**.
- h. Copie la configuración en ejecución en la configuración de inicio

Parte 2: Configure el gerente SNMPv2 y el agente

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. Descargar e instalar el navegador de administración (MIB por ManageEngine de URL siguiente: <https://www.manageengine.com/products/mibbrowser-free-tool/download.html>. Se le solicitará que proporcionar una dirección de correo electrónico para descargar el software.
- b. Inicie el programa de ManageEngine MibBrowser.
 - 1) Si recibe un mensaje de error con respecto a la falla de cargar el MIB. Navegue hasta la carpeta libre de MibBrowser Tool:
32bit: C:\Program archivos (x86) \ ManageEngine \ MibBrowser Tool libre
64bit: C:\Program Files\ManageEngine\MibBrowser libera Tool
 - 2) Haga **clic con el botón secundario en la carpeta mibs** y seleccione **la ficha Seguridad**. Haga clic en **Editar**. Seleccione **Usuarios**. Haga **clic en el control total**. Haga clic en **OK (Aceptar)** para cambiar el permiso.
 - 3) Repita el paso anterior a **la carpeta** de configuración.
 - 4) Inicie el programa de ManageEngine MibBrowser nuevamente.



Paso 2: Configure un agente SNMPv2.

En S1, introduzca los siguientes comandos desde el modo de configuración global para configurar el switch como agente SNMP. En la línea 1 a continuación, la cadena de la comunidad SNMP es **ciscolab**, con privilegios de solo lectura, y la lista de acceso con nombre **SNMP_ACL** define qué hosts pueden obtener la información sobre SNMP de S1. 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 notificaciones SNMP predeterminadas, y las líneas 6 y 7 crean la lista de acceso con nombre para controlar qué hosts pueden obtener información sobre SNMP del switch.

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

Paso 3: Verifique la configuración de SNMPv2.

Utilice los comandos **show** para verificar la configuración de SNMPv2.

```
S1# show snmp
Chasis: FCQ1628Y5MG
Contacto: admin@company.com
Ubicación: 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
Desvío global de SNMP: habilitado

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: active access-list permanente: SNMP_ACL
```

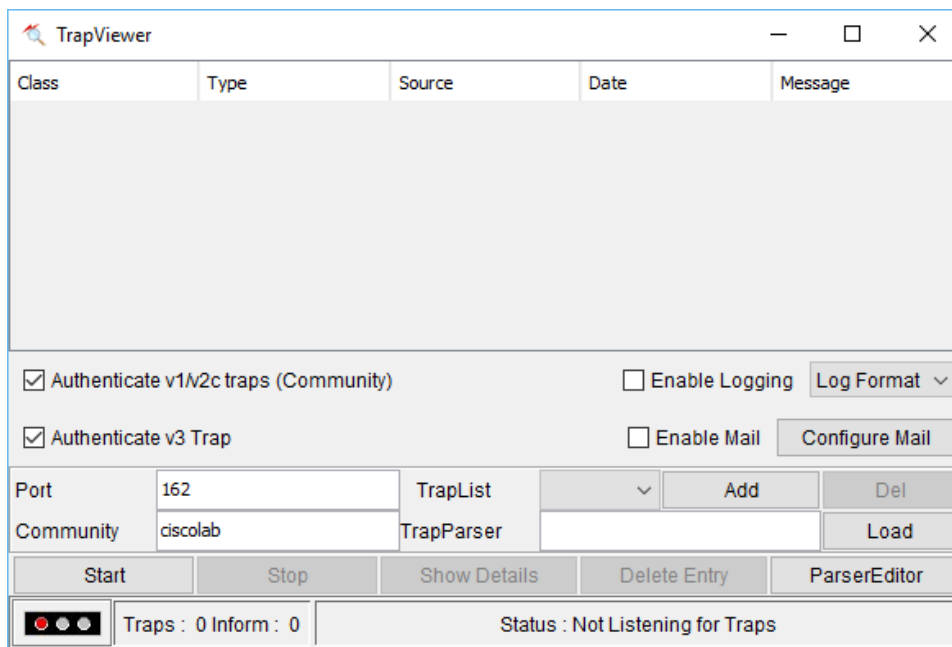
```
<se omitió el resultado>
```

¿Cuál es la comunidad SNMP configurada?

Paso 4:

En este paso, iniciará la trampa de SNMP y observará los mensajes cuando se configura y activa una SVI en VLAN 1 para S1.

- En el MibBrowser, haga clic en **Editar > las configuraciones**. Verifique que el **v2c** esté seleccionado como la versión de SNMP. Haga clic en **OK** (Aceptar) para continuar.
- Haga clic en el visor UI de desvío ()
- Verifique que **162** es el número de puerto y configure el **ciscolab** como la comunidad.



- Haga clic en **Inicio** después de verificar las configuraciones. El campo de TrapList muestra **162: ciscolab**.
- Para generar mensajes SNMP, configure y habilite la SVI en S1. Utilice la dirección IP **192.168.1.2 /24** para VLAN 1 y Deshabilite y habilite la interfaz.
- Introduzca el comando **show snmp** para verificar que los mensajes SNMP se enviaron.

```
S1# show snmp
```

```
Chasis: FCQ1628Y5MG
```

```
Contacto: admin@company.com
```

Práctica de laboratorio: Configuración de SNMP

Ubicación: 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
```

Desvío global de SNMP: habilitado

SNMP logging: enabled

Logging to 192.168.1.3.162, 0/10, 2 sent, 0 dropped.

SNMP agent enabled

SNMP agent enabled

- g. Navegue hasta TrapViewer. Ver mensajes que han sido podemos por MibBrowser. Para ver los detalles de cada mensaje, haga clic en **Show Details** (Mostrar detalles).

The screenshot shows the TrapViewer application window. It features a table with the following data:

Class	Type	Source	Date	Message
Clear	v2c Trap	192.168.1.2	Wed Oct 05 14:31:35...	.iso.org.dod.internet...
Clear	v2c Trap	192.168.1.2	Wed Oct 05 14:31:36...	.iso.org.dod.internet...

Below the table, there are several control elements:

- Checkboxes for "Authenticate v1/v2c traps (Community)" and "Authenticate v3 Trap", both checked.
- Buttons for "Enable Logging" and "Enable Mail", both unchecked.
- A "Log Format" dropdown menu.
- A "Configure Mail" button.
- A "Port" field with the value "162" and a "TrapList" dropdown with "162:ciscolab" selected.
- A "Community" field with the value "ciscolab" and a "TrapParser" dropdown.
- Buttons for "Add", "Del", and "Load".
- Buttons for "Start", "Stop", "Show Details", "Delete Entry", and "ParserEditor".
- A status bar at the bottom showing "Traps : 2 Inform : 0" and "Status : Listening for Traps".

Parte 3: Configure el gerente SNMPv3 y el agente

Paso 1: Configure un agente SNMPv3 en R1.

En el R1, introduzca los siguientes comandos del modo de configuración global para configurar el router como agente SNMP. En las líneas 1 – 3 a continuación, una ACL estándar of al PERMIT-ADMIN sólo a los hosts de la red 192.168.1.0 /24 para acceder al agente SNMP que se ejecuta en R1. La línea 4 configura una vista de SNMP, SNMP-RO, e incluye el árbol de la ISO de la MIB. En la línea 5, configuran con el nombre ADMIN, se establecen en SNMPv3 con autenticación y cifrado requeridos, y permite sólo un grupo SNMP límite de acceso a los hosts permitidos en el PERMIT-ADMIN ACL. La línea 5 define un usuario denominado USER1 con el grupo ADMIN. La autenticación se establece para usar SHA con la contraseña cisco12345 y el cifrado se establece para AES 128 con cisco54321 como contraseña configurada.

```
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...
```

Paso 2: Verifique una configuración SNMPv3 en R1.

Utilice los comandos **show** para verificar la configuración de SNMPv3.

```
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

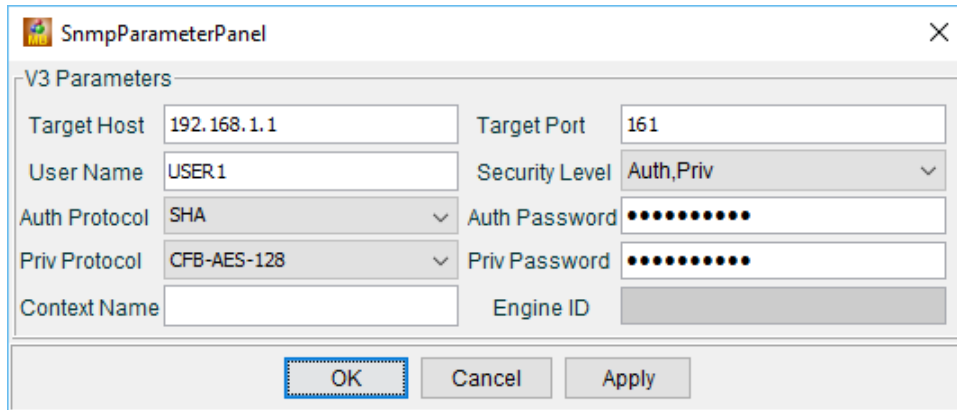
User name: USER1
ID de motor: 800000090300D48CB5CEA0C0
storage-type: nonvolatile          active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN
```

Paso 3: Acceso al administrador SNMP de configurar el agente SNMPv3.

- Desplácese a PC-A Wireshark **abierto**. Inicie una captura en vivo en la interfaz adecuada.
- Introduzca **snmp** en el campo Filter (Filtro).
- En el MibBrowser, haga clic en **Editar > las configuraciones**. Seleccione **v3** permite la versión de SNMP. Luego haga clic en **Agregar**.

Práctica de laboratorio: Configuración de SNMP

- d. Introduzca la configuración de SNMPv3 que fueron configuradas en R1. Haga clic en **OK** (Aceptar) para continuar.



The screenshot shows a dialog box titled "SnmpParameterPanel" with a close button (X) in the top right corner. The dialog is divided into a "V3 Parameters" section and a button area at the bottom. The "V3 Parameters" section contains the following fields:

- Target Host: 192.168.1.1
- Target Port: 161
- User Name: USER1
- Security Level: Auth,Priv (dropdown menu)
- Auth Protocol: SHA (dropdown menu)
- Auth Password: cisco12345 (masked with dots)
- Priv Protocol: CFB-AES-128 (dropdown menu)
- Priv Password: cisco54321 (masked with dots)
- Context Name: (empty)
- Engine ID: (empty)

At the bottom of the dialog, there are three buttons: "OK" (highlighted with a dashed border), "Cancel", and "Apply".

Parámetros de SNMPv3	Configuración
Host objetivo	192.168.1.1
Nombre de usuario	USER1
Protocolo de autenticación	SHA
Protocolo PRIV	CFB-AES-128
Puerto objetivo	161
Nivel de seguridad	Original, Priv
Contraseña de autenticación	cisco12345
Contraseña PRIV	cisco54321

- e. Haga clic en **Editar > nodo de descubrimiento**. Ingrese **ipAddrTable** por encontrar qué cierre del campo y **haga clic en Iniciar**. Verifique que **ipAddrTable** esté seleccionado en el panel izquierdo y **.iso.org.dod.internet.mgmt.mib-2.ip.ip AddrTable** se indica en el campo de ObjectID.

Práctica de laboratorio: Configuración de SNMP

- f. Haga clic en la operación > GET obtener todos los objetos en objetos MIB (Seleccionar, en este caso ipAddrTable).

The screenshot shows the ManageEngine MibBrowser Free Tool interface. The left sidebar displays a tree view of MIB objects, with 'ipAddrTable' selected. The main window shows the configuration for the selected object, including Host (192.168.1.1), Port (161), and Community (*****). Below the configuration, a table lists the object instances and their values:

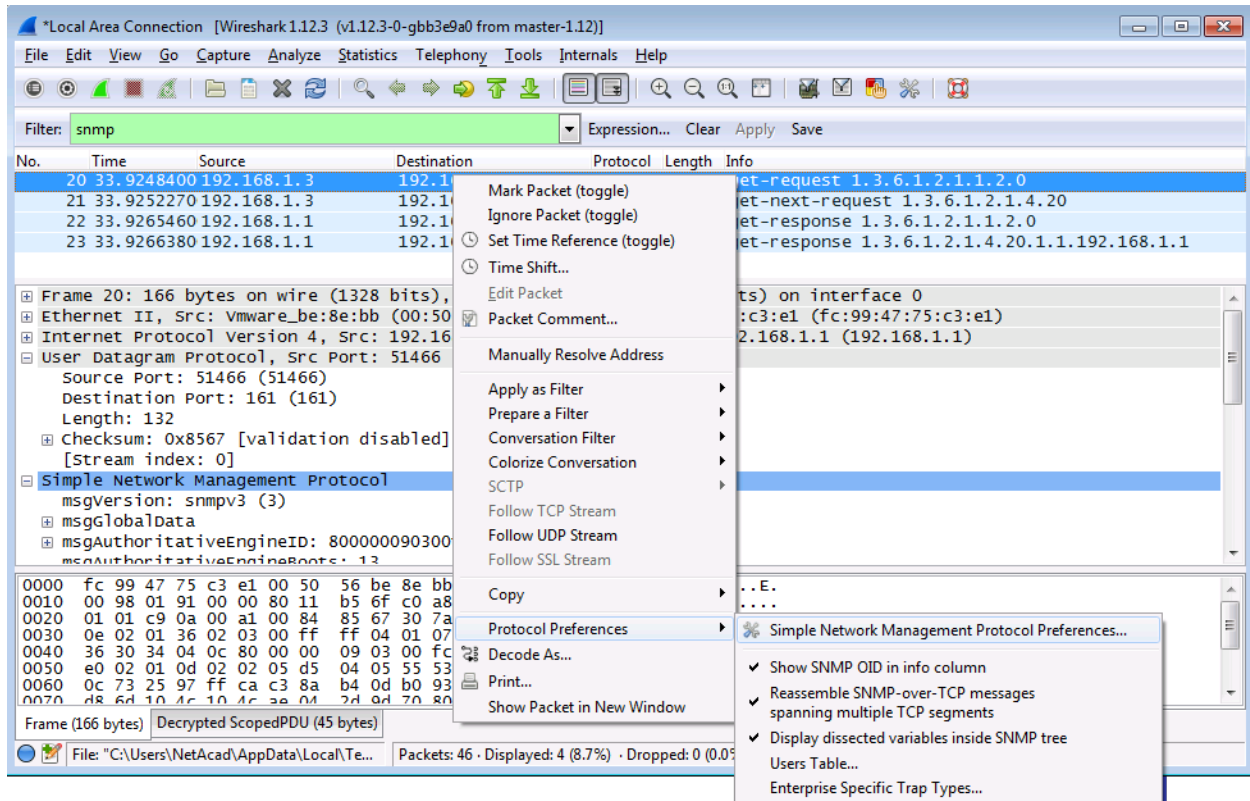
Object Name	Value
ipAdEntAddr.192.168.1.1	192.168.1.1
ipAdEntAddr.192.168.2.1	192.168.2.1
ipAdEntIfIndex.192.168.1.1	3
ipAdEntIfIndex.192.168.2.1	5
ipAdEntNetMask.192.168.1.1	255.255.255.0
ipAdEntNetMask.192.168.2.1	255.255.255.252

Below the table, the 'Description' tab is active, showing the following details:

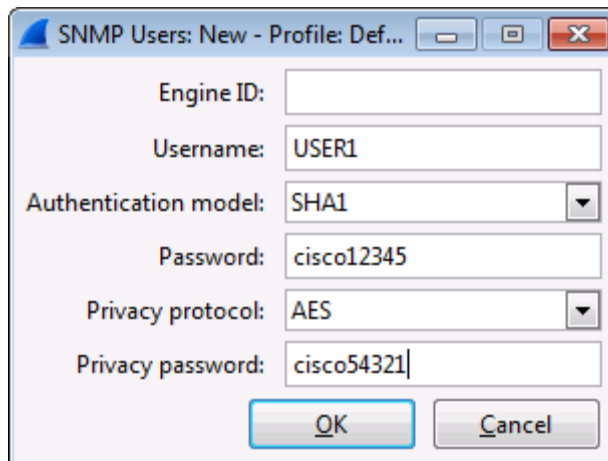
Field	Value
Syntax	Multivar
Status	mandatory
Access	not-accessible
Reference	
Index	
Object ID	.1.3.6.1.2.1.4.20
Description	"The table of addressing information relevant to this entity's IP addresses."

- g. Vuelva a la pantalla de Wireshark. Detenga la captura en vivo.
- h. En los resultados artesone, haga clic con el botón secundario en uno de los resultados. Seleccionar **preferencias de protocolo > las preferencias de administración de la red**.

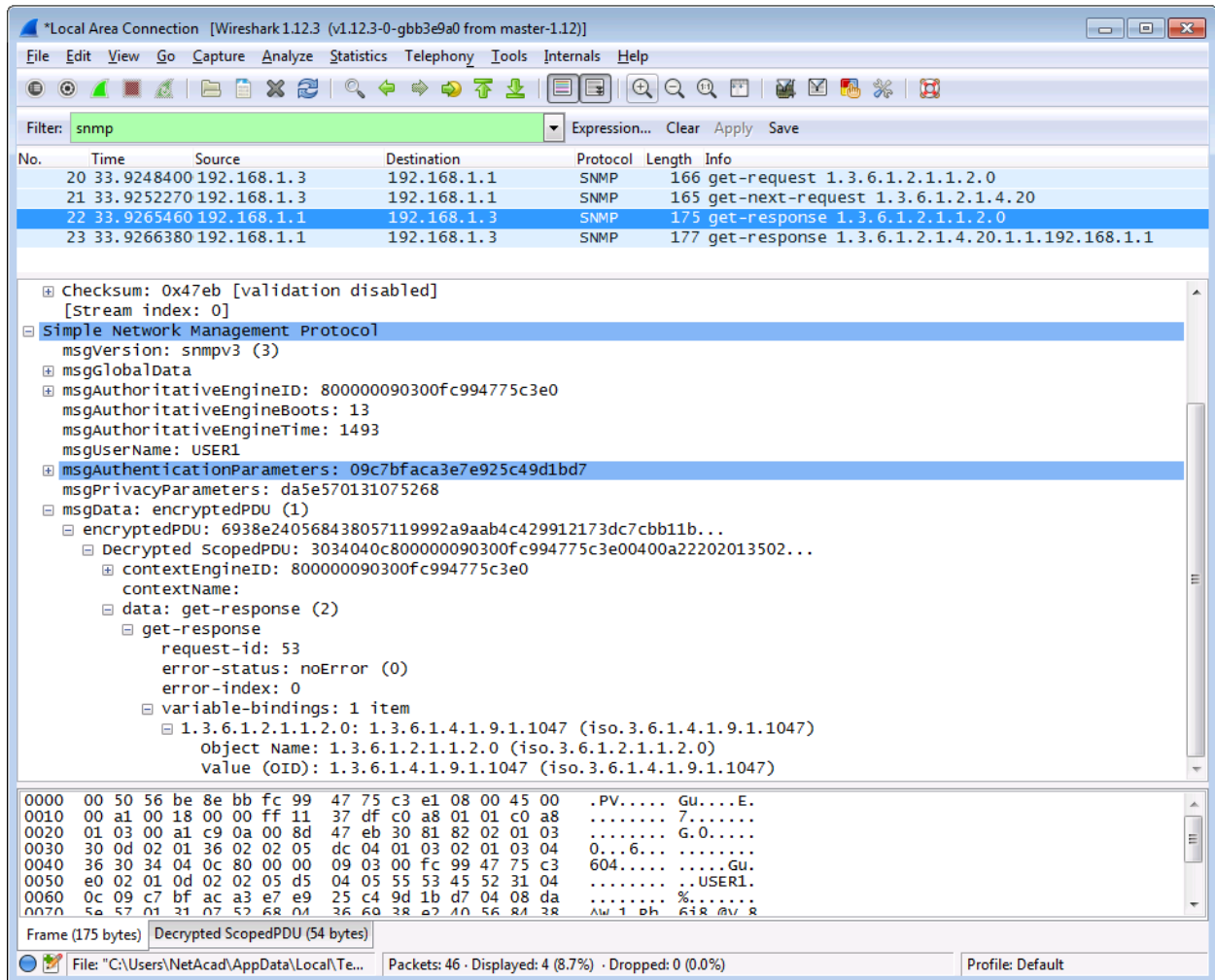
Práctica de laboratorio: Configuración de SNMP



- i. Haga clic en **Editar** para la tabla de usuarios. Haga clic en **Nuevo** e ingrese la información del usuario en el Paso 1. Haga clic en **Aceptar**.



- j. Haga clic en **OK** para aceptar la información de usuario. Haga clic en **OK** nuevamente para salir de la ventana de preferencias de Wireshark.
- k. Seleccione una de las líneas. Expanda el resultado de SNMP y vea los mensajes descriptados.



Paso 4: Revise los resultados.

¿Cuáles son las direcciones IP configuradas en R1 en los resultados de SNMPv3?

Compare los resultados descryptados Wireshark de los paquetes snmp y explorador MIB. Registre sus observaciones.

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?

3. ¿Cuáles son los beneficios de usar SNMPv3 por sobre SNMPv2?

Tabla de resumen de interfaces de router

Resumen de interfaces de router				
Modelo de router	Interfaz Ethernet 1	Interfaz Ethernet 2	Interfaz serial 1	Interfaz serial 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 hacer 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 ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.