SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE MINATITLÁN

INGENIERÍA EN SISTEMAS COMPUTACIONALES

“MANUAL DE PRÁCTICAS “

MATERIA

REDES DE COMPUTADORAS

MINATITLÁN, VER. AGOSTO DEL 2023

3.2 ÍNDICE DEL MANUAL DE PRÁCTICAS

ÍNDICE

3.1 INTRODUCCIÓN

El presente manual dará a conocer las prácticas relacionadas con los temas de la materia Redes de Computadoras, los cuales están divididos en 38 prácticas con respecto al temario de la materia:

1) Realización de un esquema de Internet.
2) Navegación de IOS.
3) Establecimiento de una sesión de consola con Tera Term.
4) Configuración de los parámetros iniciales del switch.
5) Implementación de conectividad básica.
6) Creación de una red simple.
7) Configuración de una dirección de administración del switch.
8) Exploración de una red.
9) Uso de Wireshark para ver el tráfico de la red.
10) Armado de un cable cruzado Ethernet.
11) Conexión de una LAN por cable y una LAN inalámbrica.
12) Identificación de direcciones MAC y direcciones IP.
13) Revisión de la tabla ARP.
14) Configuración de switches de capa 3.
15) Exploración de dispositivos de internetworking.
16) Configuración inicial del router.
17) Conexión de un router a una LAN.
18) Armado de una red de switch y route.
19) Comunicaciones TCP y UDP.

20) Uso de la calculadora de Windows con direcciones de red.

21) Conversión de direcciones IPv4 al sistema binario.

22) Identificación de direcciones IPv4.

23) Configuración de direccionamiento IPv6.

24) Prueba de conectividad de red con ping y traceroute.

25) Cálculo de subredes IPv4.

26) División de topologías de red en subredes.

27) Diseño e implementación de un esquema de direccionamiento IPv4 dividido en subredes.

28) Diseño e implementación de un esquema de direccionamiento VLSM.

29) Servidores Web y de correo electrónico.

30) Servidores de DHCP y servidores DNS.

31) Servidores FTP.

32) Acceso a dispositivos de red mediante SSH.

33) Protección de dispositivos de red.

34) Prueba de la conectividad con traceroute.

35) Prueba de la latencia de red con los comandos ping y traceroute.

36) Administración de los archivos de configuración del router con software de emulación de terminal.

37) Administración de archivos de configuración de dispositivos con TFTP, flash y USB.

38) Procedimientos de recuperación de contraseña.

3.2 JUSTIFICACIÓN

Un Manual de prácticas puede definirse como un compendio de documentos que contemplan una serie de aportes a la práctica científica y social de los alumnos que se encuentren realizando dicha práctica, las cuales también incluyen las normas y procedimientos que orientarán el desempeño del alumno y facilitarán la integración de la teoría con la práctica, en un contexto real de aprendizaje.

Este manual de prácticas está basado según el contenido de “el libro Guía para la elaboración y registro de textos o trabajos académicos”, con el que cuenta el Tecnológico Nacional de México.

El manual de prácticas servirá como apoyo de aprendizaje para los alumnos de la materia de Graficación, así como apoyo didáctico para los maestros de dicha materia, ya que se presentarán consejos y sugerencias para dicha realización de las prácticas, también se dará materia de apoyo para estas mismas.

3.3 OBJETIVO GENERAL DEL MANUAL DE PRÁCTICAS

El objetivo que se pretende lograr con este manual de prácticas es el diseño e implementación de representaciones gráficas de los datos y sus relaciones, utilizando algoritmos y herramientas computacionales. La graficación permite crear objetos gráficos bidimensionales y tridimensionales, aplicar transformaciones, efectos y animaciones, y mejorar el aspecto visual y la comprensión de la información.

3.4 DESARROLLO

3.4.1 Práctica 1. Realización de un esquema de Internet.

3.4.1.1 Objetivo

Parte 1: Probar la conectividad de red mediante el comando ping.

Parte 2: Rastrear una ruta a un servidor remoto mediante la herramienta tracert de Windows.

Parte 3: Rastrear una ruta a un servidor remoto mediante herramientas de software y herramientas basadas en Web.

3.4.1.2 Introducción

El software de rastreo de rutas es una utilidad que enumera las redes que atraviesan los datos desde el dispositivo final del usuario que los origina hasta una red de destino remoto.

Esta herramienta de red generalmente se ejecuta en la línea de comandos como:

tracert <nombre de la red de destino o dirección del terminal>
(sistemas Microsoft Windows)

o

traceroute <nombre de la red de destino o dirección del terminal>
(Unix y sistemas similares)

Las utilidades de rastreo de rutas permiten a un usuario determinar la trayectoria o las rutas, así como la demora a través de una red IP. Existen varias herramientas para llevar a cabo esta función.

La herramienta traceroute se usa generalmente para resolver problemas de redes. Al mostrar una lista de los routers atravesados, permite al usuario identificar la ruta tomada para llegar a un destino determinado de la red o a través del cual se envió el paquete de datos. La cantidad de routers de conocer como la cantidad de ‘saltos’ que viajaron los datos desde el origen hasta el destino.

La lista que se muestra puede ayudar a identificar problemas de flujo de datos cuando se intenta acceder a un servicio como, por ejemplo, un sitio Web. También se puede usar para realizar tareas como descarga de datos. Si hay varios sitios Web (espejos) disponibles para el mismo archivo de datos, se puede rastrear cada espejo para darse una buena idea de que espejo sería el más rápido para usar.

Dos rutas de rastreo entre el mismo origen y destino establecidas en diferentes momentos pueden producir distintos resultados. Esto se debe a la naturaleza ‘en malla’ de las redes interconectadas que componen internet y a la

capacidad de los protocolos de internet para seleccionar distintas rutas por las cuales enviar paquetes.

Por lo general, el sistema operativo del dispositivo final tiene herramientas de rastreo de rutas basadas en la línea de comandos integradas.

Otras herramientas, Como VisualRoute, son programas patentados que proporcionan información adicional. VisualRoute utiliza información disponible en la línea para mostrar la ruta gráficamente.

Esta práctica de laboratorio supone la instalación de VisualRoute.

3.4.1.3 Correlación Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.1 Orígenes y evolución.

1.2 Conceptos básicos de redes

3.4.1.4 Material Y Equipo Necesario

1. Pc (Windows 7, Vista o XP, con acceso a internet).

3.4.1.5 Metodología

Parte 1: Probar la conectividad de red mediante el comando ping

Paso 1: Determinar si hay posibilidad de conexión al servidor remoto

Para rastrear la ruta hacia una red distante, la PC que se utiliza debe tener una conexión a Internet en funcionamiento.

a. La primera herramienta que utilizaremos es ping. Ping es una herramienta que se utiliza para probar si hay posibilidad de conexión a un host. Se envían paquetes de información al host remoto con instrucciones de que responda. La PC local mide si se recibe una respuesta para cada paquete y cuánto tiempo tardan esos paquetes en atravesar la red. El nombre “ping” proviene de la tecnología de sonar activo en la cual un pulso de sonido se envía por debajo del agua y rebota en tierra o en otras embarcaciones.

b. En la PC, haga clic en el ícono Inicio de Windows, escriba cmd en el cuadro de diálogo Buscar programas y archivos y, a continuación, presione Entrar.

c. En el símbolo del sistema, escriba ping www.cisco.com

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

d. En la primera "nea de resultados, aparece el nombre de dominio completamente calificado (FUN) e144.dscb.akamaiedge net. A continuación, aparece la dirección IP 23.1.48.170. Cisco aloja el mismo contenido Web en diferentes servidores en todo el mundo (conocidos como espejos). Por lo tanto, según dónde se encuentre geográficamente, el FQDN y la dirección IP serán diferentes.
En cuanto a esta porción del resultado:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

e. Se enviaron cuatro pings y se recibió una respuesta de cada ping. Como se respondió cada ping, hubo una pérdida de paquetes del 0%. En promedio, los paquetes tardaron 54 ms (milisegundos) en cruzar la red. Un milisegundo es 1/1000.* de un segundo.
El streaming video y los juegos en línea son dos aplicaciones que se ven afectadas cuando hay pérdida de paquetes o una conexión de red lenta. Es posible determinar la velocidad de una conexión a Internet de manera más precisa al enviar 100 pings, en lugar de los cuatro predeterminados. Para ello, se debe hacer lo siguiente:

```
C:\>ping -n 100 www.cisco.com
```

Así se ve el resultado:

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

f. Ahora, haga ping a los sitios Web de registros regionales de Internet (RIR) en distintas partes del mundo: Para África:

```
C:\> ping www.afrinic.net
```

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Para Australia:

```
C:\> ping www.apnic.net
```

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Para Europa:

```
C:\> ping www.ripe.net
```

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Para América del Sur:

```
C:\> ping lacnic.net
```

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Parte 2: Rastrear una ruta a un servidor remoto mediante la herramienta Tracert

Paso 1: Determinar qué ruta a través del tráfico de Internet llega al servidor remoto

Ahora que se verificó la posiblidad de conexión básica utilizando la herramienta ping, resulta útil observar con mayor detalle cada segmento de red que se atraviesa. Para ello, se utilizará la herramienta tracert.

a. En el símbolo del sistema, escriba tracert www.cisco.com.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

b. Guarde el resultado de tracert en un archivo de texto de la siguiente manera:
   1. Haga clic con el botón secundario en la barra de título de la ventana del símbolo del sistema y seleccione Editar > Seleccionar todo.
   2. Vuelva a hacer clic con el botón secundario en la barra de título del símbolo del sistema y seleccione Editar > Copiar.
   3. Abra el programa Bloc de notas de Windows: ícono Inicio de Windows > Todos los programas > Accesorios > Bloc de notas.
   4. Para pegar el resultado en el bloc de notas, seleccione Editar > Pegar.
   5. Seleccione Archivo > Guardar como y guarde el archivo del bloc de notas en el escritorio con el nombre tracert1.txt

c. Ejecute tracert para cada sitio Web de destino y guarde el resultado en archivos numerados secuencialmente.

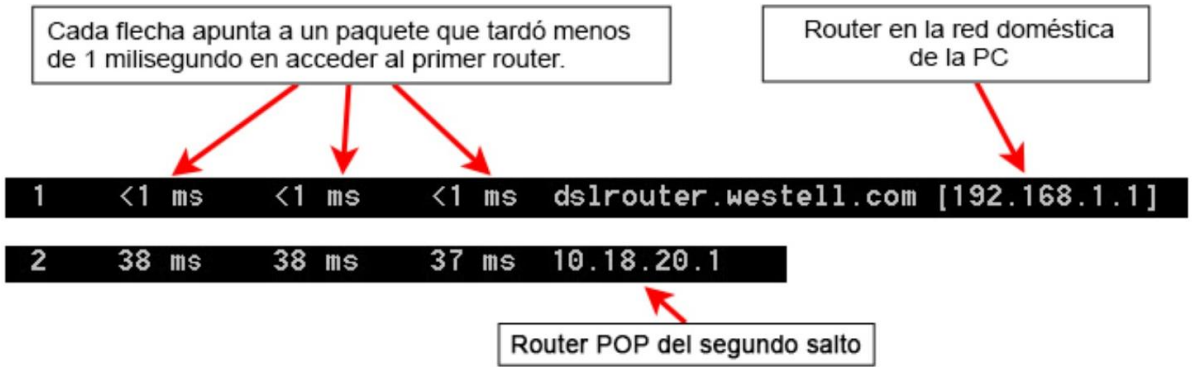
```
C:\> tracert www.afrinic.net
C:\> tracert www.lacnic.net
```

d. Interpretación de los resultados de tracert.
   Las rutas rastreadas pueden atravesar muchos saltos y distintos proveedores de servicios de Internet (1SP), según el tamaño del ISP y la ubicación de los hosts de origen y destino. Cada “salto” representa un router. Un router es un tipo especializado de computadora que se utiliza para dirigir el tráfico a través de Internet. Imagine que realiza un viaje en automóvil por varios países atravesando muchas carreteras. En distintos puntos del viaje, se encuentra con una bifurcación en el camino, donde debe optar entre varias carreteras diferentes. Ahora, imagine además que hay un dispositivo en cada

bifurcación del camino que lo orienta para tomar la carretera correcta hacia el destino final. Esto es lo que hace el router con los paquetes en una red.
Dado que las PC se comunican mediante números, en lugar de palabras, los routers se identifican de manera mediante direcciones IP (números con el formato xxx) exclusivas. La herramienta tracert muestra qué ruta toma un paquete de información a través de la red para llegar a su destino final. La herramienta tracert también le da una idea de la velocidad con la que avanza el tráfico en cada segmento de la red. Se envían tres paquetes a cada router en el trayecto, y el tiempo de retomo se mide en milisegundos. Ahora utilice esta información para analizar los resultados de tracert para www.cisco.com
El traceroute completo es el siguiente:

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

A continuación, se muestra el desglose:



En el resultado de ejemplo que se muestra arriba, los paquetes de tracert viajan desde la FC de origen hasta el gateway predeterminado del router local (salto 1: 192.168.1.1) y, desde allí, hasta el router de punto de presencia (POP) de ISP (salto 2: 10.18.20.1). Cada ISP tiene numerosos routers POP.

Estos routers POP se encuentran en el extremo de la red del ISP y son los medios por los cuales los clientes se conectan a Internet. Los paquetes viajan por la red de Verizon a través de dos saltos y, luego, saltan a un router que pertenece a alter.net. Esto podría significar que los paquetes viajaron a otro ISP. Esto es importante porque a veces se produce una pérdida de paquetes en la transición entre ISP, o a veces un ISP es más lento que otro. ¿Cómo podríamos determinar si alter.net es otro ISP o el mismo?

e. Existe una herramienta de Internet que se conoce como "whois". La herramienta whois nos permite determinar a quién pertenece un nombre de dominio. En http://whois.domaintools.com/, encontrará una herramienta whois basada en la Web. Según la herramienta whois basada en la Web, este dominio también pertenece a Verizon.

```
Registrant:
        Verizon Business Global LLC
        Verizon Business Global LLC
        One Verizon Way
         Basking Ridge NJ 07920
        US
         domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

    Domain Name: alter.net
```

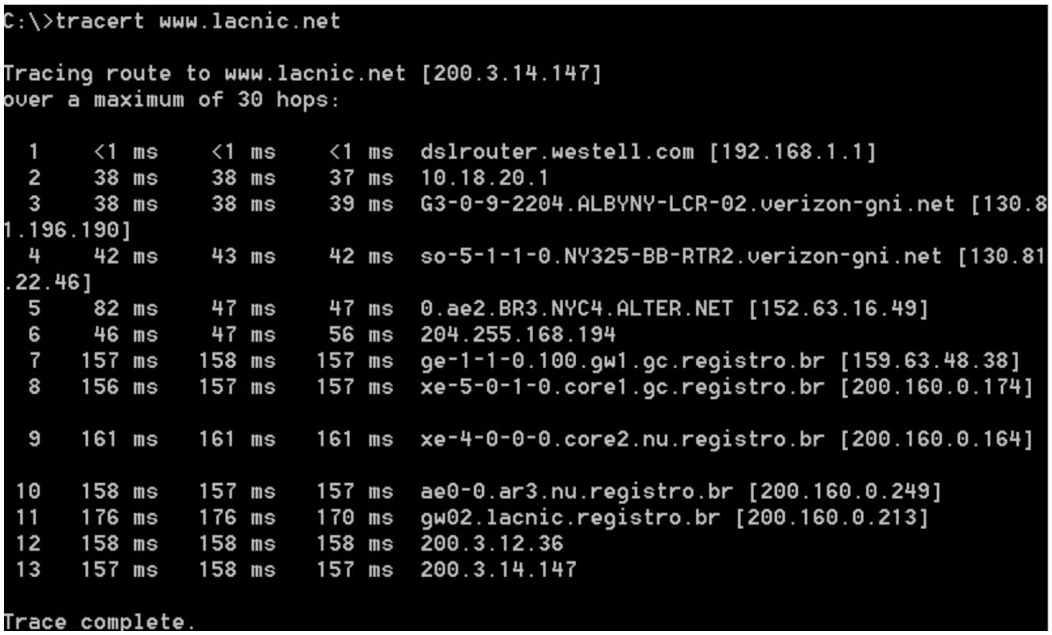
f. En resumen, el tráfico de Internet comienza en una PC doméstica y atraviesa el router doméstico (salto 1). Luego, se conecta al ISP y atraviesa la red (saltos de 2 a 7) hasta que llega al servidor remoto (salto 8). Este es un ejemplo relativamente inusual en el que solo participa un ISP desde el inicio hasta el final. Es común que haya dos o más ISP participantes, como se muestra en los ejemplos siguientes.

g. Ahora, examine un ejemplo en el que se incluye tráfico de Internet que pasa por varios ISP. A continuación, se muestra el comando tracert para www afrinic.net

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

¿Qué sucede en el salto 7? ¿level3 net es el mismo ISP que el de los saltos del 2 al 6 0 es un ISP diferente? Utilicé la herramienta whois para responder esta pregunta.
¿Qué sucede en el salto 10 con la cantidad de tiempo que le toma a un paquete viajar entre Washington D.C. y París, en comparación con los saltos anteriores (del 1 al 9)?
¿Qué sucede en el salto 18? Realice una búsqueda de whois para 168.209,201.74 utilizando la herramienta whois. ¿A quién pertenece esta red?

h. Escriba tracert www.lacnic.net



```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Parte 3: Rastrear una ruta a un servidor remoto mediante herramientas de software y herramientas basadas en Web

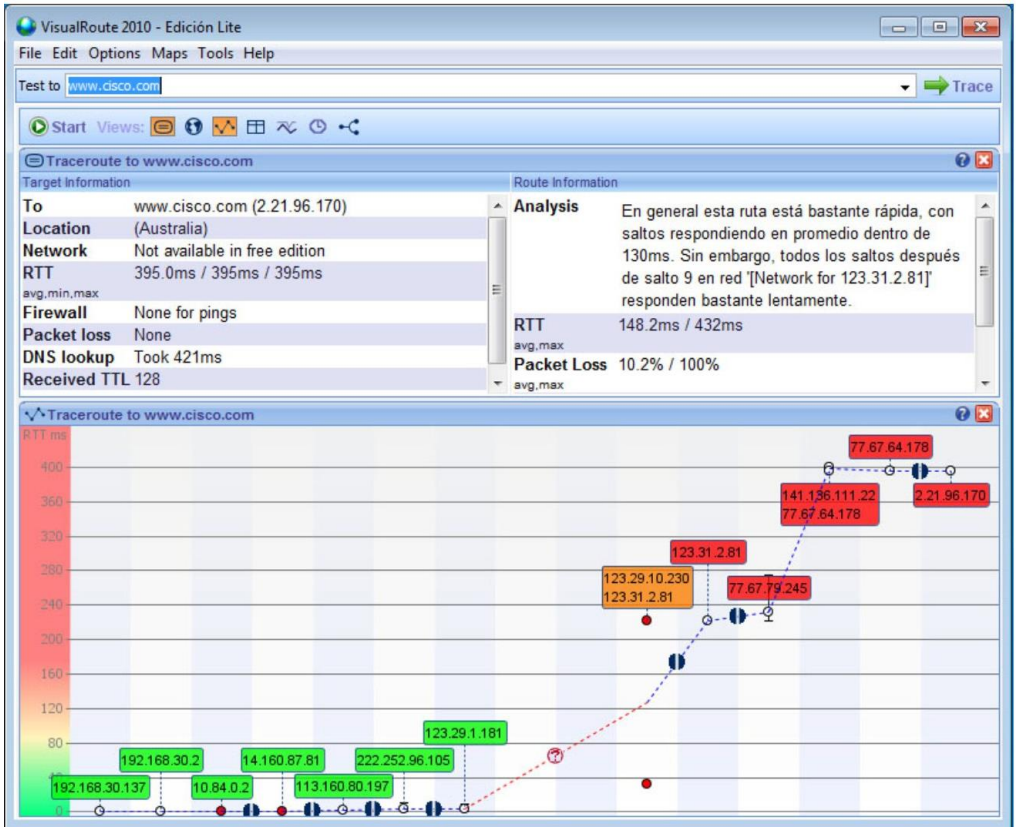
Paso 1: Utilizar una herramienta traceroute basada en la Web

a. Utilice h hp para rastrear la ruta a los siguientes sitios Web
www.cisco.com
wwwafrinic.net
Capture y guarde el resultado en el bloc de notas.
¿En qué se diferencia el comando traceroute cuando se accede a y desde el símbolo del sistema (consulte la parte 1) en lugar de hacerlo desde el sitio Web en línea? (Los resultados pueden variar dependiendo de dónde se encuentre geográficamente y de qué ISP proporcione conectividad al lugar de estudios)
Compare el comando tracert de la parte 1 que va a África con el comando tracert que va a África desde la interfaz Web ¿Qué diferencia advierte?
Algunos de los traceroutes contienen la abreviatura asymm. ¿Tiene alguna idea de a qué se refiere? ¿Qué significa?

Paso 2: Usar VisualRoute Lite Edition

VisualRoute es un programa traceroute patentado que puede mostrar gráficamente los resultados de la ruta de rastreo.

a. Si VisualRoute Lite Edition no está instalado, descárguelo del enlace siguiente:
   http://www visualroute.comidownload.himl
   Si tiene problemas para descargar o instalar VisualRoute, solicite ayuda al instructor. Asegúrese de descargar la edición Lite.
b. Rastree las rutas a www.cisco.com utilizando VisualRoute 2010 Lite Edition.
c. Registre las direcciones IP del trayecto en el bloc de notas.



3.4.1.6 Sugerencias Didácticas

- Se sugiere que el alumno tenga conocimientos básicos en redes de computadoras para poder cumplir con esta práctica.

3.4.1.7 Reporte Del Alumno

El alumno debe de realizar la actividad respondiendo a las preguntas que se le cuestionan durante el desarrollo de la práctica.

3.4.1.8 Bibliografías

Esta práctica de laboratorio supone la instalación de VisualRoute. Si la computadora que utiliza no tiene VisualRoute instalado, puede descargar el programa desde el siguiente enlace:

http://www.visualroute.com/download.html

3.4.2 Práctica 2 Navegación de IOS.

3.4.2.1 Objetivo

Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda.

Parte 2: Exploración de los modos EXEC.

Parte 3: Configuración del comando clock.

3.4.2.2 Introducción

En esta actividad, practicará las habilidades necesarias para navegar Cisco IOS, incluso distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicara el acceso a la ayuda contextual mediante la configuración del comando clock.

3.4.2.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.4.2.4 Material Y Equipo Necesario

Pc (Windows 7, Vista o XP, con acceso a internet).

3.4.2.5 Metodología

Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda

En la parte 1 de esta actividad, conectará una PC a un switch mediante una conexión de consola e investigará diferentes modos de comando y características de ayuda.

Paso 1: La conexión de la PC1 a S1 requiere un cable de consola.

a. Haga clic en el ícono **Connections** (Conexiones), similar a un rayo, en la esquina inferior izquierda de la ventana de Packet Tracer.

b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

c. Haga clic en **PC1**. Aparece una ventana que muestra una opción para una conexión RS-232.

d. Arrastre el otro extremo de la conexión de consola al switch S1 y haga clic en el switch para abrir la lista de conexiones.

e. Seleccione el puerto de consola para completar la conexión.

Paso 2: Establezca una sesión de terminal con el S1.

a. Haga clic en **PC1** y después en la ficha **Desktop** (Escritorio).

b. Haga clic en el ícono de la aplicación **Terminal**. Verifique que la configuración predeterminada de Port Configuration (Configuración del puerto) sea la correcta.

¿Cuál es el parámetro de bits por segundo?

c. Haga clic en **OK** (Aceptar).

d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga `Press RETURN to get started!` (Presione REGRESAR para comenzar). Presione **Entrar**.

¿Cuál es la petición de entrada que aparece en la pantalla?

Paso 3: Examine la ayuda de IOS.

a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina **Modo EXEC del usuario** y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

```
S1> ?
```

¿Qué comando comienza con la letra "C"?

b. En la petición de entrada, escriba **t**, seguido de un signo de interrogación (**?**).

```
S1> t?
```

¿Qué comandos se muestran?

c. En la petición de entrada, escriba **te**, seguido de un signo de interrogación (**?**).

```
S1> te?
```

¿Qué comandos se muestran?

Este tipo de ayuda se conoce como **ayuda contextual**, ya que proporciona más información a medida que se amplían los comandos.

Parte 2: Exploración de los modos EXEC

En la parte 2 de esta actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Ingrese al modo EXEC privilegiado.

a. En la petición de entrada, escriba el signo de interrogación (**?**).

```
S1> ?
```

¿Qué información de la que se muestra describe el comando **enable**?

b. Escriba **en** y presione la tecla **Tabulación**.

```
S1> en<Tab>
```

¿Qué se muestra después de presionar la tecla **Tabulación**?

Esto se denomina completar un comando o completar la tabulación. Cuando se escribe parte de un comando, la tecla **Tabulación** se puede utilizar para completar el comando parcial. Si los caracteres que se escriben son suficientes para formar un comando único, como en el caso del comando **enable**, se muestra la parte restante.

¿Qué ocurriría si escribiera **te<Tabulación>** en la petición de entrada?

c. Introduzca el comando **enable** y presione tecla **Entrar**. ¿En qué cambia la petición de entrada?

d. Cuando se le solicite, escriba el signo de interrogación (**?**).

```
S1# ?
```

Antes había un comando que comenzaba con la letra "C" en el modo EXEC del usuario. ¿Cuántos comandos se muestran ahora que está activo el modo EXEC privilegiado? (**Sugerencia**: puede escribir c? para que aparezcan solo los comandos que comienzan con la letra "C").

Paso 2: Ingresar en el modo de configuración global

a. Cuando se está en el modo EXEC privilegiado, uno de los comandos que comienzan con la letra "C" es **configure**. Escriba el comando completo o la cantidad de caracteres suficiente para formar el comando único; presione la tecla <**Tabulación**> para emitir el comando y, a continuación, la tecla **<Entrar>**.

```
S1# configure
```

¿Cuál es el mensaje que se muestra?

b. Presione la tecla **<Entrar>** para aceptar el parámetro predeterminado **[terminal]** entre corchetes.

¿En qué cambia la petición de entrada?

c. Esto se denomina "modo de configuración global". Este modo se analizará en más detalle en las próximas actividades y prácticas de laboratorio. Por el momento, escriba **end**, **exit** o **Ctrl-Z** para volver al modo EXEC privilegiado.

```
S1(config)# exit
S1#
```

Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock

a. Utilice el comando **clock** para explorar en más detalle la ayuda y la sintaxis de comandos. Escriba **show clock** en la petición de entrada de EXEC privilegiado.

```
S1# show clock
```

¿Qué información aparece en pantalla? ¿Cuál es el año que se muestra?

b. Utilice la ayuda contextual y el comando **clock** para establecer la hora del switch en la hora actual. Introduzca el comando **clock** y presione tecla **Entrar**.

```
S1# clock<ENTER>
```

¿Qué información aparece en pantalla?

c. El IOS devuelve el mensaje `% Incomplete command` (% comando incompleto), que indica que el comando **clock** necesita otros parámetros. Cuando se necesita más información, se puede proporcionar ayuda escribiendo un espacio después del comando y el signo de interrogación (?).

```
S1# clock ?
```

¿Qué información aparece en pantalla?

d. Configure el reloj con el comando **clock set**. Continúe utilizando este comando paso por paso.

```
S1# clock set ?
```

¿Qué información se solicita?

¿Qué información se habría mostrado si solo se hubiera ingresado el comando **clock set** y no se hubiera solicitado ayuda con el signo de interrogación?

e. Según la información solicitada al emitir el comando **clock set ?**, introduzca la hora 3:00 p. m. con el formato de 24 horas, 15:00:00. Revise si se necesitan otros parámetros.

```
S1# clock set 15:00:00 ?
```

El resultado devuelve la solicitud de más información:

```
<1-31>  Day of the month
MONTH   Month of the year
```

f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Es posible que para completar el proceso deba solicitar más ayuda mediante la ayuda contextual. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:

```
S1# show clock
*15:0:4.869 UTC Tue Jan 31 2035
```

g. Si no pudo lograrlo, pruebe con el siguiente comando para obtener el resultado anterior:

```
S1# clock set 15:00:00 31 Jan 2035
```

Paso 2: Explorar los mensajes adicionales del comando

a. El IOS proporciona diversos resultados para los comandos incorrectos o incompletos, como se vio en secciones anteriores. Continúe utilizando el comando **clock** para explorar los mensajes adicionales con los que se puede encontrar mientras aprende a utilizar el IOS.

b. Emita el siguiente comando y registre los mensajes:

```
S1# cl
```

¿Qué información se devolvió?

```
S1# clock
```

¿Qué información se devolvió?

```
S1# clock set 25:00:00
```

¿Qué información se devolvió?

```
S1# clock set 15:00:00 32
```

¿Qué información se devolvió?

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda	Paso 2a	5	
	Paso 2c	5	
	Paso 3a	5	
	Paso 3b	5	
	Paso 3c	5	
Total de la parte 1		**25**	
Parte 2: Exploración de los modos EXEC	Paso 1a	5	
	Paso 1b	5	
	Paso 1c	5	
	Paso 1d	5	
	Paso 2a	5	
	Paso 2b	5	
Total de la parte 2		**30**	
Parte 3: Configuración del comando clock	Paso 1a	5	
	Paso 1b	5	
	Paso 1c	5	
	Paso 1d	5	
	Paso 2b	5	
Total de la parte 3		**25**	
Puntuación de Packet Tracer		**20**	
Puntuación total		**100**	

3.4.2.6 Sugerencias Didácticas

- Se sugiere que el alumno tenga noción de lo que significa una red.

3.4.2.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando

detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.2.8 Bibliografías

- Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023, 25 agosto). Networking Academy. https://www.netacad.com/.

3.4.3 práctica 3 Establecimiento de una sesión de consola con Tera Term.

3.4.3.1 Objetivo

Parte 1: Acceder a un switch Cisco a través del puerto serie de consola.

Parte 2: Mostrar y configurar parámetros básicos de los dispositivos.

Parte 3: Acceder a un router Cisco mediante un cable de consola mini-USB (optativo).

3.4.3.2 Introducción

Se utiliza una variedad de modelos de switches y routers Cisco en redes de todo tipo. Estos dispositivos se administran mediante una conexión de consola local o una conexión remota. Casi todos los dispositivos Cisco tienen un puerto serie de consola al que el usuario puede conectarse. Algunos modelos más nuevos como el router de servicios integrados (ISR) 1941 G2, que se utiliza en esta práctica de laboratorio, también tienen un puerto de consola USB.

En esta práctica de laboratorio, aprenderá como acceder a un dispositivo Cisco a través de una conexión local directa al puerto de consola mediante un programa de emulación de terminal (Tera Term). También aprenderá a configurar los parámetros del puerto serie para la conexión de consola de Tera Term. Después de establecer una conexión de la consola con el dispositivo Cisco, puede ver o modificar la configuración del dispositivo. En está practica de laboratorio, solo mostrará los parámetros y configurará el reloj.

3.4.3.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.1 Orígenes y evolución y 1.2 Conceptos básicos de redes

3.4.3.4 Material Y Equipo Necesario

- Una PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term).

3.4.3.5 Metodología

Parte 1: Acceder a un switch Cisco a través del puerto serie de consola

Conectará una PC a un switch Cisco mediante un cable de consola. Esta conexión le permitirá acceder a la interfaz de línea de comandos (CLI) y mostrar los parámetros o configurar el switch.

Paso 1: Conectar un switch Cisco y una PC mediante un cable de consola

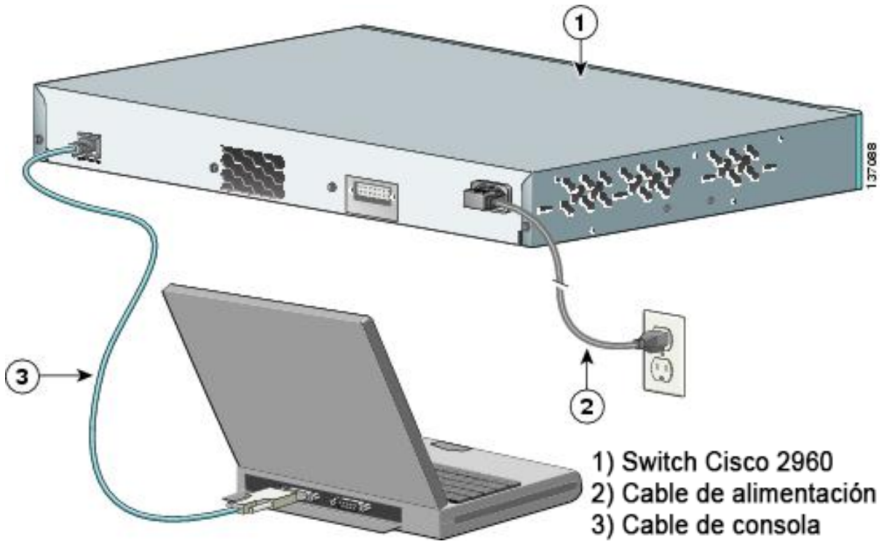
a. Conecte el cable de consola al puerto de consola RJ-45 del switch.

b. Conecte el otro extremo del cable al puerto serie COM de la PC.

Nota: la mayoría de las PC actuales no tienen puertos serie COM. Se puede utilizar un adaptador de USB a DB9 con el cable de consola para realizar la conexión de consola entre la PC y un dispositivo Cisco. Estos adaptadores de USB a DB9 pueden adquirirse en cualquier tienda de electrónica informática.

Nota: si utiliza un adaptador de USB a DB9 para conectar el puerto COM, puede ser necesario instalar un controlador para el adaptador proporcionado por el fabricante de la PC. Para determinar el puerto COM que utiliza el adaptador, consulte el paso 4 de la parte 3. Se requiere el número de puerto COM correcto para conectar el dispositivo Cisco IOS por medio de un emulador de terminal en el paso 2.

c. Si aún no están encendidos, encienda el switch Cisco y la PC.



Paso 2: Configurar Tera Term para establecer una sesión de consola con el switch

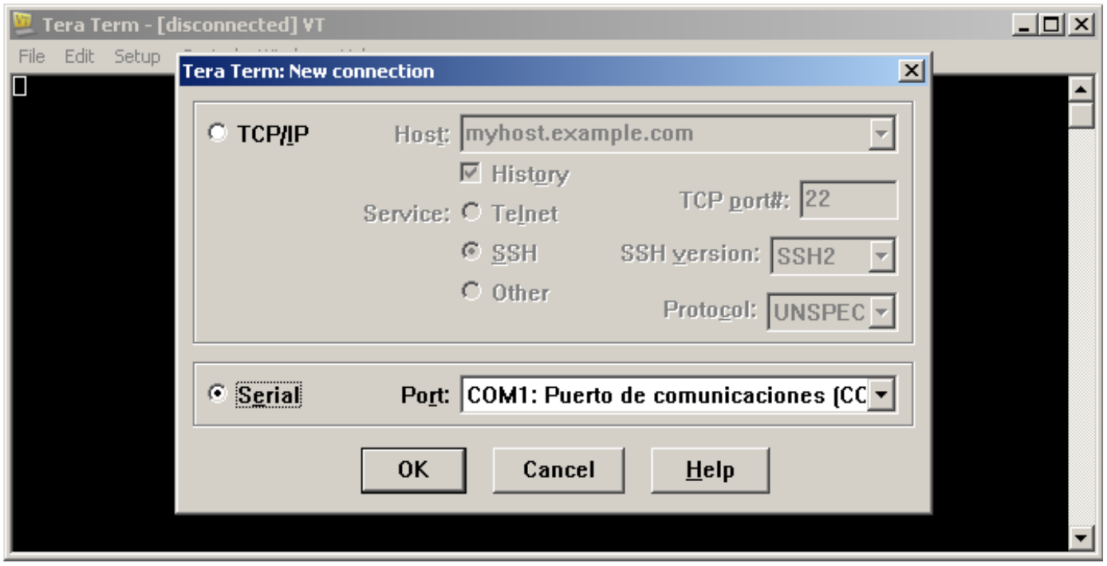
Tera Term es un programa de emulación de terminal. Este programa le permite acceder al resultado para la terminal del switch y también le permite configurar el switch.

a. Inicie Tera Term haciendo clic en el botón **Inicio de Windows**, situado en la barra de tareas. Localice **Tera Term** en **Todos los programas**.

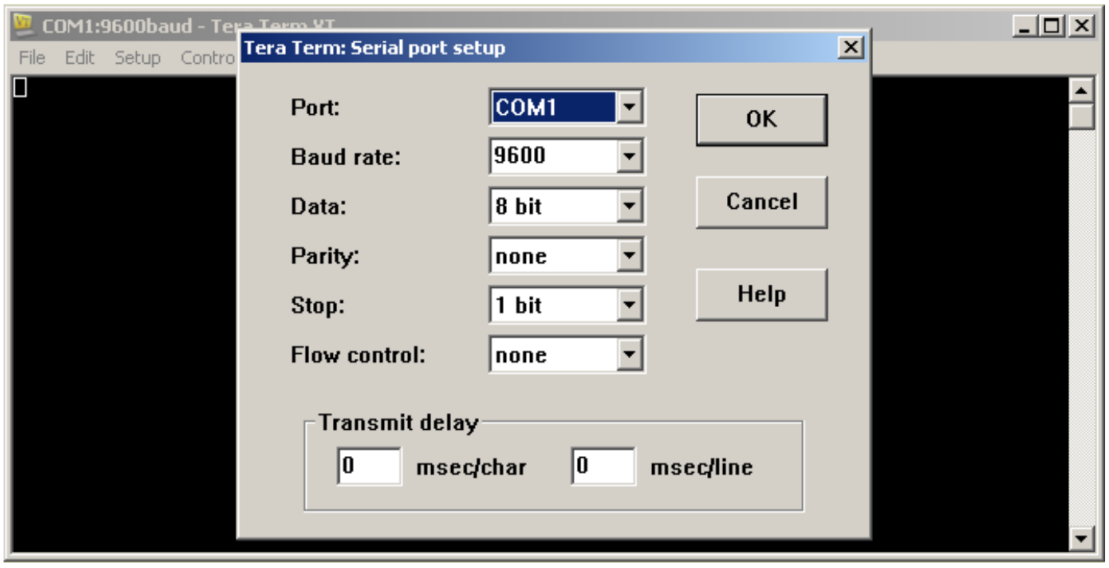
Nota: si no está instalado en el sistema, Tera Term se puede descargar del siguiente enlace seleccionando **Tera Term**:

http://logmett.com/index.php?/download/free-downloads.html

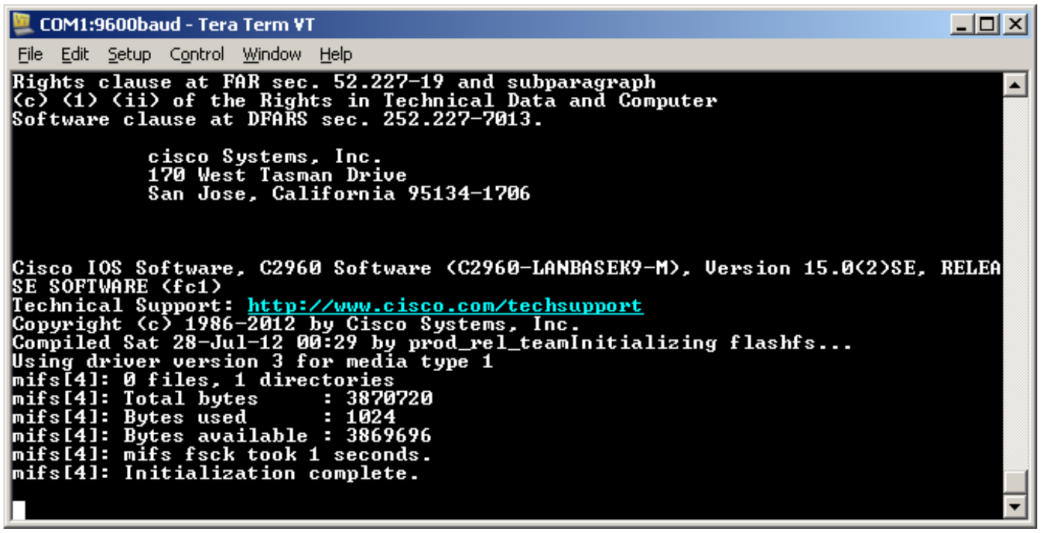
b. En el cuadro de diálogo New Connection (Conexión nueva), haga clic en el botón de opción **Serial**. Verifique que esté seleccionado el puerto COM correcto y haga clic en **OK** (Aceptar) para continuar.



c. En el menú **Setup** (Configuración) de Tera Term, seleccione **Serial port...** (Puerto serie) para verificar los parámetros de serie. Los parámetros predeterminados para el puerto de consola son 9600 baudios, 8 bits de datos, ninguna paridad, 1 bit de parada y ningún control del flujo. Los parámetros predeterminados de Tera Term coinciden con los parámetros del puerto de consola para las comunicaciones con el switch Cisco IOS.



d. Cuando pueda ver el resultado de terminal, estará listo para configurar un switch Cisco. El siguiente ejemplo de la consola muestra el resultado para la terminal del switch durante la carga.



Parte 2: Mostrar y configurar parámetros básicos de los dispositivos

En esta sección, se le presentan los modos de ejecución privilegiado y de usuario. Debe determinar la versión del Sistema operativo Internetwork (IOS), mostrar los parámetros del reloj y configurar el reloj en el switch.

Paso 1: Mostrar la versión de la imagen del IOS del switch

a. Una vez que el switch completa el proceso de inicio, se muestra el siguiente mensaje (introduzca **n** para continuar).

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Nota: si no ve el mensaje que se muestra arriba, consulte con el instructor para restablecer el switch a la configuración inicial.

b. En el modo EXEC del usuario, muestre la versión del IOS para el switch.

```
Switch> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"
<resultado omitido>
```

¿Qué versión de la imagen del IOS utiliza actualmente el switch?

Paso 2: Configurar el reloj.

A medida que aprenda más sobre redes, verá que configurar la hora correcta en un switch Cisco puede resultar útil cuando trabaja en la resolución de problemas. Mediante los siguientes pasos, se configura manualmente el reloj interno del switch.

a. Muestre la configuración actual del reloj.

```
Switch> show clock
*00:30:05.261 UTC Mon Mar 1 1993
```

b. La configuración del reloj se cambia en el modo EXEC privilegiado. Para acceder al modo EXEC privilegiado, escriba **enable** en la petición de entrada del modo EXEC del usuario.

```
Switch> enable
```

c. Configure los parámetros del reloj. El signo de interrogación (?) proporciona ayuda y le permite determinar la información de entrada esperada para configurar la hora, la fecha y el año actuales. Presione Entrar para completar la configuración del reloj.

```
Switch# clock set ?
  hh:mm:ss  Current Time

Switch# clock set 15:08:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year

Switch# clock set 15:08:00 Oct 26 ?
  <1993-2035>  Year

Switch# clock set 15:08:00 Oct 26 2012
Switch#
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43
UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by
console.
```

d. Introduzca el comando **show clock** para verificar que los parámetros del reloj se hayan actualizado.

```
Switch# show clock
15:08:07.205 UTC Fri Oct 26 2012
```

Parte 3: Acceder a un router Cisco mediante un cable de consola mini-USB (optativo)

Si utiliza un router Cisco 1941 u otros dispositivos Cisco IOS con un puerto de consola mini-USB, puede acceder al puerto de consola del dispositivo mediante un cable mini-USB conectado al puerto USB en su PC.

Nota: el cable de consola mini-USB es el mismo tipo de cable mini-USB que se utiliza con otros dispositivos electrónicos, como discos duros USB, impresoras USB o hubs USB. Estos cables mini-USB pueden adquirirse a través de Cisco Systems, Inc. o de otros proveedores externos. Asegúrese de utilizar un cable mini-USB (y no un cable micro-USB) para conectarse al puerto de consola mini-SUB en un dispositivo Cisco IOS.

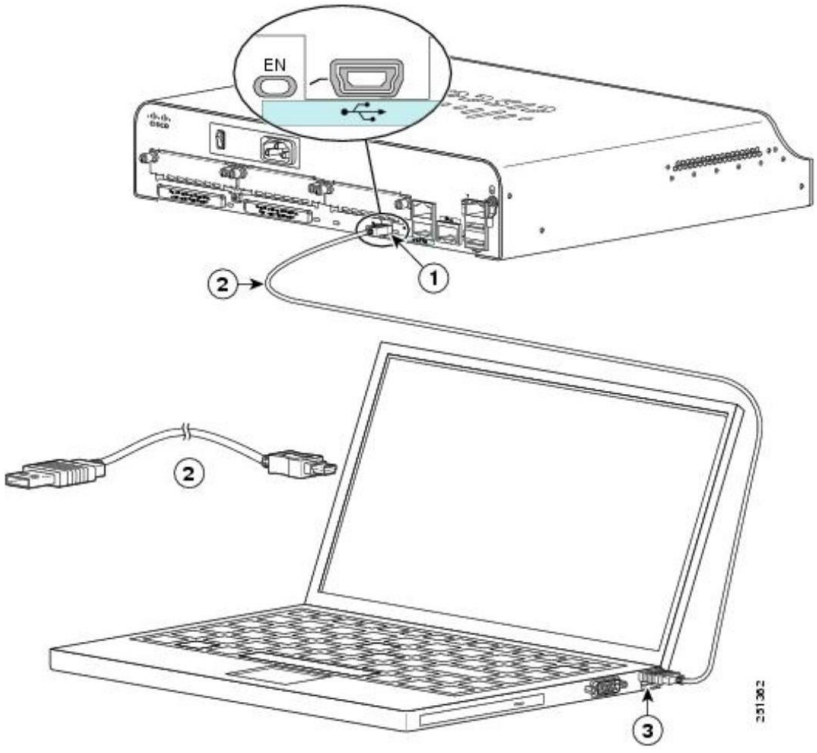
Nota: debe utilizar el puerto USB o el puerto RJ-45; no se deben usar ambos de manera simultánea. Cuando se utiliza el puerto USB, tiene prioridad sobre el puerto de consola RJ-45 usado en la parte 1.

Paso 1: Configurar la conexión física con un cable mini-USB

a. Conecte el cable mini-USB al puerto de consola mini-USB del router.

b. Conecte el otro extremo del cable a un puerto USB de la PC.

c. Si aún no están encendidos, encienda el router Cisco y la PC.



1) Puerto de consola USB tipo B mini de 5 pines
2) Cable de consola USB tipo B mini de 5 pines a USB tipo A
3) Conector USB tipo A

Paso 2: Verificar que la consola USB está lista

Si utiliza una PC con Microsoft Windows y el indicador LED del puerto de consola USB (con el rótulo EN) no se vuelve de color verde, instale el controlador de consola USB de Cisco.

En PC con Microsoft Windows conectadas a un dispositivo Cisco IOS con un cable USB, se debe instalar un controlador USB antes de su uso. El controlador se puede encontrar en www.cisco.com con el dispositivo Cisco IOS relacionado. El controlador USB se puede descargar en el siguiente enlace:

http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Nota: para descargar este archivo, debe tener una cuenta válida de Cisco Connection Online (CCO).

Nota: este enlace está relacionado con el router Cisco 1941; sin embargo, el controlador de consola USB no es específico del modelo de dispositivo Cisco IOS. Este controlador de consola USB funciona solamente con switches y routers Cisco. Para finalizar la instalación del controlador USB, se debe reiniciar la PC.

Nota: una vez extraídos los archivos, la carpeta contiene instrucciones de instalación y remoción, y los controladores necesarios para los distintos sistemas operativos y arquitecturas. Seleccione la versión adecuada para su sistema.

Cuando el indicador LED del puerto de consola USB se vuelve de color verde, el puerto está listo para el acceso.

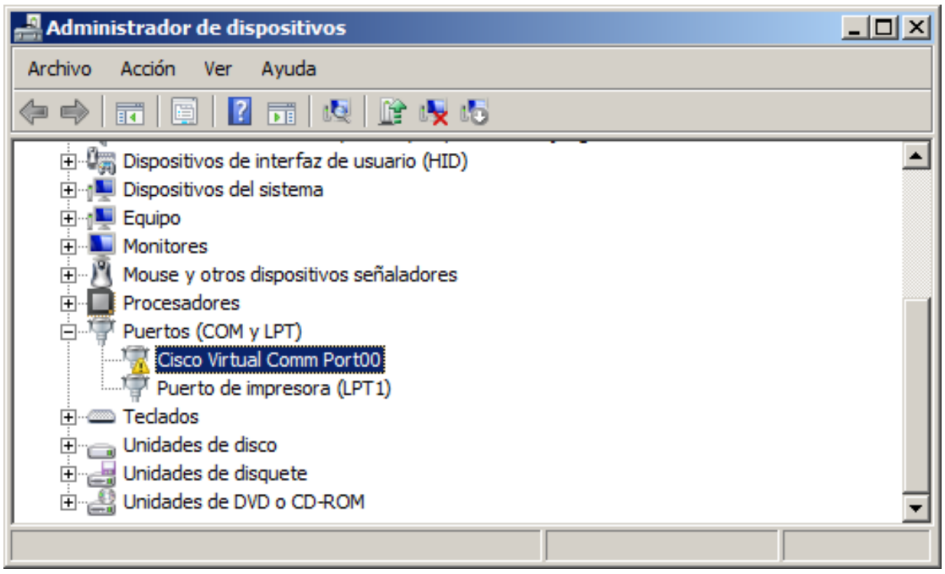
Paso 3: Habilitar el puerto COM para la PC con Windows 7 (optativo)

Si utiliza una PC con Microsoft Windows 7, tal vez necesita realizar los siguientes pasos para habilitar el puerto COM:

a. Haga clic en el ícono de **Inicio de Microsoft** para acceder al **Panel de control**.

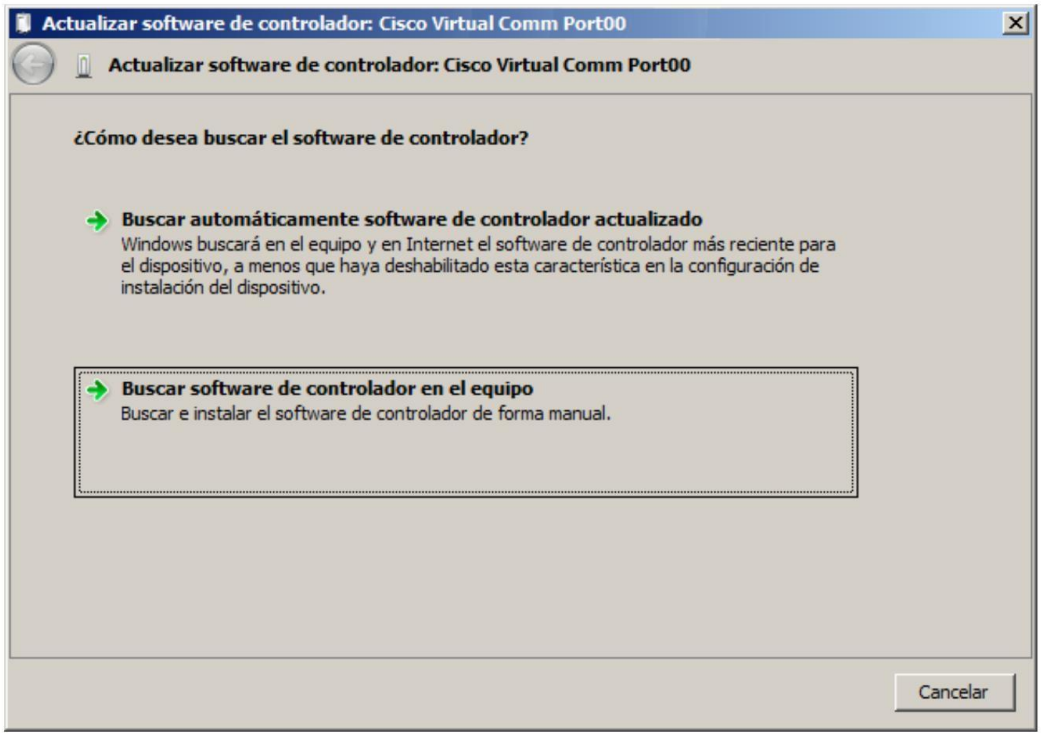
b. Abra el **Administrador de dispositivos**.

c. Haga clic en el enlace de árbol **Puertos (COM y LPT)** para expandirlo. Aparecerá el ícono de **Cisco Virtual Comm Port00** con un signo de exclamación amarillo.

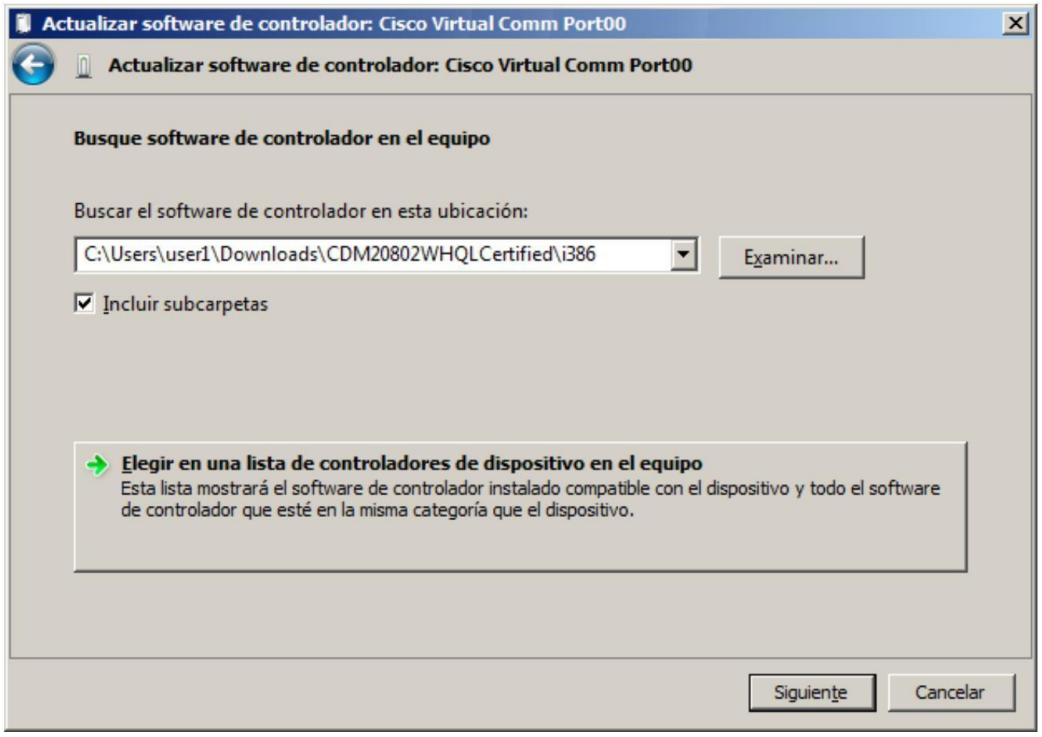


d. Para resolver el problema, haga clic con el botón secundario en el ícono **Cisco Virtual Comm Port00** y seleccione **Actualizar software de controlador**.

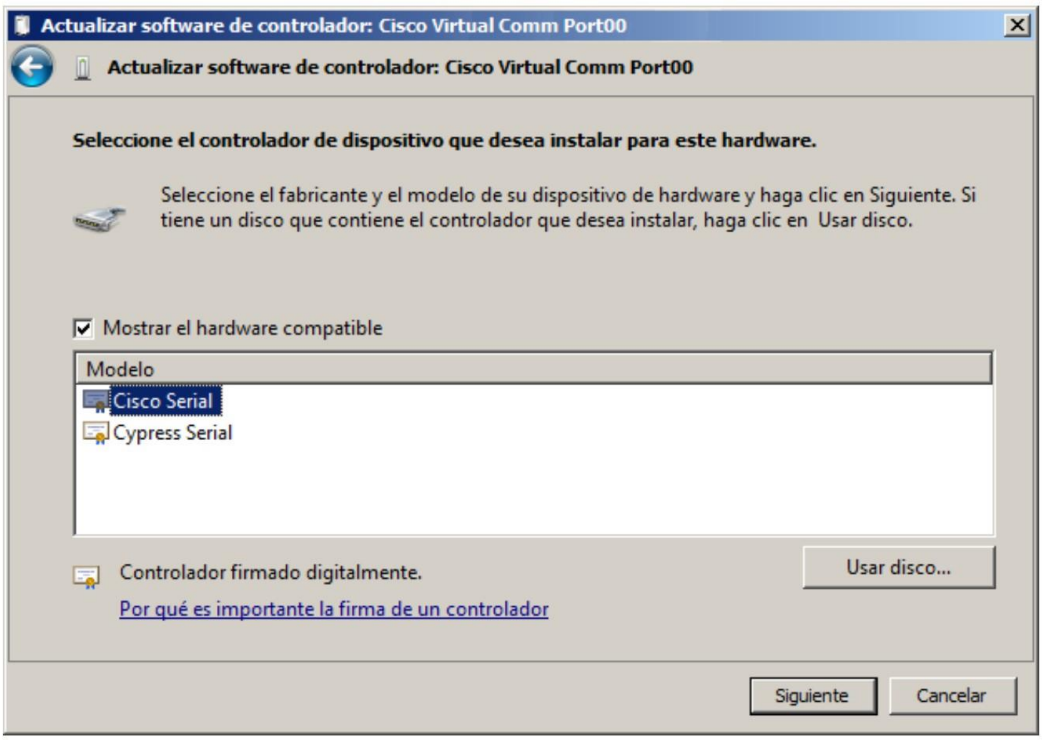
e. Seleccione **Buscar software de controlador en el equipo**.



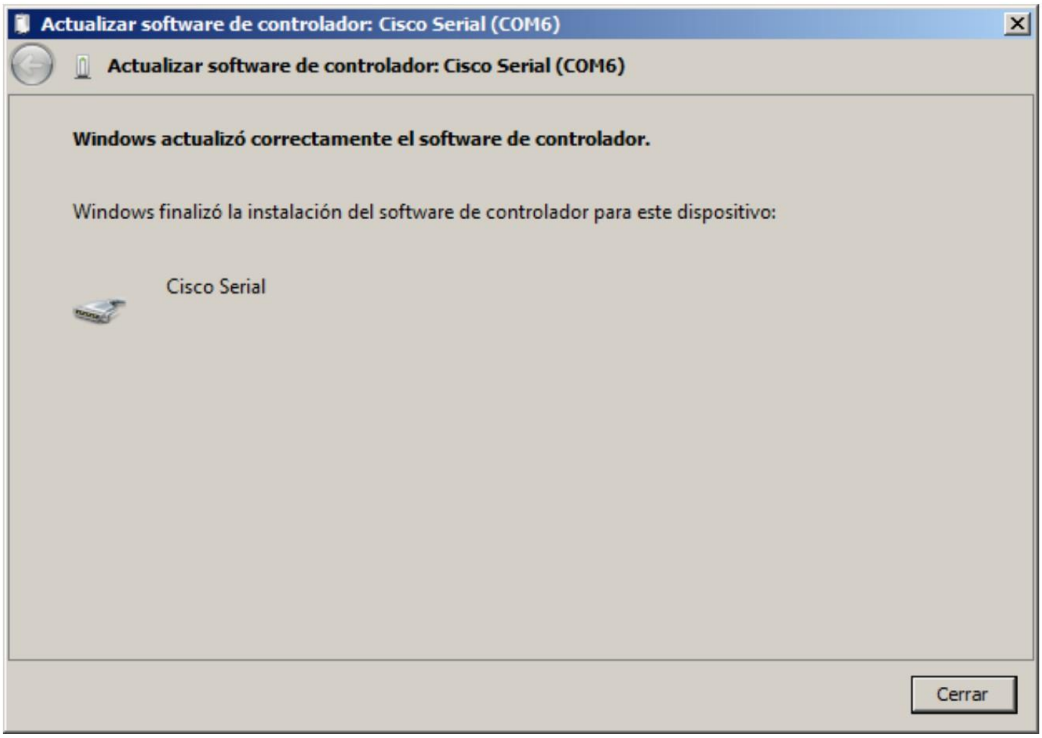
f. Seleccione **Elegir en una lista de controladores de dispositivo en el equipo** y haga clic en **Siguiente**.



g. Seleccione el controlador **Cisco Serial** y haga clic en **Siguiente**.

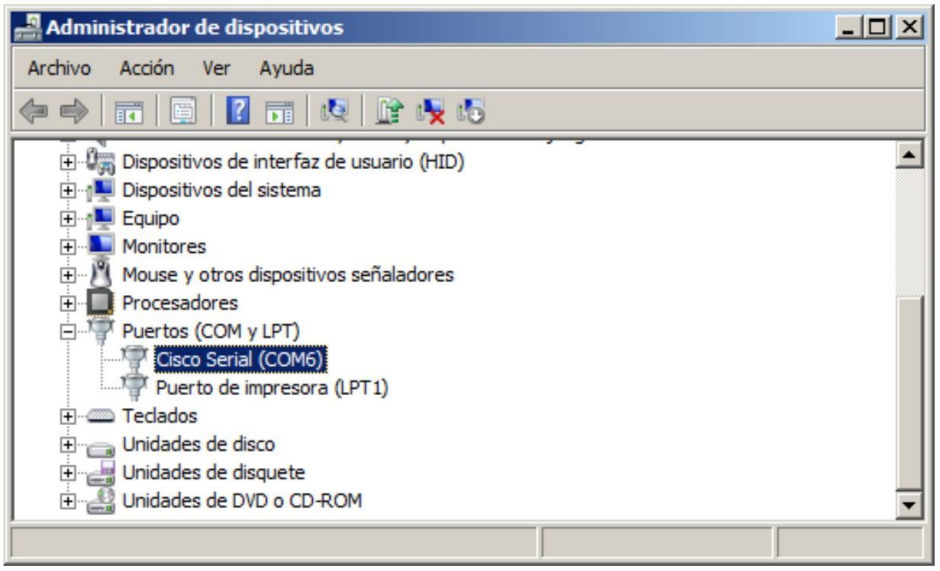


h. El controlador de dispositivo se instaló correctamente. Tome nota del número de puerto asignado en la parte superior de la ventana. En este ejemplo, se utiliza COM 6 para la comunicación con el router. Haga clic en **Cerrar**.

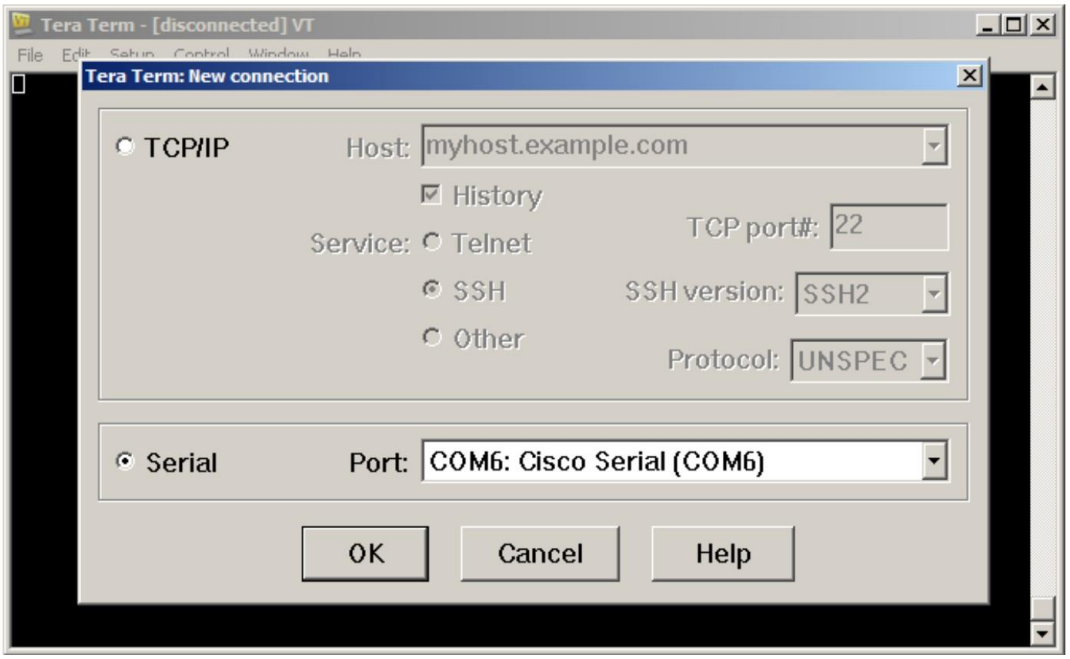


Paso 4: Determinar el número de puerto COM (optativo)

a. Si necesita determinar el número de puerto COM, abra el **Panel de control** y seleccione **Administrador de dispositivos**. Busque el encabezado **Puertos (COM y LPT)**, expándalo y determine el número de puerto COM que está en uso. En este ejemplo, se seleccionó **Cisco Serial (COM 6)** para la conexión al router, dado que hay un controlador de consola USB de Cisco en uso. Si utiliza un cable de consola o un adaptador de otro fabricante, esa información se refleja en la convención de nomenclatura.



b. Abra Tera Term. Haga clic en el botón de opción **Serial** y seleccione **Port COM6: Cisco Serial (COM 6**) (Puerto COM6: Cisco Serial [COM 6]). Este puerto ahora debe estar disponible para la comunicación con el router. Haga clic en **OK** (Aceptar).



Reflexión

1. ¿Cómo evita que personal no autorizado acceda a su dispositivo Cisco a través del puerto de consola?

2. ¿Cuáles son las ventajas y desventajas de usar la conexión serial de consola en comparación con la conexión USB de consola a un switch o un router Cisco?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

3.4.3.6 Sugerencias Didácticas

- Para esta actividad ya debemos contar con nuestra cuenta Azure.

3.4.3.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.3.8 Bibliografías

- Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023, 25 agosto). Networking Academy. https://www.netacad.com/

3.4.4 Práctica 4 Configuración de los parámetros iniciales del switch

3.4.4.1 Objetivo

Parte 1: Verificar la configuración predeterminada del switch.

Parte 2: Establecer una configuración básica del switch.

Parte 3: Configurar un título de MOTD.

Parte 4: Guardar los archivos de configuración en la NVRAM.

Parte 5: Configurar el S2.

3.4.4.2 Introducción

En esta actividad, realizará configuraciones básicas del switch. Protegerá el acceso a la interfaz de línea de comandos (CLI, command-line Interface) y a los puertos de la consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También aprenderá cómo configurar mensajes para los usuarios que inician sesión en el switch. Estos avisos también se utilizan para advertir a usuarios no autorizados que el acceso está prohibido.

3.4.4.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.1 Orígenes y evolución y 1.2 Conceptos básicos de redes

3.4.4.4 Material Y Equipo Necesario

1. Pc conectada a internet.

3.4.4.5 Metodología

Parte 1: Verificar la configuración predeterminada del switch

Paso 1: Entre al modo privilegiado.

Puede acceder a todos los comandos del switch en el modo privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene el acceso a los modos de comando restantes.

a. Haga clic en **S1** y, a continuación, en la ficha **CLI**. Presione **<Entrar>**.

b. Ingrese al modo EXEC privilegiado introduciendo el comando **enable**:

```
Switch> enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Paso 2: Examine la configuración actual del switch.

a. Ingrese el comando **show running-config**.

```
Switch# show running-config
```

b. Responda las siguientes preguntas:

¿Cuántas interfaces FastEthernet tiene el switch?

¿Cuántas interfaces Gigabit Ethernet tiene el switch?

¿Cuál es el rango de valores que se muestra para las líneas vty?

¿Qué comando muestra el contenido actual de la memoria de acceso aleatorio no volátil (NVRAM)?

¿Por qué el switch responde con `startup-config is not present`?

Parte 2: Crear una configuración básica del switch

Paso 1: Asignar un nombre a un switch

Para configurar los parámetros de un switch, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el switch.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Paso 2: Proporcionar un acceso seguro a la línea de consola

Para proporcionar un acceso seguro a la línea de la consola, acceda al modo config-line y establezca la contraseña de consola en **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

¿Por qué se requiere el comando **login**?

Paso 3: Verifique que el acceso a la consola sea seguro.

Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.

```
S1# exit
```

```
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Nota: si el switch no le pidió una contraseña, entonces no se configuró el parámetro **login** en el paso 2.

Paso 4: Proporcionar un acceso seguro al modo privilegiado

Establezca la contraseña de **enable** en **c1$c0**. Esta contraseña protege el acceso al modo privilegiado.

Nota: el **0** en **c1$c0** es un cero, no una O mayúscula. Esta contraseña no calificará como correcta hasta que se la encripte tal como se indica en el paso 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Paso 5: Verificar que el acceso al modo privilegiado sea seguro

a. Introduzca el comando **exit** nuevamente para cerrar la sesión del switch.

b. Presione **<Entrar>**; a continuación, se le pedirá que introduzca una contraseña:

```
User Access Verification
Password:
```

c. La primera contraseña es la contraseña de consola que configuró para **line con 0**. Introduzca esta contraseña para volver al modo EXEC del usuario.

d. Introduzca el comando para acceder al modo privilegiado.

e. Introduzca la segunda contraseña que configuró para proteger el modo EXEC privilegiado.

f. Para verificar la configuración, examine el contenido del archivo de configuración en ejecución:

```
S1# show running-configuration
```

Observe que las contraseñas de consola y de enable son de texto no cifrado. Esto podría presentar un riesgo para la seguridad si alguien está viendo lo que hace.

Paso 6: Configure una contraseña encriptada para proporcionar un acceso seguro al modo privilegiado.

La **contraseña de enable** se debe reemplazar por una nueva contraseña secreta encriptada mediante el comando **enable secret**. Establezca la contraseña secreta de enable en **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Nota: la contraseña **secreta de enable** sobrescribe la contraseña de **enable**. Si ambas están configuradas en el switch, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Paso 7: Verificar si la contraseña secreta de enable se agregó al archivo de configuración

a. Introduzca el comando **show running-configuration** nuevamente para verificar si la nueva contraseña **secreta de enable** está configurada.

Nota: puede abreviar el comando **show running-configuration** de la siguiente manera:

```
S1# show run
```

b. ¿Qué se muestra como contraseña **secreta de enable**?

c. ¿Por qué la contraseña **secreta de enable** se ve diferente de lo que se configuró?

Paso 8: Encriptar las contraseñas de consola y de enable

Como pudo observar en el paso 7, la contraseña **secreta de enable** estaba encriptada, pero las contraseñas de **enable** y de **consola** aún estaban en texto no cifrado. Ahora encriptaremos estas contraseñas de texto no cifrado con el comando **service password-encryption**.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma encriptada en el archivo de configuración? Explique por qué.

Parte 3: Configurar un título de MOTD

Paso 1: Configurar un mensaje del día (MOTD).

El conjunto de comandos IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se denominan “mensajes del día” o “mensajes MOTD”. Encierre el texto del mensaje entre comillas o utilice un delimitador diferente de cualquier carácter que aparece en la cadena de MOTD.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"

S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

¿Cuándo se muestra este mensaje?

¿Por qué todos los switches deben tener un mensaje MOTD?

Parte 4: Guardar los archivos de configuración en la NVRAM

Paso 1: Verificar que la configuración sea precisa mediante el comando show run

Paso 2: Guardar el archivo de configuración

Usted ha completado la configuración básica del switch. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

```
S1# copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

¿Cuál es la versión abreviada más corta del comando **copy running-config startup-config**?

Paso 3: Examinar el archivo de configuración de inicio

¿Qué comando muestra el contenido de la NVRAM?

¿Todos los cambios realizados están grabados en el archivo?

Parte 5: Configurar S2

Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.

Configure el S2 con los siguientes parámetros:

a. Nombre del dispositivo: **S2**

b. Proteja el acceso a la consola con la contraseña **letmein**.

c. Configure la contraseña **c1$c0** para enable y la contraseña secreta de enable, **itsasecret**.

d. Configure el siguiente mensaje para aquellas personas que inician sesión en el switch:

```
Acceso autorizado únicamente. Unauthorized access is prohibited and
violators will be prosecuted to the full extent of the law.
```

e. Encripte todas las contraseñas de texto no cifrado.

f. Asegúrese de que la configuración sea correcta.

g. Guarde el archivo de configuración para evitar perderlo si el switch se apaga.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Verificar la configuración predeterminada del switch	Paso 2b, p1	2	
	Paso 2b, p2	2	
	Paso 2b, p3	2	
	Paso 2b, p4	2	
	Paso 2b, p5	2	
	Total de la parte 1	**10**	
Parte 2: Crear una configuración básica del switch	Paso 2	2	
	Paso 7b	2	
	Paso 7c	2	
	Paso 8	2	
	Total de la parte 2	**8**	
Parte 3: Configurar un título de MOTD	Paso 1, pregunta 1	2	
	Paso 1, pregunta 2	2	
	Total de la parte 3	**4**	
Parte 4: Guardar los archivos de configuración en la NVRAM	Paso 2	2	
	Paso 3, p1	2	
	Paso 3, p2	2	
	Total de la parte 4	**6**	
	Puntuación de Packet Tracer	**72**	
	Puntuación total	**100**	

3.4.4.6 Sugerencias Didácticas

- Para esta actividad debe de contar con el programa de Packet Tracer versión 7.8.

3.4.4.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.4.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.5 Práctica 5 Implementación de conectividad básica

3.4.5.1 Objetivo

Parte 1: Realizar una configuración básica en S1 y S2.

Parte 2: Configurar la PC.

Parte 3: Configurar la interfaz de administración de switches.

3.4.5.2 Introducción

En esta actividad, primero realizará configuraciones básicas del switch. A continuación, implementará conectividad básica mediante la configuración del direccionamiento IP en switches y PC. Cuando haya finalizado la configuración del direccionamiento IP, utilizará diversos comandos show para revisar las configuraciones y utilizará el comando ping para verificar la conectividad básica entre los dispositivos.

3.4.5.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

5.1 Memoria técnica

5.2 Análisis de necesidades y requerimientos.

3.4.5.4 Material Y Equipo Necesario

1. Equipo De Cómputo.

3.4.5.5 Metodología

Parte 1: Realizar una configuración básica en el S1 y el S2

Complete los siguientes pasos en el S1 y el S2.

Paso 1: Configurar un nombre de host en el S1

a. Haga clic en **S1** y, a continuación, haga clic en la ficha **CLI**.

b. Introduzca el comando correcto para configurar el nombre de host **S1**.

Paso 2: Configurar las contraseñas de consola y del modo EXEC privilegiado

a. Use **cisco** para la contraseña de consola.

b. Use **class** para la contraseña del modo EXEC privilegiado.

Paso 3: Verificar la configuración de contraseñas para el S1

¿Cómo puede verificar que ambas contraseñas se hayan configurado correctamente?

Paso 4: Configurar un mensaje del día (MOTD).

Utilice un texto de aviso adecuado para advertir contra el acceso no autorizado. El siguiente texto es un ejemplo:

Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley.

Paso 5: Guarde el archivo de configuración en la NVRAM.

¿Qué comando emite para realizar este paso?

Paso 6: Repetir los pasos 1 a 5 para el S2

Parte 2: Configurar las PC

Configure la PC1 y la PC2 con direcciones IP.

Paso 1: Configurar ambas PC con direcciones IP

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).

b. Haga clic en **IP Configuration** (Configuración de IP). En la **tabla de direccionamiento** anterior, puede ver que la dirección IP para la PC1 es 192.168.1.1 y la máscara de subred es 255.255.255.0. Introduzca esta información para la PC1 en la ventana **IP Configuration**.

c. Repita los pasos 1a y 1b para la PC2.

Paso 2: Probar la conectividad a los switches

a. Haga clic en **PC1**. Cierre la ventana **IP Configuration** si todavía está abierta. En la ficha **Desktop**, haga clic en **Command Prompt** (Símbolo del sistema). .

b. Escriba el comando **ping** y la dirección IP para el S1 y presione **Entrar**.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.253
```

¿Tuvo éxito? ¿Por qué o por qué no?

Parte 3: Configurar la interfaz de administración de switches

Configure el S1 y el S2 con una dirección IP.

Paso 1: Configurar el S1 con una dirección IP

Los switches se pueden usar como dispositivos Plug and Play, lo que significa que no es necesario configurarlos para que funcionen. Los switches reenvían información desde un puerto hacia otro sobre la base de direcciones de control de acceso al medio (MAC). Por lo tanto, ¿para qué lo configuraríamos con una dirección IP?

Use los siguientes comandos para configurar el S1 con una dirección IP.

```
S1 #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

¿Por qué debe introducir el comando **no shutdown**?

Paso 2: Configurar el S2 con una dirección IP

Use la información de la tabla de direccionamiento para configurar el S2 con una dirección IP.

Paso 3: Verificar la configuración de direcciones IP en el S1 y el S2

Use el comando **show ip interface brief** para ver la dirección IP y el estado de todos los puertos y las interfaces del switch. También puede utilizar el comando **show running-config**.

Paso 4: Guardar la configuración para el S1 y el S2 en la NVRAM

¿Qué comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM?

Paso 5: Verificar la conectividad de la red

La conectividad de red se puede verificar mediante el comando **ping**. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Haga ping a la dirección IP del S1 y el S2 desde la PC1 y la PC2.

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).

b. Haga clic en **Command Prompt**.

c. Haga ping a la dirección IP de la PC2.

d. Haga ping a la dirección IP del S1.

e. Haga ping a la dirección IP del S2.

Nota: también puede usar el mismo comando **ping** en la CLI del switch y en la PC2.

Todos los ping deben tener éxito. Si el resultado del primer ping es 80%, vuelva a intentarlo; ahora debería ser 100%. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede hacer ping a ninguno de los dispositivos, vuelva a revisar la configuración para detectar errores.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Realizar una configuración básica en S1 y S2	Paso 3	2	
	Paso 5	2	
Paso 2: Configurar la PC	Paso 2b	2	
Parte 3: Configurar la interfaz de administración de switches	Paso 1, pregunta 1	2	
	Paso 1, pregunta 2	2	
	Paso 4	2	
	Preguntas	**12**	
	Puntuación de Packet Tracer	**88**	
	Puntuación total	**100**	

3.4.5.6 Sugerencias Didácticas

- Para esta actividad se debe de contar con el programa Packet Tracer versión 7.8.

3.4.5.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.5.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.6 Práctica 6 Creación de una red simple

3.4.6.1 Objetivo

Parte 1: Configurar la topología de la red (Ethernet únicamente).

Parte 2: Configurar hosts en las PC.

Parte 3: Configurar y verificar los parámetros básicos del switch.

3.4.6.2 Introducción

Las redes están formadas por tres componentes principales: hosts, switches y routers. En esta práctica de laboratorio, armará una red simple con dos hosts y dos switches. También configurará parámetros básicos, incluidos nombres de host, contraseñas locales y mensaje de inicio de sesión. Utilice los comandos show para mostrar la configuración en ejecución, la versión del IOS y el estado de la interfaz. Utilice el comando copy para guardar las configuraciones de los dispositivos.

En esta práctica de laboratorio, aplicará direccionamiento IP a las PC para habilitar la comunicación entre estos dos dispositivos. Use la utilidad ping para verificar la conectividad.

3.4.6.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.3 Clasificación de redes y 1.4 Topologías de redes: físicas y Lógicas.

3.4.6.4 Material Y Equipo Necesario

1. Equipo De Cómputo.

3.4.6.5 Metodología

Parte 1: Configurar la topología de la red (Ethernet únicamente).

En la parte 1, realizará el cableado para conectar los dispositivos según la topología de la red.

Paso 1: Encender los dispositivos

Encienda todos los dispositivos de la topología. Los switches no tienen un interruptor de corriente; se encienden en cuanto enchufa el cable de alimentación.

Paso 2: Conectar los dos switches

Conecte un extremo de un cable Ethernet a F0/1 en el S1 y el otro extremo del cable a F0/1 en el S2. Las luces de F0/1 en los dos switches deberían tornarse ámbar y, luego, verde. Esto indica que los switches se conectaron correctamente.

Paso 3: Conectar las PC a sus respectivos switches

a. Conecte un extremo del segundo cable Ethernet al puerto NIC en la PC-A. Conecte el otro extremo del cable a F0/6 en el S1. Después de conectar la PC al switch, la luz de F0/6 debería tornarse ámbar y luego verde, lo que indica que la PC-A se conectó correctamente.

b. Conecte un extremo del último cable Ethernet al puerto NIC en la PC-B. Conecte el otro extremo del cable a F0/18 en el S2. Después de conectar la PC al switch, la luz de F0/18 debería tornarse ámbar y luego verde, lo que indica que la PC-B se conectó correctamente.

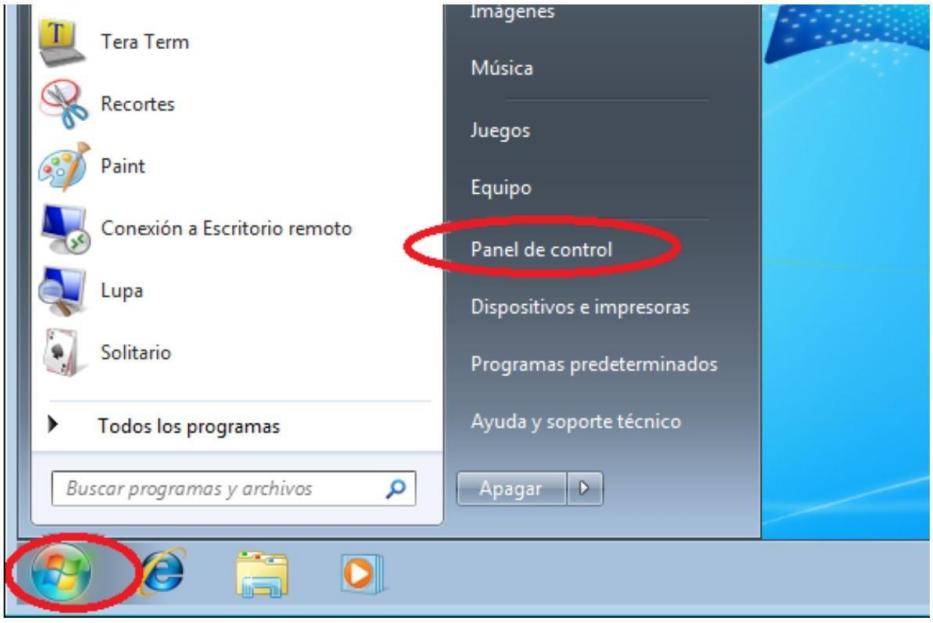
Paso 4: Inspeccionar visualmente las conexiones de la red

Después de realizar el cableado de los dispositivos de red, tómese un momento para verificar cuidadosamente las conexiones con el fin de minimizar el tiempo necesario para resolver problemas de conectividad de red más adelante.

Parte 2: Configurar hosts en las PC

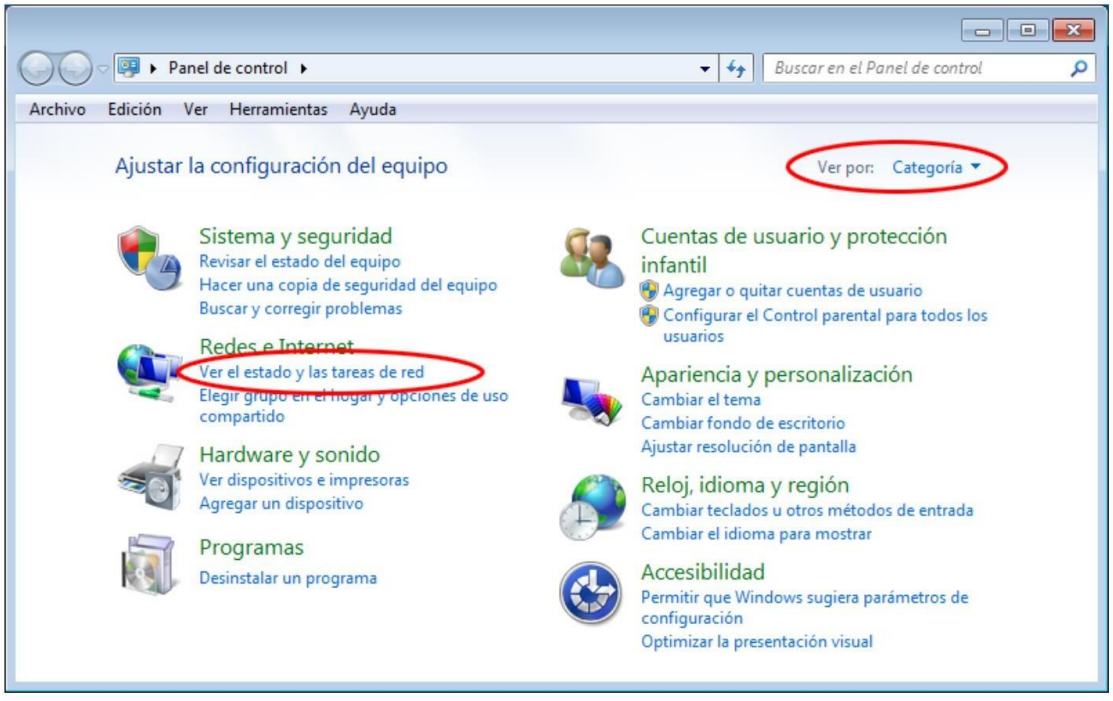
Paso 1: Configurar la información de dirección IP estática en las PC

a. Haga clic en el ícono **Inicio de Windows** y, a continuación, seleccione **Panel de control**.

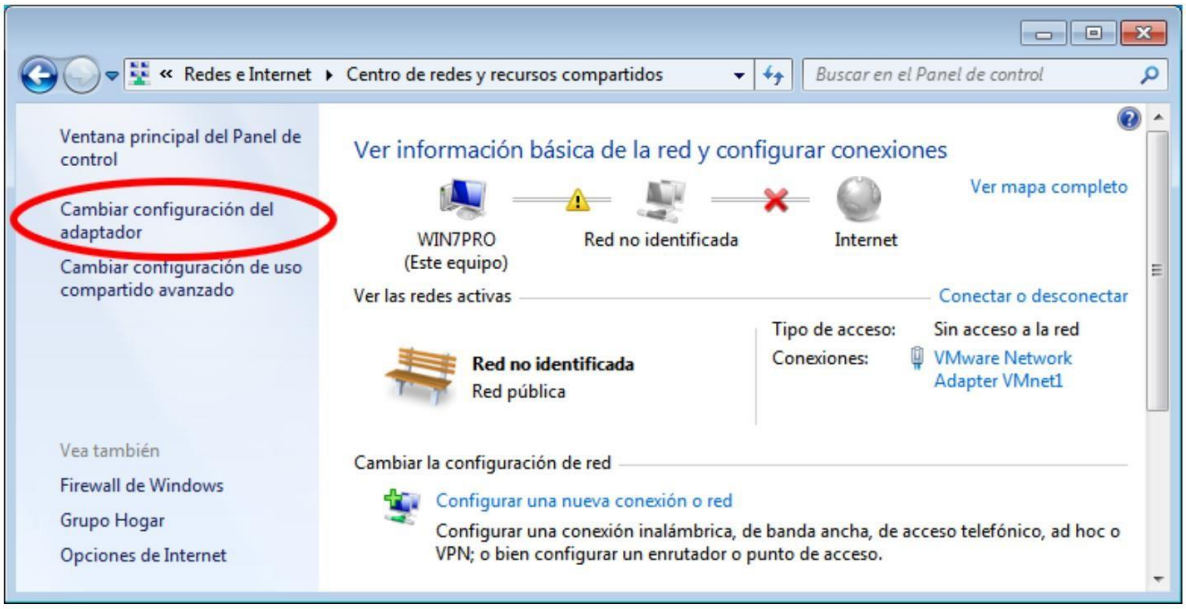


b. En la sección Redes e Internet, haga clic en el enlace **Ver el estado y las tareas de red**.

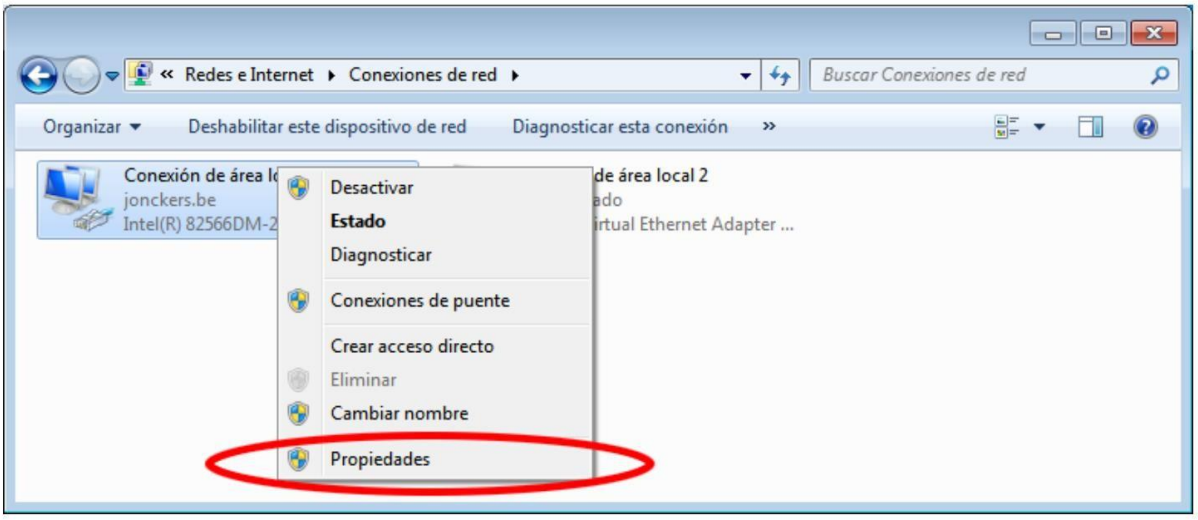
Nota: si en el panel de control se muestra una lista de íconos, haga clic en la opción desplegable que está junto a **Ver por:** y cambie la opción para que se muestre por **Categoría**.



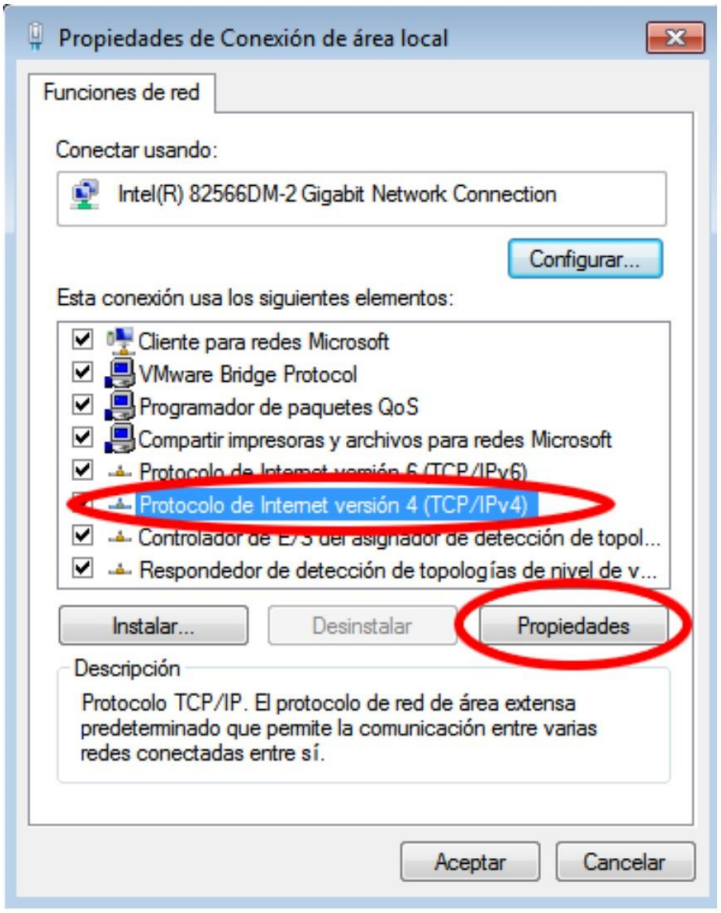
c. En el panel izquierdo de la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**.



d. En la ventana Conexiones de red, se muestran las interfaces disponibles en la PC. Haga clic con el botón secundario en la interfaz **Conexión de área local** y seleccione **Propiedades**.

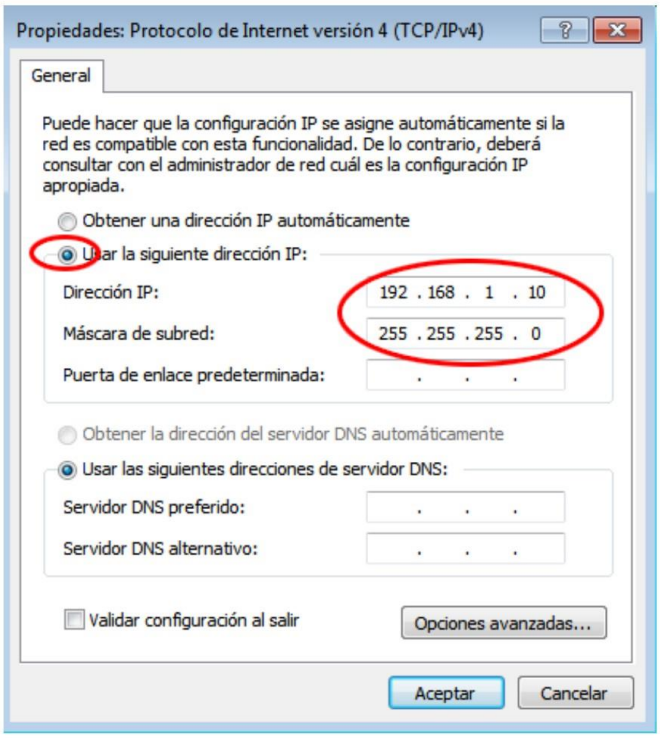


e. Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades**.



Nota: también puede hacer doble clic en **Protocolo de Internet versión 4 (TCP/IPv4** para que se muestre la ventana Propiedades.

f. Haga clic en el botón de opción **Usar la siguiente dirección IP** para introducir manualmente una dirección IP, la máscara de subred y el gateway predeterminado.



Nota: en el ejemplo mencionado arriba, se introdujeron la dirección IP y la máscara de subred para la PC-A. El gateway predeterminado no se introdujo porque no hay un router conectado a la red. Consulte la tabla de direccionamiento de la página 1 para obtener información de dirección IP para la PC- B.

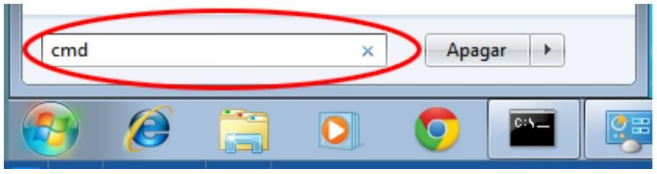
g. Después de introducir toda la información IP, haga clic en **Aceptar**. Haga clic en **Aceptar** en la ventana Propiedades de Conexión de área local para asignar la dirección IP al adaptador LAN.

h. Repita los pasos anteriores para introducir la información de dirección IP para la PC-B.

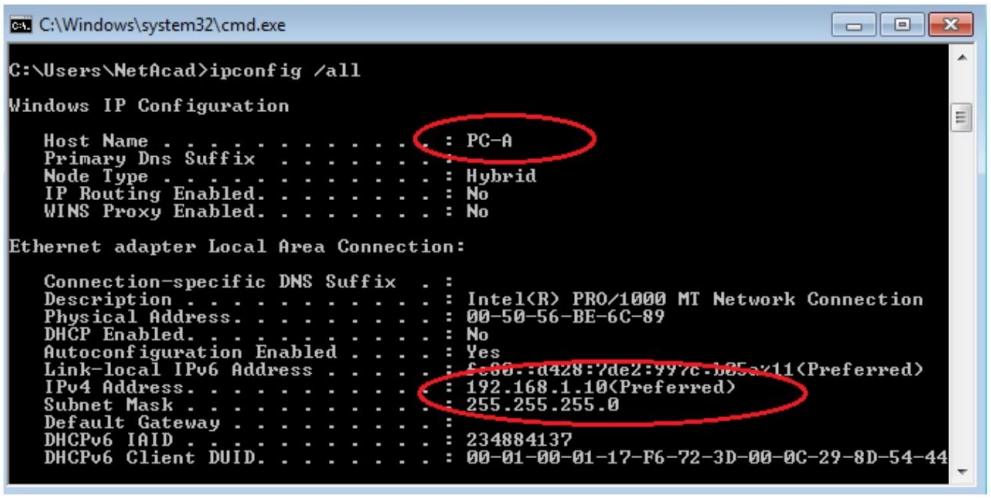
Paso 2: Verificar la configuración y la conectividad de la PC

Utilice la ventana del símbolo del sistema (**cmd.exe)** para verificar la configuración y la conectividad de la PC.

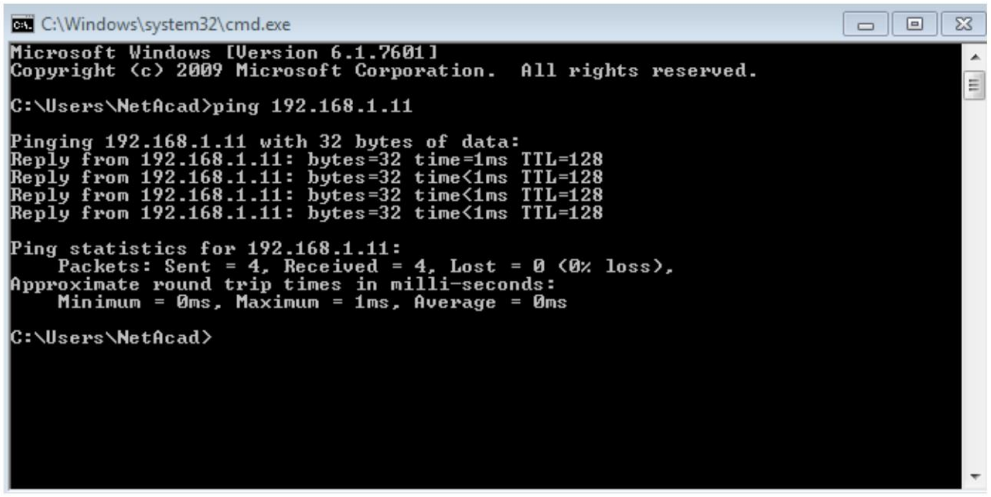
a. En la PC-A, haga clic en el ícono **Inicio de Windows**, escriba **cmd** en el cuadro de diálogo **Buscar programas y archivos** y, a continuación, presione Entrar.



b. En la ventana cmd.exe, puede introducir comandos directamente en la PC y ver los resultados de esos comandos. Verifique la configuración de la PC mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4.



c. Escriba **ping 192.168.1.11** y presione Entrar.



¿Fueron correctos los resultados del ping?

Si no lo fueron, resuelva los problemas que haya presentes.

Nota: si no obtuvo una respuesta de PC-B, intente hacer ping a PC-B nuevamente. Si aún no recibe una respuesta de PC-B, intente hacer ping a PC-A desde PC-B. Si no puede obtener una respuesta de la PC remota, solicite ayuda al instructor para resolver el problema.

Parte 3: Configurar y verificar los parámetros básicos del switch

Paso 1: Acceda al switch mediante el puerto de consola.

Utilice Tera Term para establecer una conexión de consola al switch desde la PC-A.

Paso 2: Ingrese al modo EXEC privilegiado.

Puede acceder a todos los comandos del switch en el modo EXEC privilegiado. El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes. Entre al modo EXEC privilegiado introduciendo el comando **enable**.

```
Switch> enable
Switch#
```

La petición de entrada cambió de **Switch>** a **Switch#**, lo que indica que está en el modo EXEC privilegiado.

Paso 3: Entre al modo de configuración.

Utilice el comando **configuration terminal** para ingresar al modo de configuración.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

La petición de entrada cambió para reflejar el modo de configuración global.

Paso 4: Asignar un nombre al switch

Utilice el comando **hostname** para cambiar el nombre del switch a **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Paso 5: Evitar búsquedas de DNS no deseadas

Para evitar que el switch intente traducir comandos introducidos de manera incorrecta como si fueran nombres de host, desactive la búsqueda del Sistema de nombres de dominios (DNS).

```
S1(config)# no ip domain-lookup
S1(config)#
```

Paso 6: Introducir contraseñas locales

Para impedir el acceso no autorizado al switch, se deben configurar contraseñas.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Paso 7: Introducir un mensaje MOTD de inicio de sesión

Se debe configurar un mensaje de inicio de sesión, conocido como “mensaje del día” (MOTD), para advertir a cualquier persona que acceda al switch que no se tolerará el acceso no autorizado.

El comando **banner motd** requiere el uso de delimitadores para identificar el contenido del mensaje de aviso. El carácter delimitador puede ser cualquier carácter siempre que no aparezca en el mensaje. Por este motivo, a menudo se usan símbolos como **#**.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full extent
of the law. #
S1(config)# exit
S1#
```

Paso 8: Guardar la configuración.

Utilice el comando **copy** para guardar la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil (NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Paso 9: Mostrar la configuración actual

El comando **show running-config** muestra toda la configuración en ejecución, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas. Los comandos configurados en los pasos del 1 al 8 están resaltados a continuación.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
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
!

<resultado omitido>

!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
 password cisco
 login
line vty 0 4
 login
line vty 5 15
 login
!
end

S1#
```

Paso 10: Mostrar la versión del IOS y otra información útil del switch

Utilice el comando **show version** para que se muestre la versión del IOS que se ejecuta en el switch, junto con otra información útil. Una vez más, necesitará utilizar la barra espaciadora para avanzar por la información que se muestra.

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

S1 uptime is 1 hour, 38 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
```

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.
Processor board ID FCQ1628Y5LE
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address	: 0C:D9:96:E2:3D:00
Motherboard assembly number	: 73-12600-06
Power supply part number	: 341-0097-03
Motherboard serial number	: FCQ16270N5G
Power supply serial number	: DCA1616884D
Model revision number	: R0
Motherboard revision number	: A0
Model number	: WS-C2960-24TT-L
System serial number	: FCQ1628Y5LE
Top Assembly Part Number	: 800-32797-02
Top Assembly Revision Number	: A0
Version ID	: V11
CLEI Code Number	: COM3L00BRF
Hardware Board Revision Number	: 0x0A

Switch	Ports	Model	SW Version	SW Image
* 1	26	WS-C2960-24TT-L	15.0(2)SE	C2960-LANBASEK9-M

Configuration register is 0xF
S1#

Paso 11: Mostrar el estado de las interfaces conectadas en el switch

Para revisar el estado de las interfaces conectadas, utilice el comando **show ip interface brief**. Presione la barra espaciadora para avanzar hasta el final de la lista.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

Paso 12: Repetir los pasos del 1 al 12 para configurar el switch S2

La única diferencia para este paso es cambiar el nombre de host a S2.

Paso 13: Registrar el estado de interfaz para las interfaces siguientes

Interfaz	S1		S2	
	Estado	Protocolo	Estado	Protocolo
F0/1				
F0/6				
F0/18				
VLAN 1				

¿Por qué algunos puertos FastEthernet en los switches están activos y otros inactivos?

Reflexión

¿Qué podría evitar que se envíe un ping entre las PC?

Nota: puede ser necesario desactivar el firewall de las PC para hacer ping entre ellas.

Apéndice A: Inicialización y recarga de un switch

Paso 1: Conéctese al switch.

Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Paso 2: Determine si se crearon redes de área local virtuales (VLAN, Virtual Local-Area Networks).

Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Paso 3: Elimine el archivo VLAN.

a. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Entrar si introdujo el nombre de manera correcta.

b. Cuando se le pregunte sobre la eliminación de este archivo, presione Entrar para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Paso 4: Borre el archivo de configuración de inicio.

Utilice el comando **erase startup-config** para borrar el archivo de configuración de inicio de la NVRAM. Cuando se le pregunte sobre la eliminación del archivo de configuración, presione Entrar para confirmar el borrado. (Si se presiona cualquier otra tecla, se anula la operación).

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Paso 5: Recargar el switch.

Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Cuando se le pregunte sobre la recarga del switch, presione Entrar para continuar con la recarga. (Si se presiona cualquier otra tecla, se anula la recarga).

```
Switch# reload
Proceed with reload? [confirm]
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 6: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Escriba **no** en la petición de entrada y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

3.4.6.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.6.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.6.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.7 Práctica 7. Configuración de una dirección de administración del switch

3.4.7.1 Objetivo

Parte 1: Configurar un dispositivo de red básico.

Parte 2: Verificar y probar la conectividad de red.

3.4.7.2 Introducción

Los switches Cisco tienen una interfaz especial, conocida como “interfaz virtual del switch” (SVI). La SVI se puede configurar con una dirección IP, comúnmente conocida como la dirección de administración que se utiliza para el acceso remoto al switch para mostrar o configurar parámetros.

En esta práctica de laboratorio, armará una red simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Configurará los parámetros básicos del switch y el direccionamiento IP, y demostrará el uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host, y utiliza puertos Ethernet y de consola únicamente.

3.4.7.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.3 Clasificación de redes y 1.4 Topologías de redes: físicas y Lógicas.

3.4.7.4 Material Y Equipo Necesario

1. Equipo De Cómputo.
2. Conexión A Internet.
3. Packet Tracer

3.4.7.5 Metodología

Parte 1: Configurar un dispositivo de red básico

En la parte 1, configurará la red y los parámetros básicos, como nombres de host, direcciones IP de las interfaces y contraseñas.

Paso 1: Conectar la red

a. Realizar el cableado de red tal como se muestra en la topología.

b. Establezca una conexión de consola al switch desde la PC-A.

Paso 2: Configurar los parámetros básicos del switch

En este paso, configurará los parámetros básicos del switch, como el nombre de host, y configurará una dirección IP para la SVI. Asignar una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administrará el switch. Telnet y Shell seguro (SSH) son dos de los métodos de administración más comunes; sin embargo, Telnet es un protocolo muy inseguro. Toda la información que fluye entre los dos dispositivos se envía como texto no cifrado. Las contraseñas y otra información confidencial pueden ser fáciles de ver si se las captura mediante un programa detector de paquetes.

a. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del usuario en el switch, con la petición de entrada `Switch>`. Ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

b. Verifique que haya un archivo de configuración vacío con el comando **`show running-config`** del modo EXEC privilegiado. Si previamente se guardó un archivo de configuración, deberá eliminarlo. Según cuál sea el modelo del switch y la versión del IOS, la configuración podría variar. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, solicite ayuda al instructor.

c. Ingrese al modo de configuración global y asigne un nombre de host al switch.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

d. Configure el acceso por contraseña al switch.

```
S1(config)# enable secret class
S1(config)#
```

e. Evite búsquedas no deseadas del Sistema de nombres de dominios (DNS).

```
S1(config)# no ip domain-lookup
S1(config)#
```

f. Configure un mensaje del día (MOTD) de inicio de sesión.

```
S1(config)# banner motd #
Enter Text message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
```

g. Para verificar la configuración de acceso, alterne entre los modos.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

¿Qué tecla de método abreviado se utilizan para pasar directamente del modo de configuración global al modo EXEC privilegiado?

h. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario.

```
S1> enable
Password: class
S1#
```

Nota: la contraseña no se mostrará en la pantalla al ingresar.

i. Ingrese al modo de configuración global para configurar la dirección IP de la SVI para permitir la administración remota de switch.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

j. Restrinja el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

k. Configure la línea de terminal virtual (VTY) para que el switch permita el acceso por Telnet. Si no configura una contraseña de VTY, no podrá acceder al switch mediante Telnet.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Paso 3: Configurar una dirección IP en la PC-A

a. Asigne la dirección IP y la máscara de subred a la PC, como se muestra en la Tabla de direccionamiento de la página 1. A continuación, se describe el procedimiento para asignar una dirección IP em una PC con Windows 7:

1) Haga clic en el ícono **Inicio de Windows** > **Panel de control**.
2) Haga clic en **Ver por:** > **Categoría**.
3) Seleccione **Ver el estado y las tareas de red** > **Cambiar configuración del adaptador**.
4) Haga clic con el botón secundario en **Conexión de área local** y seleccione **Propiedades**.
5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en **Propiedades** > **Aceptar**.
6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca manualmente la dirección IP y la máscara de subred.

Parte 2: Verificar y probar la conectividad de red

Ahora verificará y registrará la configuración del switch, probará la conectividad de extremo a extremo entre la PC-A y el S1, y probará la capacidad de administración remota del switch.

Paso 1: Mostrar la configuración del dispositivo S1

a. Regrese a la conexión de consola utilizando Tera Term en la PC-A para mostrar y verificar la configuración del switch por medio de la emisión del comando **show run**. A continuación, se muestra una configuración de muestra. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

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

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
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

<resultado omitido>

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
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

b. Verifique el estado de su interfaz de administración SVI. La interfaz VLAN 1 debería tener estado up/up (activo/activo) y tener una dirección IP asignada. Observe que el puerto de switch F0/6 también está activado, porque la PC-A está conectada a él. Dado que todos los puertos de switch están inicialmente en VLAN 1 de manera predeterminada, puede comunicarse con el switch mediante la dirección IP que configuró para VLAN 1.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
```

```
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
```

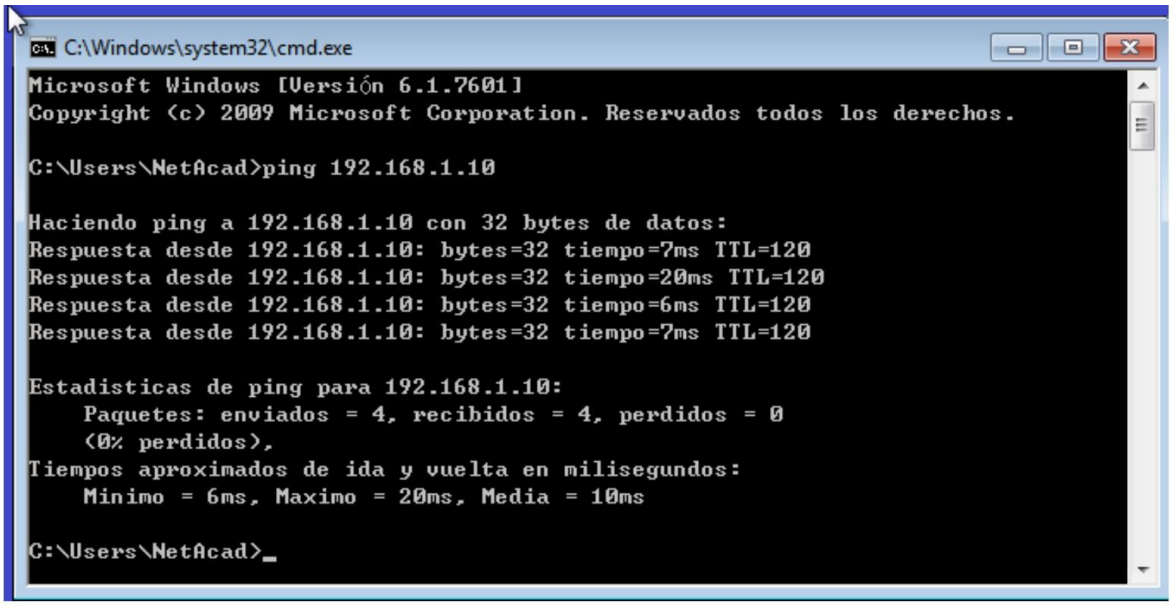
Paso 2: Probar la conectividad de extremo a extremo

Abra una ventana del símbolo del sistema (cmd.exe) en la PC-A: haga clic en el ícono **Inicio de Windows** e introduzca **cmd** en el campo **Buscar programas y archivos**. Verifique la dirección IP de la PC-A mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4. Haga ping a la propia dirección de la PC-A y a la dirección de administración del S1.

a. Haga ping a la dirección de la propia PC-A primero.

```
C:\Users\NetAcad> ping 192.168.1.10
```

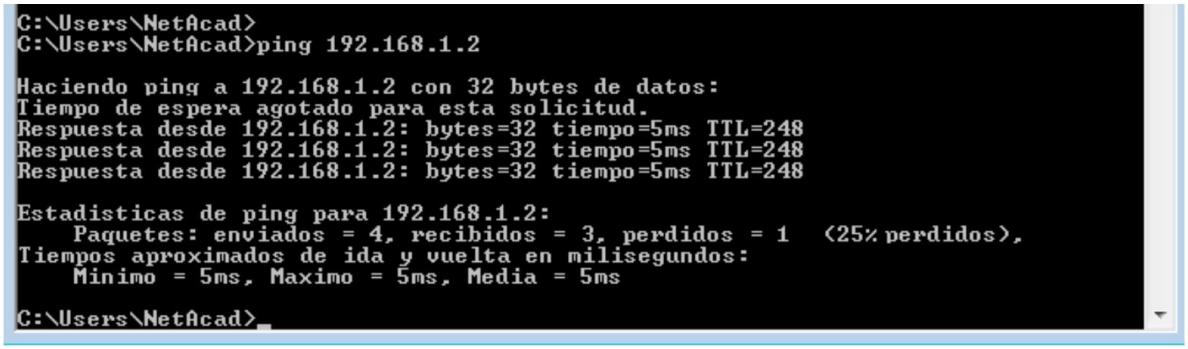
El resultado debe ser similar a la siguiente pantalla:



b. Haga ping a la dirección de administración de SVI del S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla. Si los resultados del ping no son correctos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Si es necesario, revise el cableado físico y el direccionamiento IP.



Paso 3: Probar y verificar la administración remota del S1

Ahora utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. En esta práctica de laboratorio, la PC-A y el S1 se encuentran uno junto al otro. En una red de producción, el switch podría estar en un armario de cableado en el piso superior, mientras que la PC de administración podría estar ubicada en la planta baja. Telnet no es un protocolo seguro. Sin embargo, en esta práctica de laboratorio lo usará para probar el acceso remoto. Toda la información enviada por Telnet, incluidos los comandos y las contraseñas, se envían durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, utilizará Shell seguro (SSH) para acceder a los dispositivos de red en forma remota.

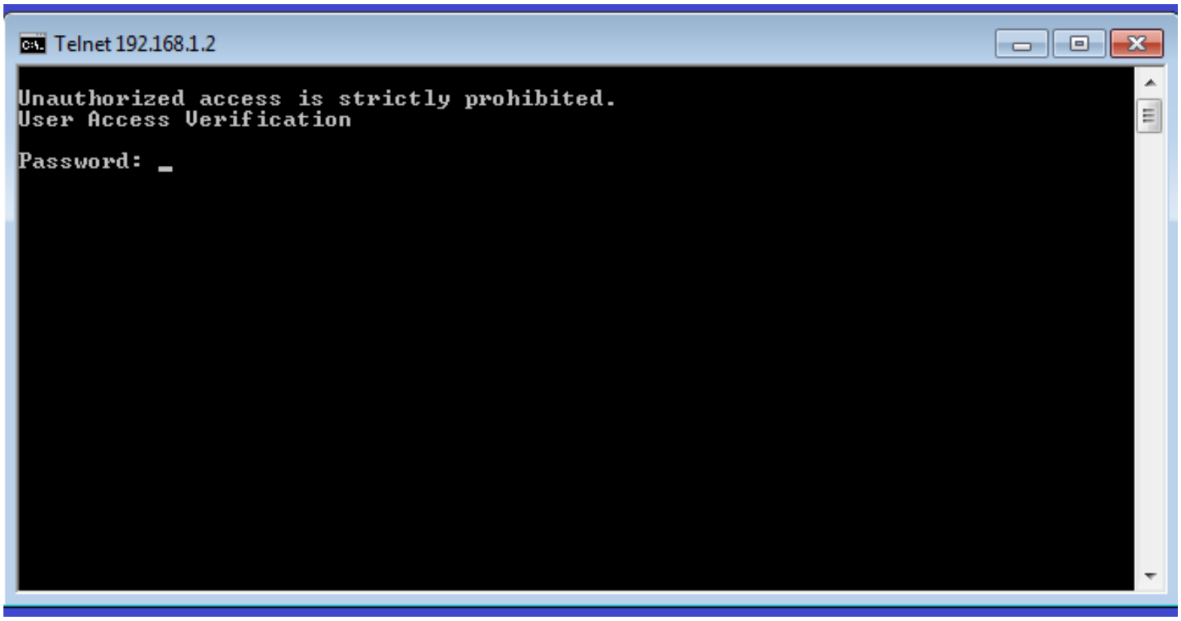
Nota: Windows 7 no admite Telnet en forma nativa. El administrador debe habilitar este protocolo. Para instalar el cliente Telnet, abra una ventana del símbolo del sistema y escriba **pkgmgr /iu:"TelnetClient"**.

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

a. Con la ventana del símbolo del sistema abierta en la PC-A, emita un comando de Telnet para conectarse al S1 a través de la dirección de administración de SVI. La contraseña es **cisco**.

```
C:\Users\NetAcad> telnet 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla:



b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Escriba **enable** en la petición de entrada. Introduzca la contraseña **class** para ingresar al modo EXEC privilegiado y para emitir un comando **show run**.

Paso 4: Guardar el archivo de configuración

a. Desde la sesión de Telnet, emita el comando **copy run start** en la petición de entrada.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

b. Salga de la sesión de Telnet escribiendo **quit**. Volverá al símbolo del sistema de Windows 7.

Reflexión

¿Por qué debe usar una conexión de consola para configurar inicialmente el switch? ¿Por qué no conectarse al switch a través de Telnet o SSH?

3.4.7.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.7.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.7.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.8 Práctica 8. Exploración de una red.

3.4.8.1 Objetivo

Parte 1: Examinar el tráfico de internetwork en la sucursal

Parte 2: Examinar el tráfico de internetwork a la central

Parte 3: Examinar el tráfico de internet desde la sucursal.

3.4.8.2 Introducción

El objetivo de esta actividad de simulación es ayudarlo a comprender el flujo de tráfico y el contenido de los paquetes de datos a medida que atraviesan una red compleja. Las comunicaciones se examinarán en tres ubicaciones distintas que simulan redes comerciales y domésticas típicas.

La ubicación central tiene tres routers y varias redes que posiblemente representen distintos edificios dentro de un campus. La ubicación Branch (Sucursal) tiene sola un router con una conexión a Internet y una conexión dedicada de red de área extensa (WAN) a la ubicación Central. La Home Office (Oficina doméstica) utiliza una conexión de banda ancha con módem por cable para proporcionar acceso a internet y a los recursos corporativos a través de Internet.

Los dispositivos en cada ubicación utilizan una combinación de direccionamiento estático y dinámico. Los dispositivos se configuran con gateways predeterminados y con información del Sistema de nombres de dominios (DNS), según corresponda.

3.4.8.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.3 Clasificación de redes y 1.4 Topologías de redes: físicas y Lógicas.

3.4.8.4 Material Y Equipo Necesario

- Equipo De Cómputo.

3.4.8.5 Metodología

Parte 1: Examinar el tráfico de internetwork en la sucursal

En la parte 1 de esta actividad, utilizará el modo de simulación para generar tráfico Web y examinar el protocolo HTTP junto con otros protocolos necesarios para las comunicaciones.

Paso 1: Cambiar del modo de tiempo real al modo de simulación

a. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.

b. Verifique que **ARP, DNS, HTTP** y **TCP** estén seleccionados en **Event List Filters** (Filtros de lista de eventos).

c. Mueva completamente hacia la derecha la barra deslizable que se encuentra debajo de los botones **Play Controls** (Controles de reproducción), **Back**, **Auto Capture/Play**, **Capture/Forward** (Retroceder, Captura/Reproducción automática, Capturar/avanzar).

Paso 2: Generar tráfico mediante un explorador Web

El panel de simulación actualmente está vacío. En Event List (Lista de eventos), en la parte superior del panel de simulación, hay seis columnas en el encabezado. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el contenido de un evento determinado.

Nota: la topología se muestra en el panel de la izquierda del panel de simulación. Utilice las barras de desplazamiento para incorporar la ubicación Branch al panel, en caso necesario. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha.

a. Haga clic en **Sales PC** (PC de ventas) en el panel del extremo izquierdo.

b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.

c. En el campo de dirección URL, introduzca **http://branchserver.pt.pta** y haga clic en **Go** (Ir). Observe la lista de eventos en el panel de simulación. ¿Cuál es el primer tipo de evento que se indica?

d. Haga clic en el cuadro de información de **DNS**. En **Out Layers** (Capas de salida), se indica DNS para la capa 7. La capa 4 utiliza UDP para comunicarse con el servidor DNS en el puerto 53 (**Dst Port:** [Pto. de destino:]). Se indica tanto la dirección IP de origen como la de destino. ¿Qué información falta para comunicarse con el servidor DNS?

e. Haga clic en **Auto Capture/Play**. En aproximadamente 45 segundos, aparece una ventana en la que se indica la finalización de la simulación actual. Haga clic en el botón **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista y observe la cantidad de eventos de **ARP**. Observe la columna Device (Dispositivo) en la lista de eventos: ¿cuántos de los dispositivos en la ubicación Branch atraviesa la solicitud de **ARP**?

f. Desplácese por los eventos en la lista hasta la serie de eventos de **DNS**. Seleccione el evento de **DNS** para el que se indica **BranchServer** en At Device (En el dispositivo). Haga clic en el cuadro de la columna **Info**. ¿Qué se puede determinar seleccionando la capa 7 en **OSI Model** (Modelo OSI)? (Consulte los resultados que se muestran directamente debajo de **In Layers** [Capas de entrada]).

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). Desplácese hasta la parte inferior de la ventana y ubique la sección DNS Answer (Respuesta de DNS). ¿Cuál es la dirección que se muestra?

h. Los eventos siguientes son eventos de **TCP** que permiten que se establezca un canal de comunicación. En el dispositivo **Sales**, seleccione el último evento de **TCP** anterior al evento de **HTTP**. Haga clic en el cuadro coloreado Info para ver la información de PDU. Resalte Layer 4 (Capa 4) en la columna **In Layers**. Observe el elemento 6 en la lista que se encuentra directamente debajo de la columna **In Layers**: ¿cuál es el estado de la conexión?

i. Los eventos siguientes son eventos de **HTTP**. Seleccione cualquiera de los eventos de **HTTP** en un dispositivo intermediario (teléfono IP o switch). ¿Cuántas capas están activas en uno de estos dispositivos y por qué?

j. Seleccione el último evento de **HTTP** en Sales PC. Seleccione la capa superior en la ficha **OSI Model**. ¿Cuál es el resultado que se indica debajo de la columna **In Layers**?

Parte 2: Examinar el tráfico de internetwork a la central

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para ver y examinar cómo se administra el tráfico que sale de la red local.

Paso 1: Configurar la captura de tráfico hacia el servidor Web de la central

a. Cierre todas las ventanas de información de PDU abiertas.

b. Haga clic en la opción **Reset Simulation** (Restablecer simulación), que se encuentra cerca del centro del panel de simulación.

c. Escriba **http://centralserver.pt.pta** en el explorador Web de Sales PC.

d. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS** y que no hay entradas de **ARP** antes de comunicarse con **Branchserver**. Según lo aprendido hasta ahora, ¿a qué se debe esto?

e. Haga clic en el último evento de DNS en la columna **Info**. Seleccione **Layer 7** (Capa 7) en la ficha **OSI Model**.

Al observar la información proporcionada, ¿qué se puede determinar sobre los resultados de DNS?

f. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante). Desplácese hasta la sección **DNS ANSWER** (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta?

g. Los eventos siguientes son eventos de **ARP**. Haga clic en el cuadro coloreado Info del último evento de **ARP**. Haga clic en la ficha **Inbound PDU Details** y observe la dirección MAC. Sobre la base de la información en la sección de ARP, ¿qué dispositivo proporciona la respuesta de ARP?

h. Los eventos siguientes son eventos de **TCP**, que nuevamente se preparan para establecer un canal de comunicación. Busque el primer evento de **HTTP** en Event List. Haga clic en el cuadro coloreado del evento de **HTTP**. Resalte Layer 2 (Capa 2) en la ficha **OSI Model**. ¿Qué se puede determinar sobre la dirección MAC de destino?

i. Haga clic en el evento de **HTTP** en el dispositivo **R4**. Observe que la capa 2 contiene un encabezado de Ethernet II. Haga clic en el evento de **HTTP** en el dispositivo **Intranet**. ¿Cuál es la capa 2 que se indica en este dispositivo?

Observe que solo hay dos capas activas, en oposición a lo que sucede cuando se atraviesa el router. Esta es una conexión WAN, y se analizará en otro curso.

Parte 3: Examinar el tráfico de Internet desde la sucursal

En la parte 3 de esta actividad, borrará los eventos y comenzará una nueva solicitud Web que usará Internet.

Paso 1: Configurar la captura de tráfico hacia un servidor Web de Internet

a. Cierre todas las ventanas de información de PDU abiertas.

b. Haga clic en la opción **Reset Simulation**, que se encuentra cerca del centro del panel de simulación. Escriba **http://www.netacad.pta** en el explorador Web de Sales PC.

c. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS**. ¿Qué advierte sobre la cantidad de eventos de **DNS**?

d. Observe algunos de los dispositivos a través de los que se transfieren los eventos de **DNS** en el camino hacia un servidor DNS. ¿Dónde se encuentran estos dispositivos?

e. Haga clic en el último evento de **DNS**. Haga clic en la ficha **Inbound PDU Details** y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para **www.netacad.pta**?

f. Cuando los routers mueven el evento de **HTTP** a través de la red, hay tres capas activas en **In Layers** y **Out Layers** en la ficha **OSI Model**. Sobre la base de esa información, ¿cuántos routers se atraviesan?

g. Haga clic en el evento de **TCP** anterior al último evento de **HTTP**. Según la información que se muestra, ¿cuál es el propósito de este evento?

h. Se indican varios eventos más de **TCP**. Ubique el evento de **TCP** donde se indique **IP Phone** (Teléfono IP) para *Last Device* (Último dispositivo) y **Sales** para *At Device*. Haga clic en el cuadro coloreado Info y seleccione **Layer 4** en la ficha **OSI Model**. Según la información del resultado, ¿cómo se configuró el estado de la conexión?

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar el tráfico de internetwork en la sucursal	Paso 2c	5	
	Paso 2d	5	
	Paso 2e	5	
	Paso 2f	5	
	Paso 2g	5	
	Paso 2h	5	
	Paso 2i	5	
	Paso 2j	5	
Total de la parte 1		**40**	
Parte 2: Examinar el tráfico de internetwork a la central	Paso 1c	5	
	Paso 1d	5	
	Paso 1e	5	
	Paso 1f	5	
	Paso 1g	5	
	Paso 1h	5	
Total de la parte 2		**30**	
Parte 3: Examinar el tráfico de Internet desde la sucursal	Paso 1c	5	
	Paso 1d	5	
	Paso 1e	5	
	Paso 1f	5	
	Paso 1g	5	
	Paso 1h	5	
Total de la parte 3		**30**	
Puntuación total		**100**	

3.4.8.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.8.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.8.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.9 Práctica 9. Uso de Wireshark para ver el tráfico de la red

3.4.9.1 Objetivo

Parte 1: Descargar e instalar Wireshark (Optativo)

Parte 2: Capturar y analizar datos ICMP locales en Wireshark

Parte 3: Capturar y analizar los datos ICMP remotos en Wireshark

3.4.9.2 Introducción

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Mientras los streams de datos van y vienen por la red, el programa detector “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con la RFC correcta u otras especificaciones.

Wireshark es una herramienta útil para cualquier persona que trabaje con redes y se puede utilizar con la mayoría de las prácticas de laboratorio en los cursos de CCNA para tareas de análisis de datos y resolución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En esta práctica de laboratorio, usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

3.4.9.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.3 Clasificación de redes y 1.4 Topologías de redes: físicas y Lógicas.

3.4.9.4 Material Y Equipo Necesario

4. Equipo De Cómputo.
5. Conexión A Internet.
6. Packet Tracer

3.4.9.5 Metodología

Parte 1: Descargar e instalar Wireshark (optativo)

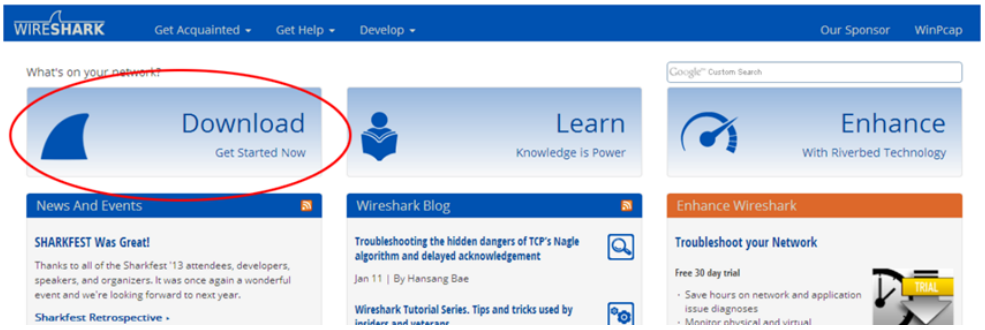
Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux. En la parte 1 de esta práctica de laboratorio, descargará e instalará el programa de software Wireshark en la PC.

Nota: si Wireshark ya está instalado en la PC, puede saltear la parte 1 e ir directamente a parte 2. Si Wireshark no está instalado en la PC, consulte con el instructor acerca de la política de descarga de software de la academia.

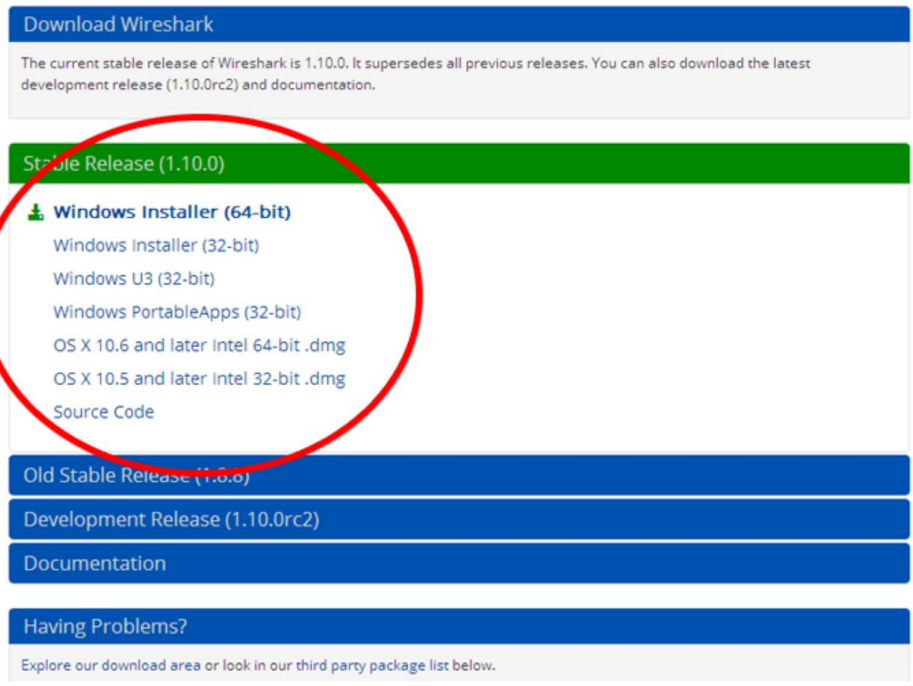
Paso 1: Descargar Wireshark

a. Wireshark se puede descargar de www.wireshark.org.

b. Haga clic en **Download Wireshark** (Descargar Wireshark).



c. Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione **Windows Installer (64-bit)** (Instalador de Windows [64 bits]).

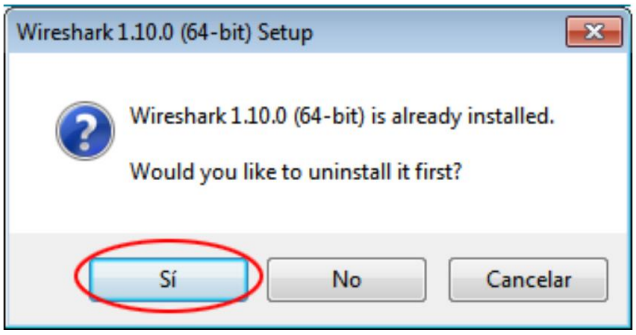


Después de realizar la selección, comienza la descarga. La ubicación del archivo descargado depende del explorador y del sistema operativo que utiliza. Para usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas**.

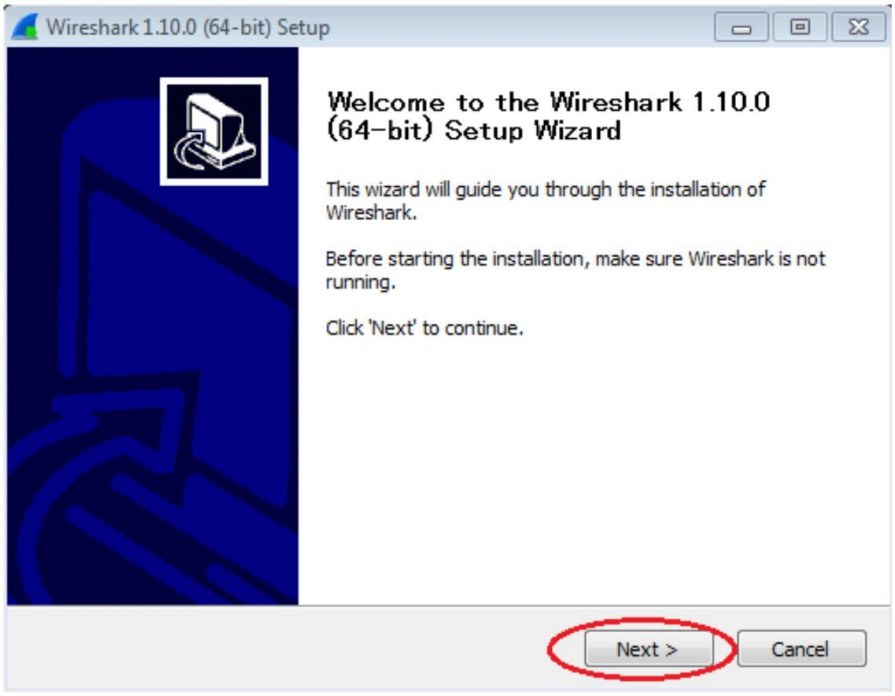
Paso 2: Instalar Wireshark

a. El archivo descargado se denomina **Wireshark-win64-x.x.x.exe**, en el que **x** representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.

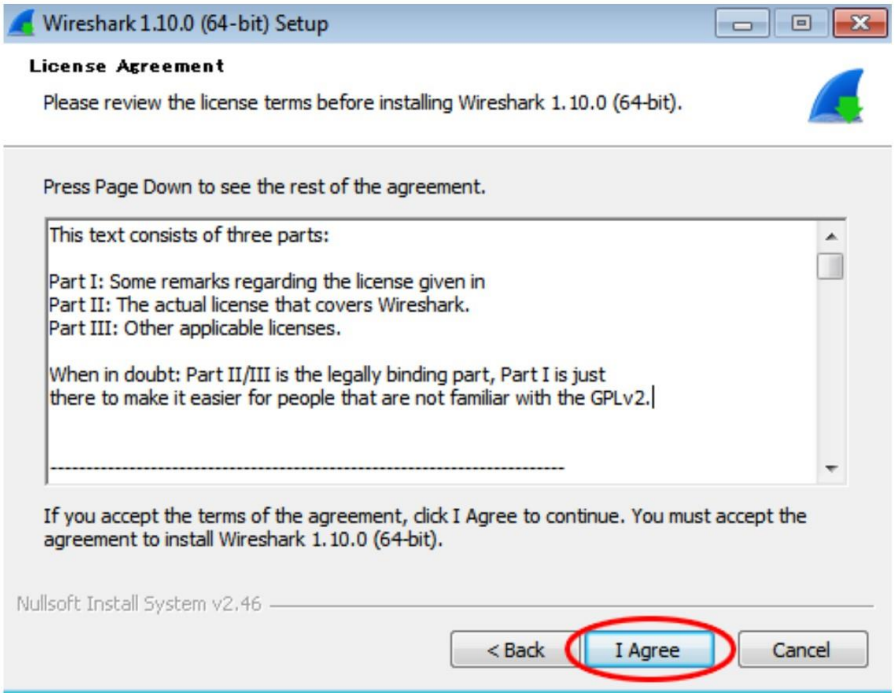
b. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí** para desinstalar la versión anterior de Wireshark.



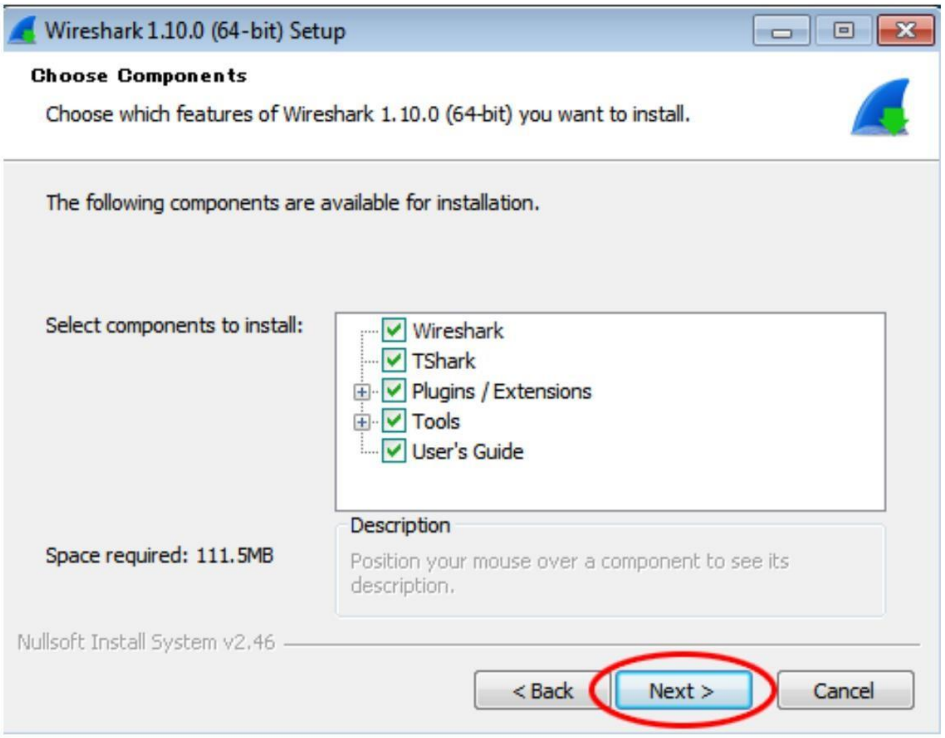
c. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Next** (Siguiente).



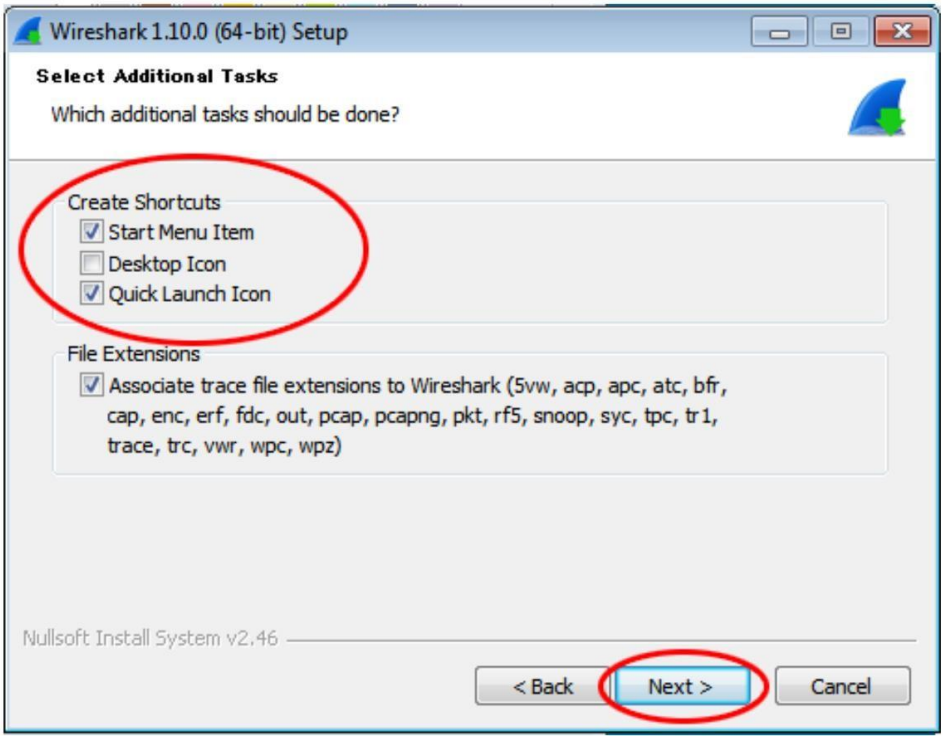
d. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement (Contrato de licencia), haga clic en **I agree** (Acepto).



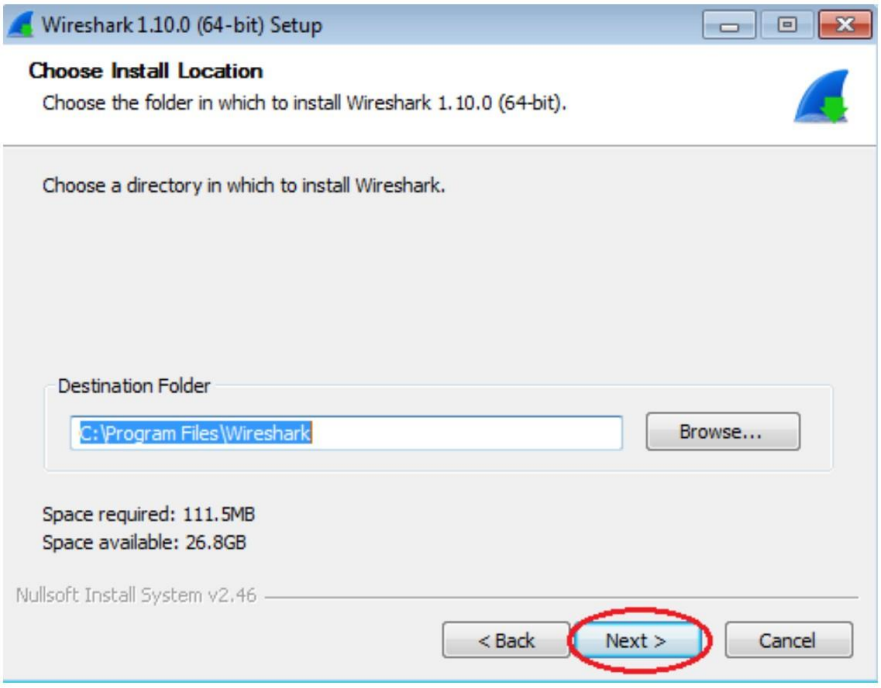
e. Guarde la configuración predeterminada en la ventana Choose Components (Elegir componentes) y haga clic en **Next** (Siguiente).



f. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Next** (Siguiente).

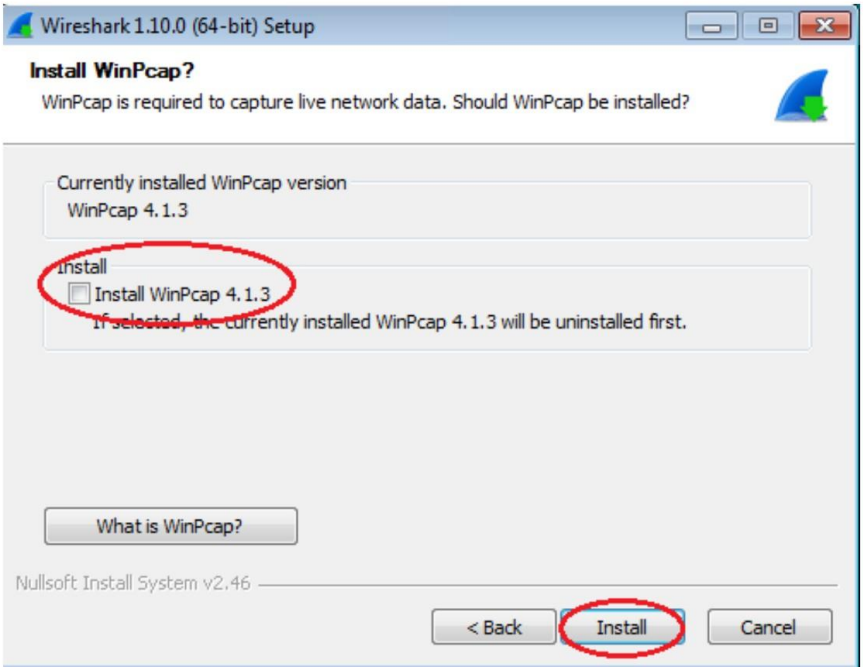


g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.

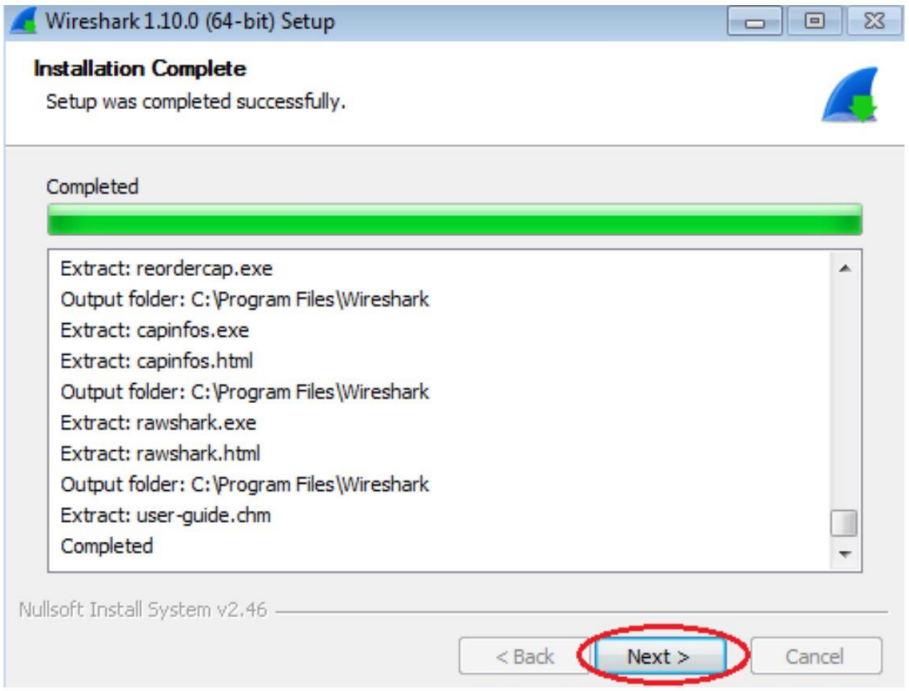


h. Para capturar datos de la red activa, WinPcap debe estar instalado en la PC. Si WinPcap ya está instalado en la PC, la casilla de verificación Install (Instalar) estará desactivada. Si la versión instalada de WinPcap es anterior a la versión que incluye Wireshark, se recomienda que permita que la versión más reciente se instale haciendo clic en la casilla de verificación **Install WinPcap x.x.x** (Instalar WinPcap [número de versión]).

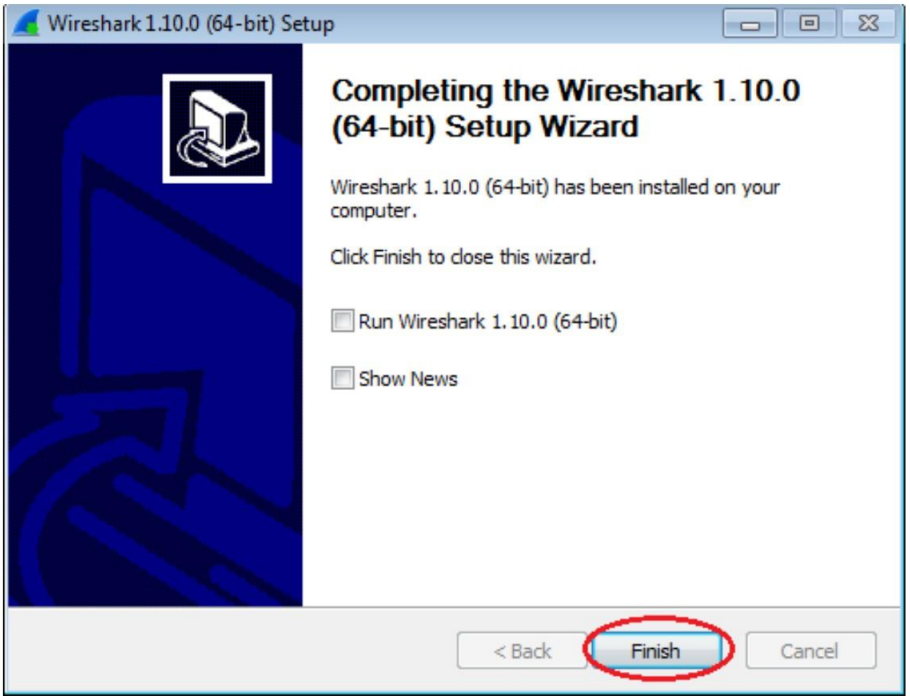
i. Finalice el asistente de instalación de WinPcap si instala WinPcap.



j. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Next** (Siguiente) cuando la instalación esté completa.



k. Haga clic en **Finish** (Finalizar) para completar el proceso de instalación de Wireshark.



Parte 2: Capturar y analizar datos ICMP locales en Wireshark

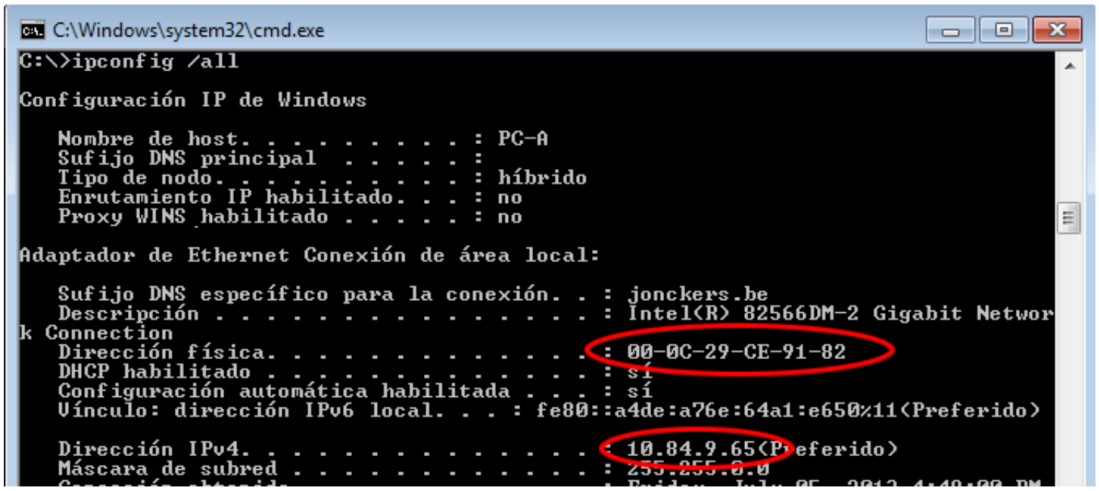
En la parte 2 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

a. Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Entrar.

b. Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.

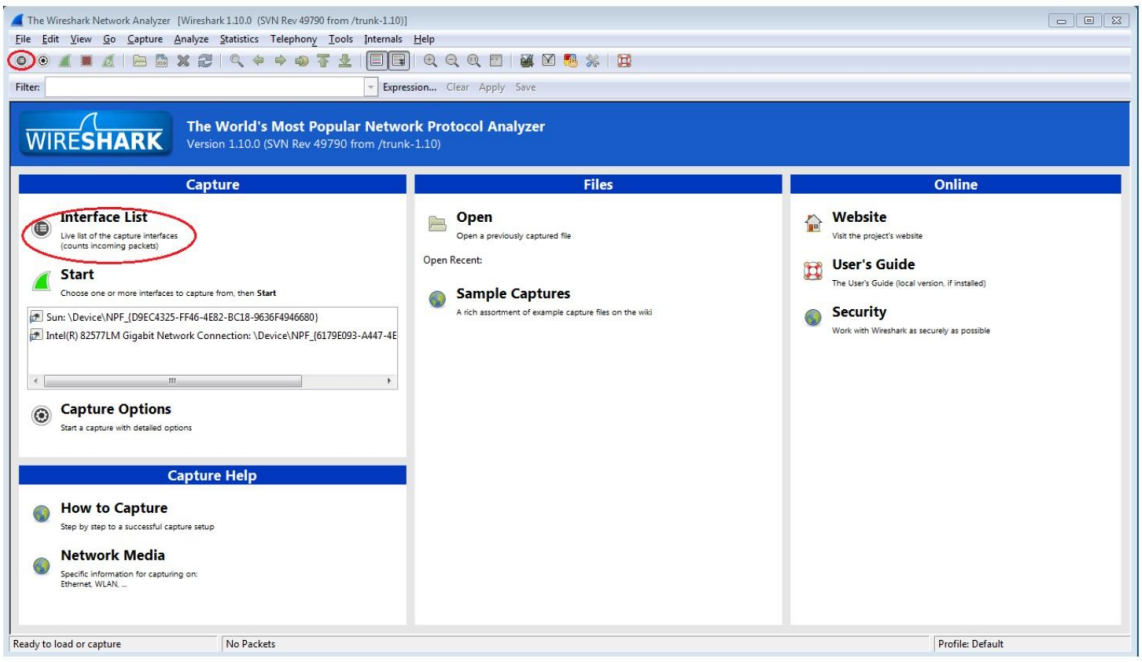


c. Solicite a un miembro del equipo la dirección IP de su PC y proporciónele la suya. En esta instancia, no proporcione su dirección MAC.

Paso 2: Iniciar Wireshark y comenzar a capturar datos

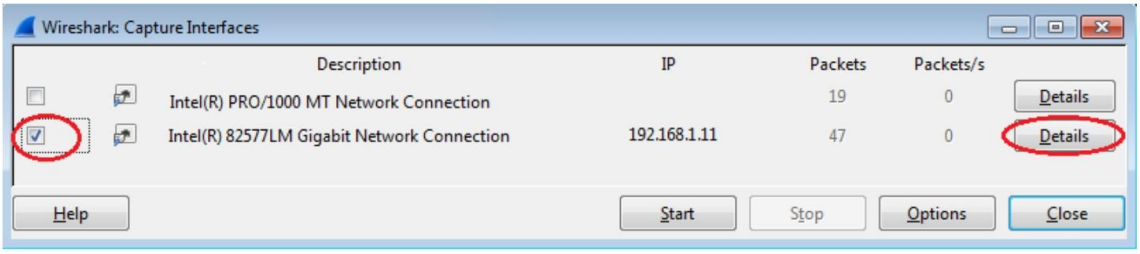
a. En la PC, haga clic en el botón **Inicio** de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en **Wireshark**.

b. Una vez que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).

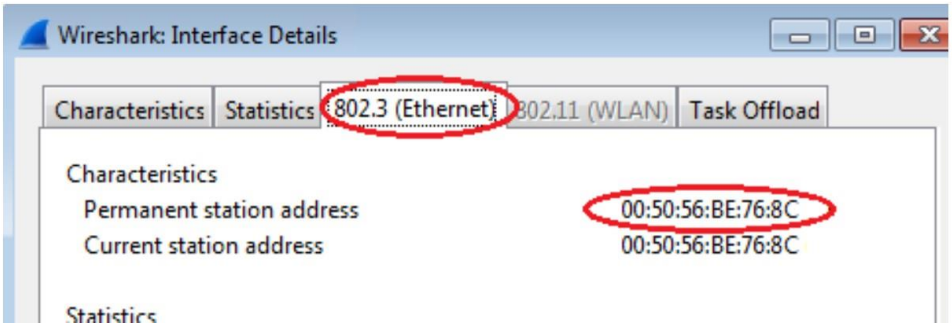


Nota: al hacer clic en el ícono de la primera interfaz de la fila de íconos, también se abre Interface List (Lista de interfaces).

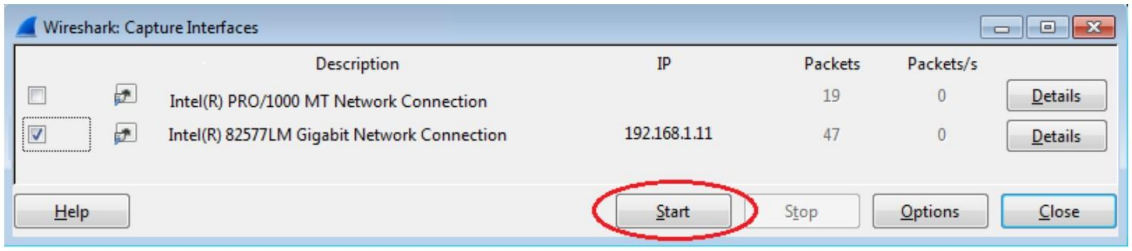
c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.



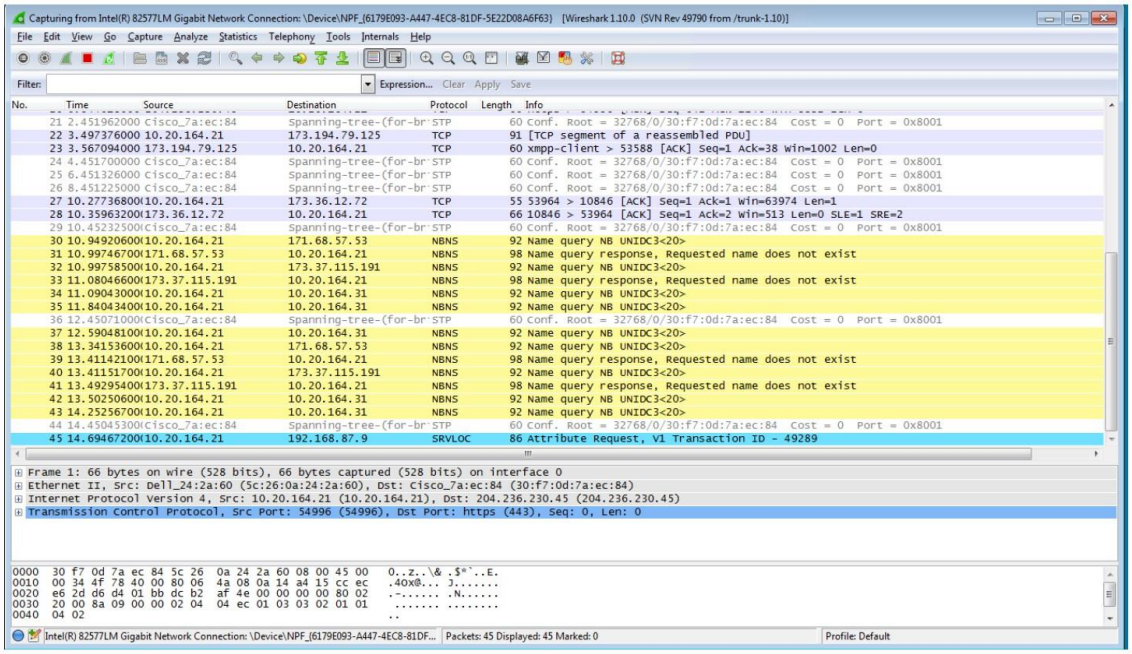
Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón **Details** (Detalles) y, a continuación, haga clic en la ficha **802.3 (Ethernet)**. Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana Interface Details (Detalles de la interfaz).



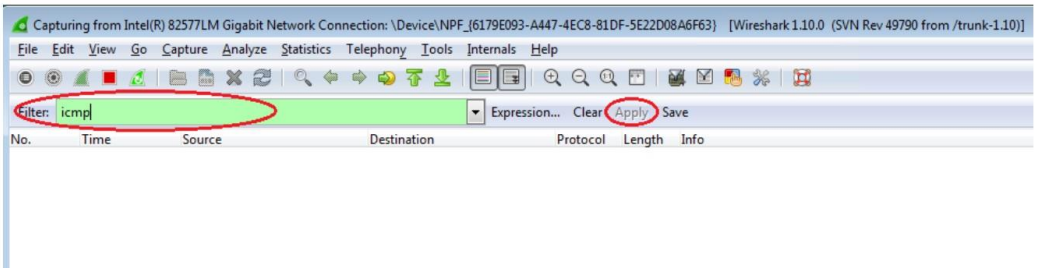
d. Después de activar la interfaz correcta, haga clic en **Start** (Comenzar) para comenzar la captura de datos.



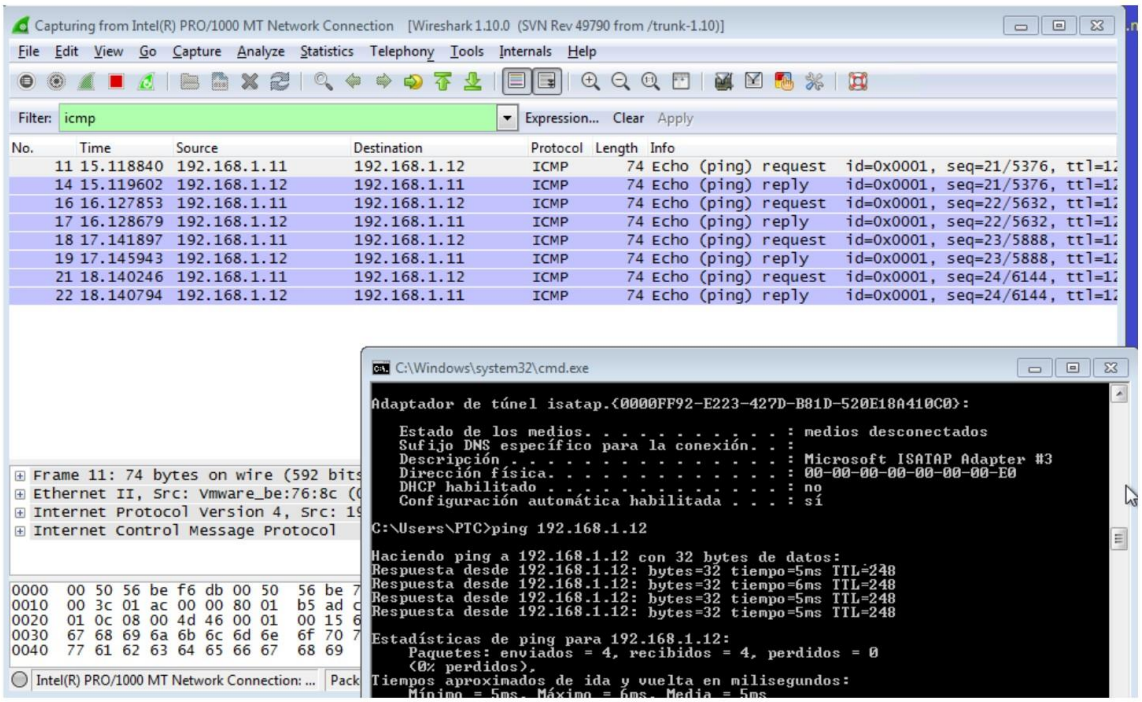
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.



e. Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro Filter (Filtro) que se encuentra en la parte superior de Wireshark y presione Entrar o haga clic en el botón **Apply** (Aplicar) para ver solamente PDU de ICMP (ping).

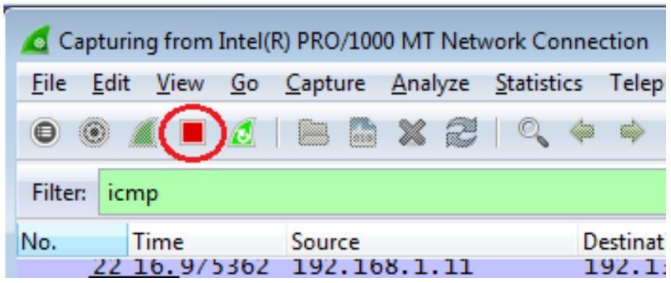


f. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.



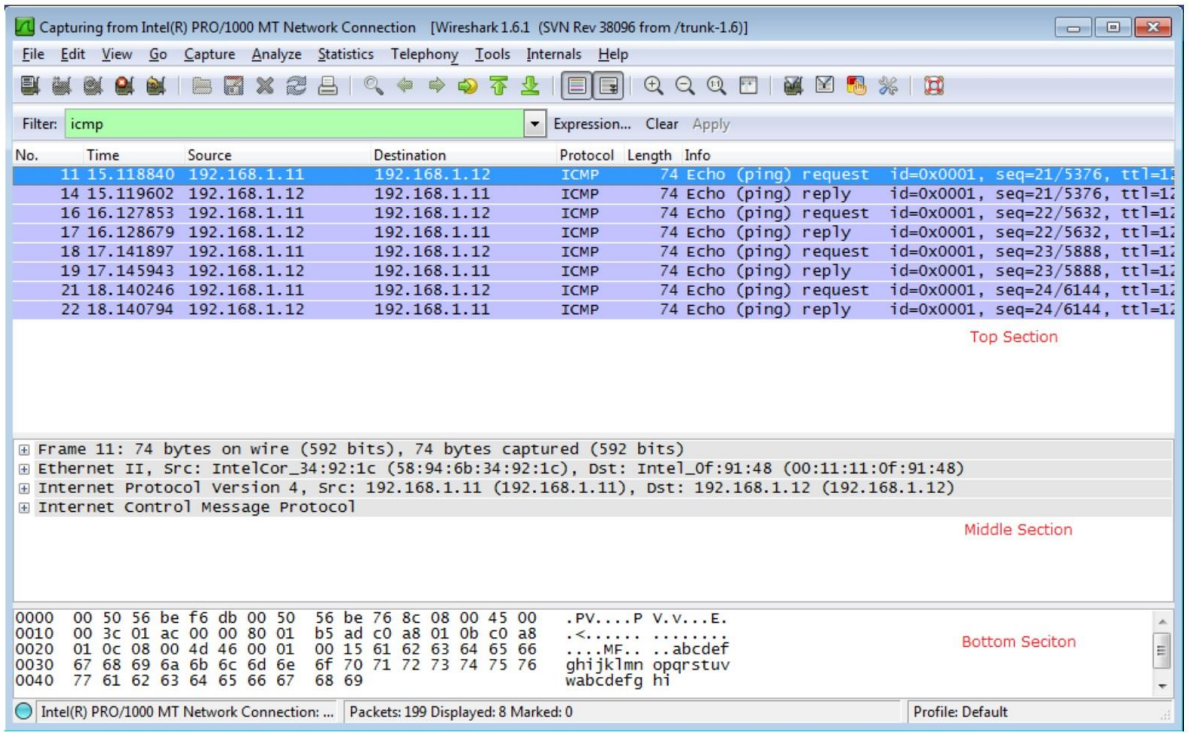
Nota: si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Apéndice A: Permitir el tráfico ICMP a través de un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows 7.

g. Detenga la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).

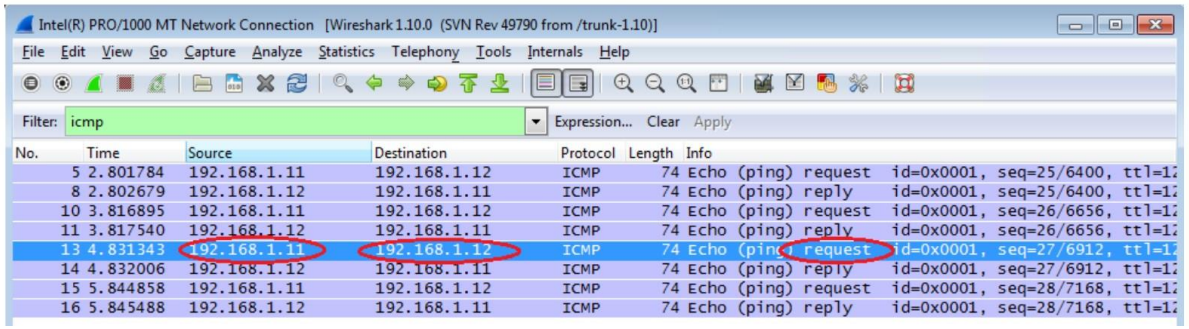


Paso 3: Examinar los datos capturados

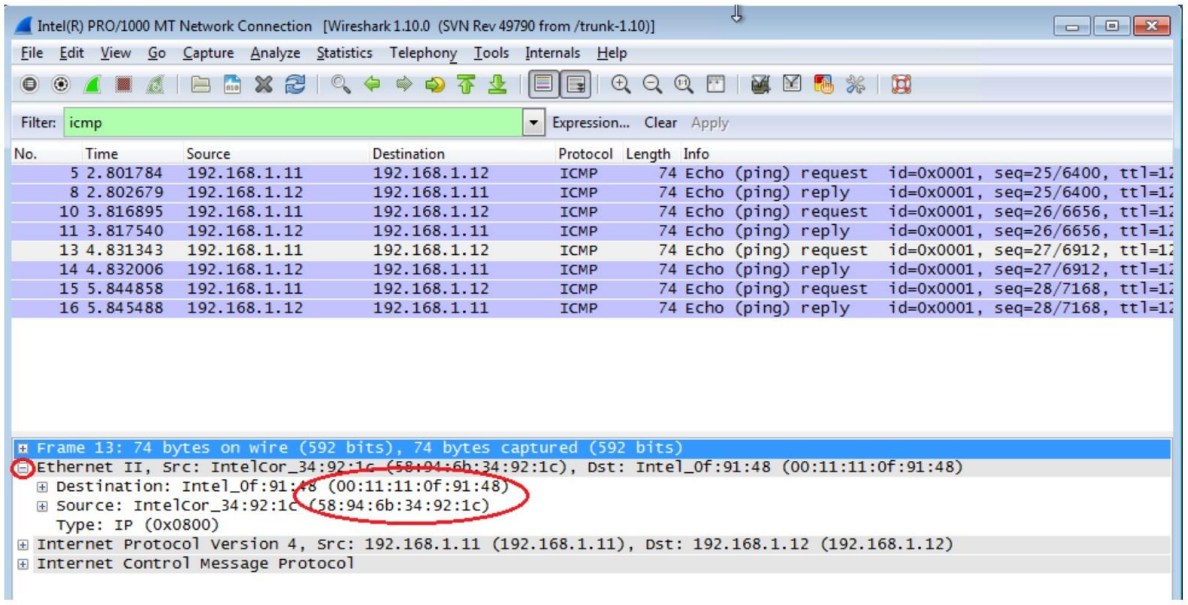
En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.



a. Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Source (Origen) contiene la dirección IP de su PC y la columna Destination (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.



b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.



¿La dirección MAC de origen coincide con la interfaz de su PC?

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del miembro del equipo?

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

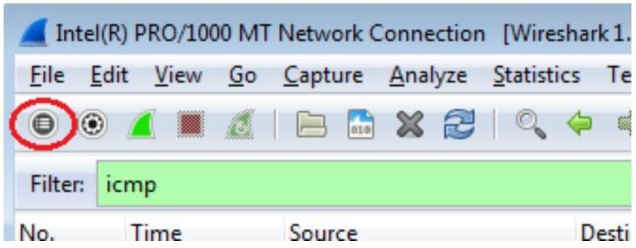
Nota: en el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPV4 (encabezado de IPv4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

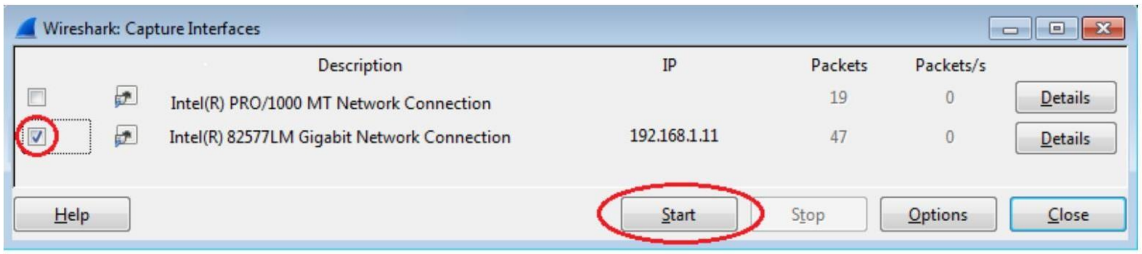
En la parte 3, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 2.

Paso 1: Comenzar a capturar datos en la interfaz

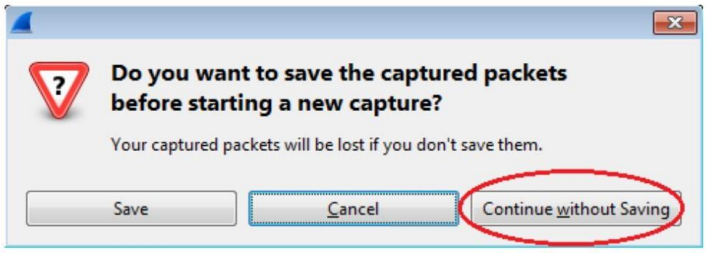
a. Haga clic en el ícono **Interface List** (Lista de interfaces) para volver a abrir la lista de interfaces de la PC.



b. Asegúrese de que la casilla de verificación junto a la interfaz LAN esté activada y, a continuación, haga clic en **Start** (Comenzar).

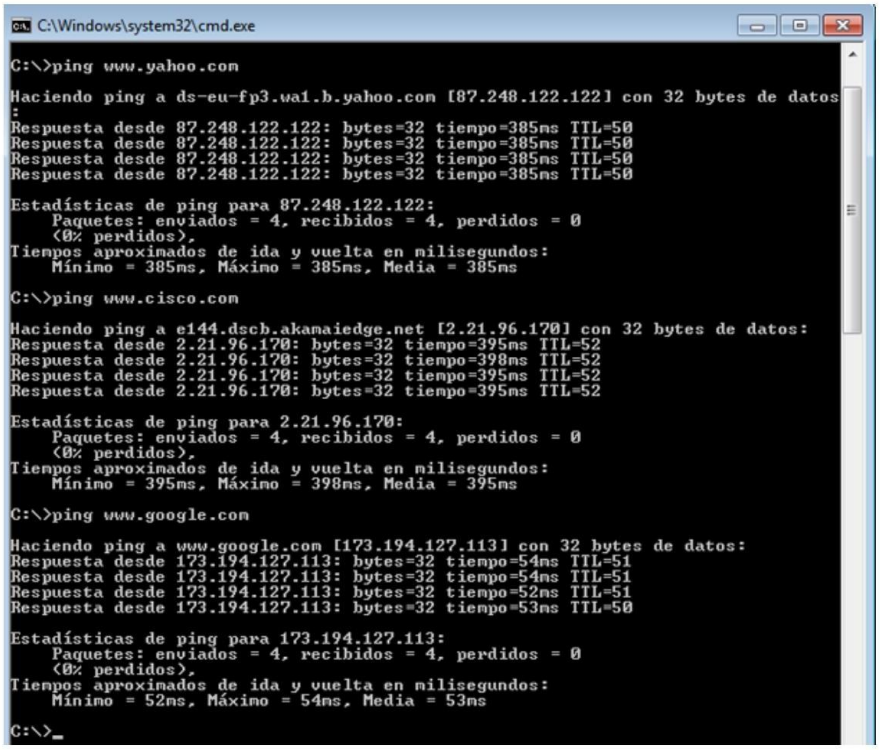


c. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



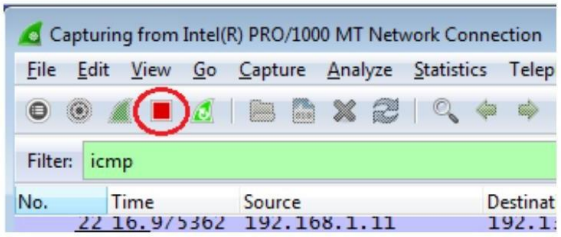
d. Con la captura activa, haga ping a los URL de los tres sitios Web siguientes:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



Nota: al hacer ping a los URL que se indican, observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IP. Observe la dirección IP recibida para cada URL.

e. Puede detener la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).



Paso 2: Inspeccionar y analizar los datos de los hosts remotos

a. Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las tres ubicaciones a las que hizo ping. Indique las direcciones IP y MAC de destino para las tres ubicaciones en el espacio proporcionado.

1.ª ubicación: IP: MAC:

2.ª ubicación: IP: MAC:

3.ª ubicación: IP: MAC:

b. ¿Qué es importante sobre esta información?

c. ¿En qué se diferencia esta información de la información de ping local que recibió en la parte 2?

Reflexión

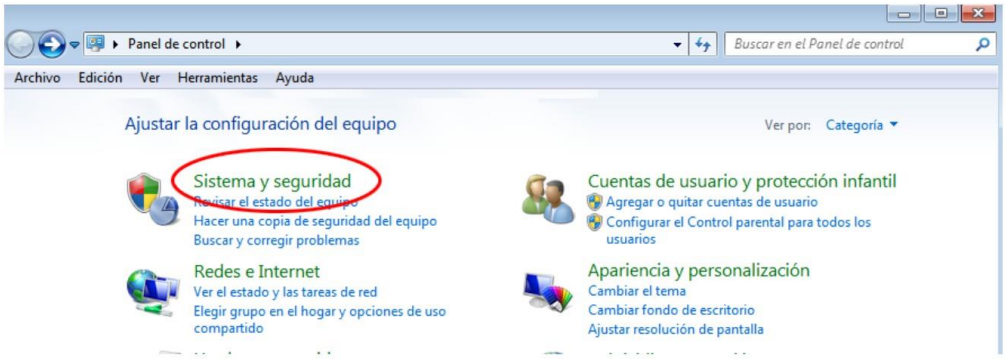
¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

Apéndice A: Permitir el tráfico ICMP a través de un firewall

Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio.

Paso 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

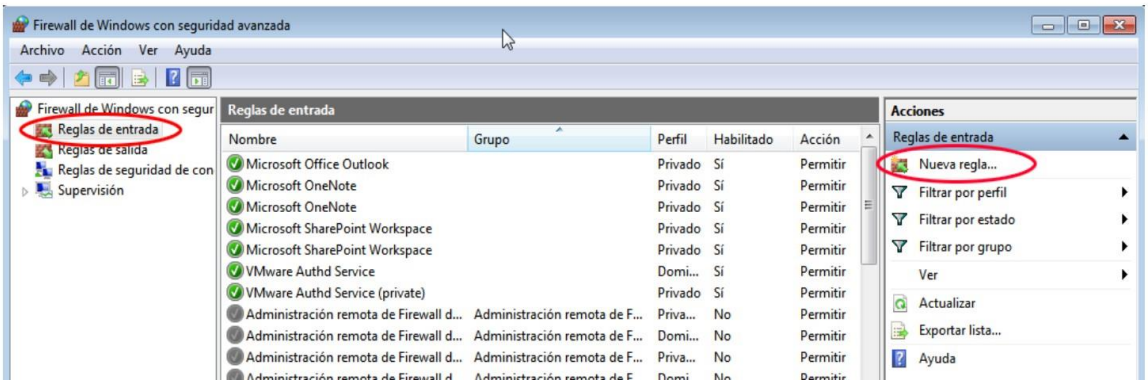
a. En el panel de control, haga clic en la opción **Sistema y seguridad**.



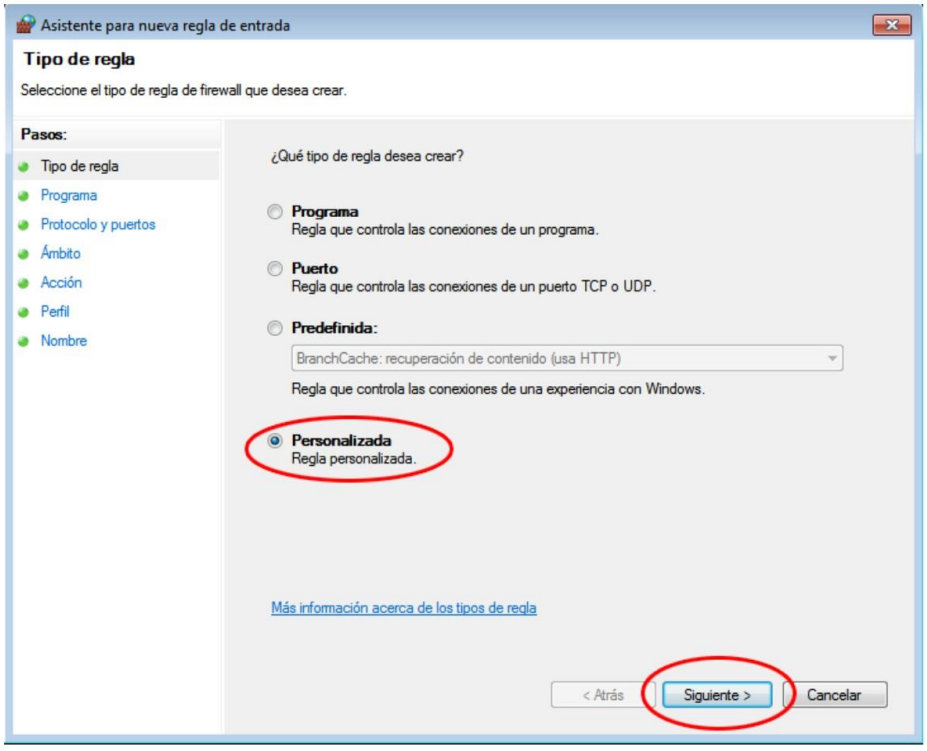
b. En la ventana Sistema y seguridad, haga clic en **Firewall de Windows**.

c. En el panel izquierdo de la ventana Firewall de Windows, haga clic en **Configuración avanzada**.

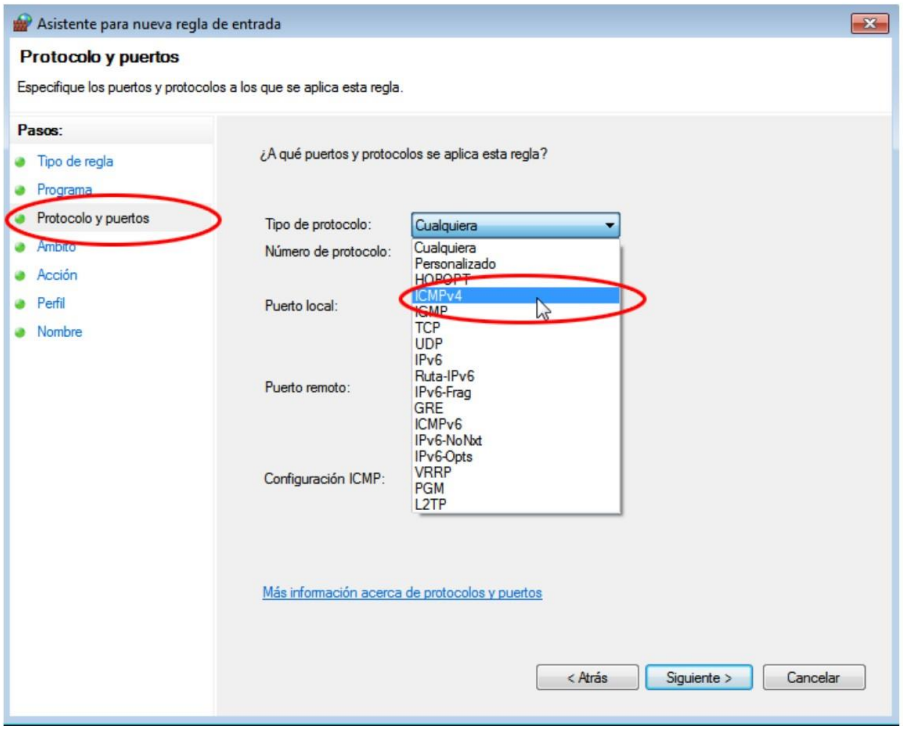
d. En la ventana Seguridad avanzada, seleccione la opción **Reglas de entrada** en la barra lateral izquierda y, a continuación, haga clic **Nueva regla** en la barra lateral derecha.



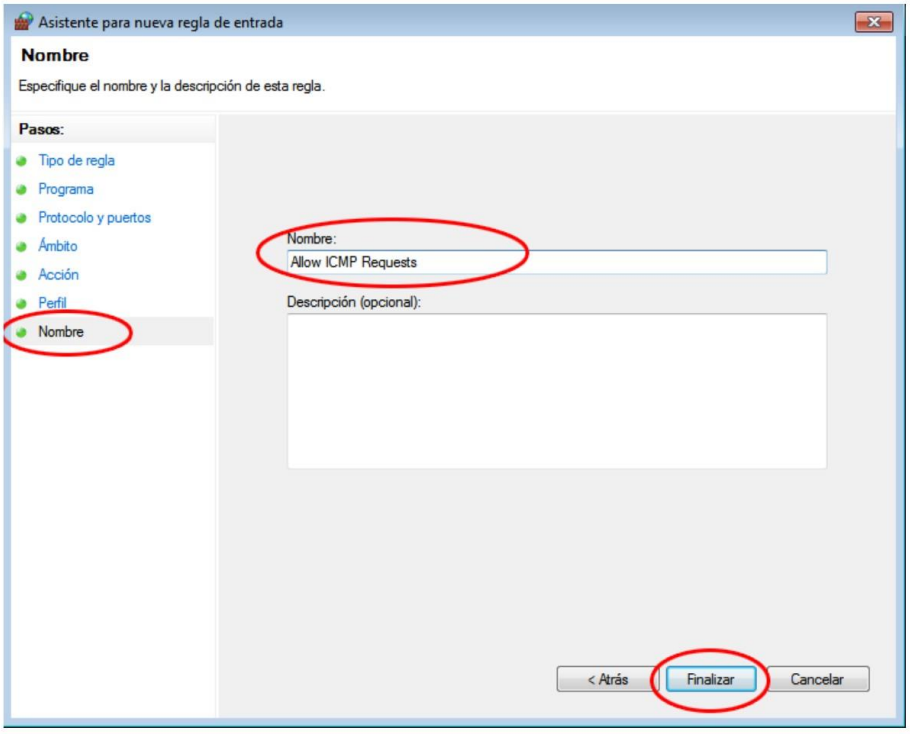
e. Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción **Personalizada** y, a continuación, en **Siguiente.**



f. En el panel izquierdo, haga clic en la opción **Protocolo y puertos**, y en el menú desplegable Tipo de protocolo, seleccione **ICMPv4**; a continuación, haga clic en **Siguiente**.



g. En el panel izquierdo, haga clic en la opción **Nombre**, y en el campo Nombre, escriba **Allow ICMP Requests** (Permitir solicitudes ICMP). Haga clic en **Finish** (Finalizar).

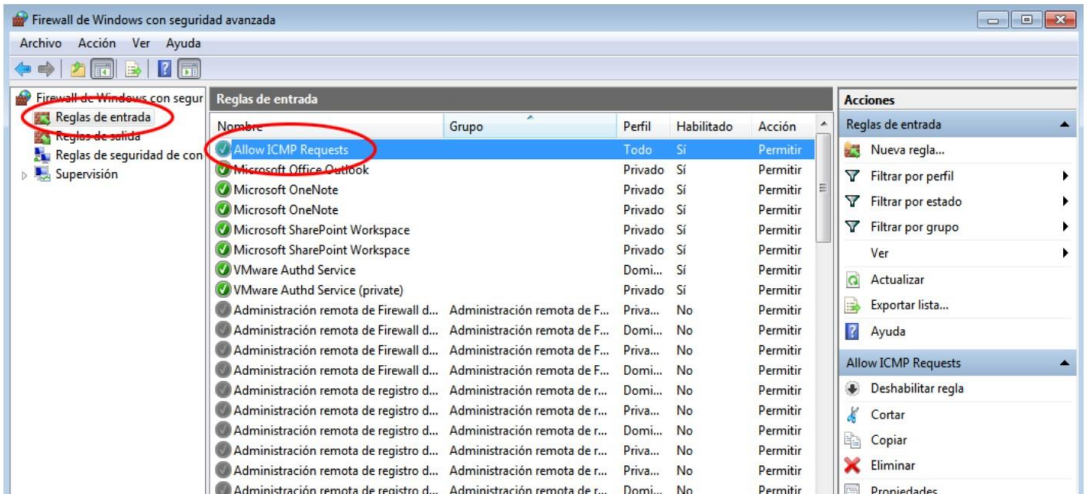


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

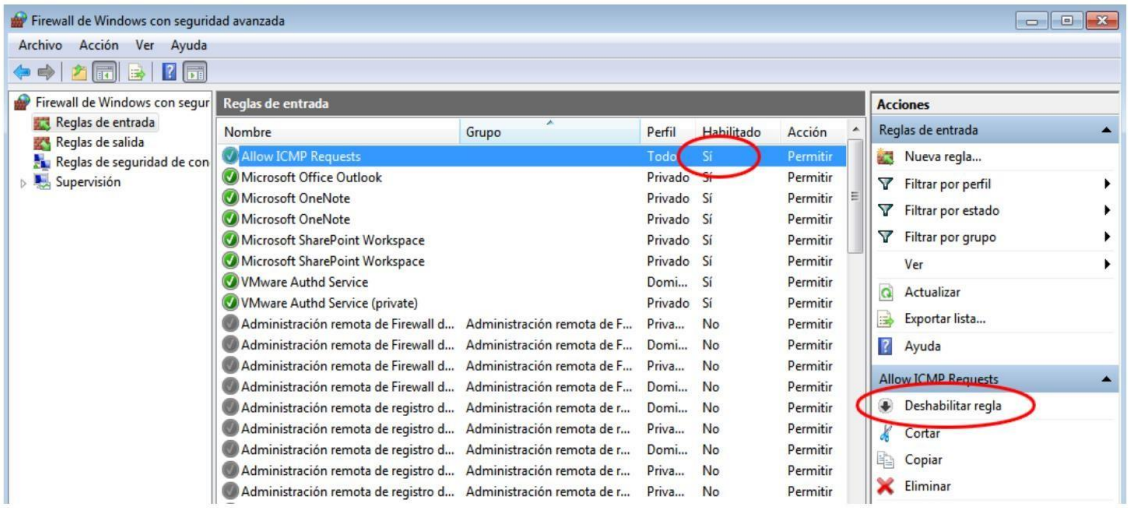
Paso 2: Deshabilitar o eliminar la nueva regla ICMP

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso eliminar la nueva regla que creó en el paso 1. La opción **Deshabilitar regla** permite volver a habilitar la regla en una fecha posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de Reglas de entrada.

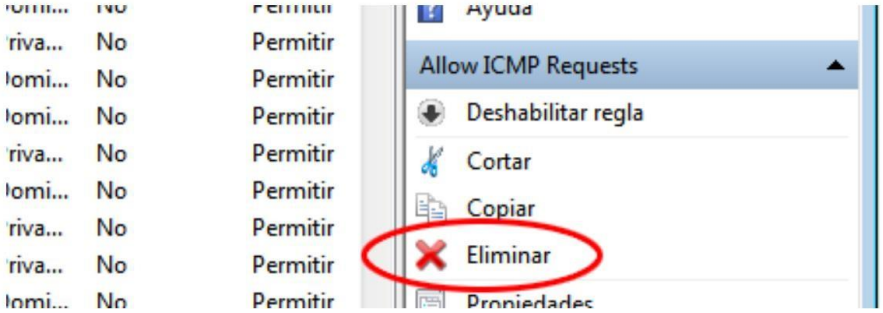
a. En el panel izquierdo de la ventana Seguridad avanzada, haga clic en **Reglas de entrada** y, a continuación, ubique la regla que creó en el paso 1.



b. Para deshabilitar la regla, haga clic en la opción **Deshabilitar regla**. Al seleccionar esta opción, verá que esta cambia a **Habilitar regla**. Puede alternar entre deshabilitar y habilitar la regla; el estado de la regla también se muestra en la columna Habilitada de la lista Reglas de entrada.



c. Para eliminar permanentemente la regla ICMP, haga clic en **Eliminar**. Si elige esta opción, deberá volver a crear la regla para permitir las respuestas de ICMP.



3.4.9.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.9.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.9.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.10 Práctica 10. Armado de un cable cruzado Ethernet

3.4.10.1 Objetivo

Parte 1: Analizar los estándares de cableado y los diagramas de pines de Ethernet.

Parte 2: Armar un cable cruzado Ethernet.

Parte 3: Probar un cable un cable cruzado Ethernet.

3.4.10.2 Introducción

En esta práctica de laboratorio, armará y conectará un cable cruzado Ethernet, y lo probará conectando dos PC y haciendo ping entre ellas. Primero analizará los estándares 568-A y 568-B de la Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) y la forma en que se aplican a los cables Ethernet. Luego armará un cable cruzado Ethernet y lo probará. Por último, utilizará el cable que acaba de armar para conectar dos PC y lo probará haciendo ping entre ellas.

3.4.10.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

1.3 Clasificación de redes y 1.4 Topologías de redes: físicas y Lógicas.

3.4.10.4 Material Y Equipo Necesario

7. Equipo De Cómputo.
8. Conexión A Internet.
9. Packet Tracer

3.4.10.5 Metodología

Parte 1: Analizar los estándares de cableado y los diagramas de pines de Ethernet

La TIA/EIA especificó estándares de cableado de par trenzado no blindado (UTP) para el uso en entornos de cableado LAN. Los estándares 568-A y 568-B de la TIA/EIA estipulan los estándares de cableado comercial para las instalaciones de LAN. Estos son los estándares que se utilizan con mayor frecuencia en el cableado LAN de las organizaciones y determinan qué color de hilo se utiliza en cada pin.

Con un cable cruzado, el segundo y el tercer par del conector RJ-45 en un extremo del cable se invierten en el otro extremo, lo que invierte los pares de envío y recepción. Los diagramas de pines de los cables se realizan conforme al estándar 568-A en un extremo y al estándar 568-B en el otro extremo. Los cables cruzados se suelen utilizar para conectar hubs a hubs o switches a switches, pero también se pueden usar para conectar directamente dos hosts, a fin de crear una red simple.

Nota: en los dispositivos de red modernos, a menudo se puede utilizar un cable directo, incluso cuando se conectan dispositivos similares, debido a su característica de detección automática. La detección automática permite a las interfaces detectar si los pares de los circuitos de envío y recepción están conectados correctamente. Si no es así, las interfaces invierten un extremo de la conexión. La detección automática también modifica la velocidad de las interfaces para que coincidan con la más lenta. Por ejemplo, si se conecta una interfaz del router Gigabit Ethernet (1000 Mb/s) a una interfaz del switch Fast Ethernet (100 Mb/s), la conexión utiliza Fast Ethernet.

El switch Cisco 2960 tiene la función de detección automática activada de manera predeterminada; por lo tanto, la conexión de dos switches 2960 funciona con un cable cruzado o con un cable directo. Con algunos switches anteriores, este no es el caso, y se debe usar un cable cruzado.

Además, las interfaces Gigabit Ethernet del router Cisco 1941 cuentan con la función de detección automática, y se puede usar un cable directo para conectar una PC directamente a la interfaz del router (lo que omite el switch). Con algunos routers anteriores, este no es el caso, y se debe usar un cable cruzado.

Cuando se conectan dos hosts directamente, por lo general, se recomienda utilizar un cable cruzado.

Paso 1: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-A.

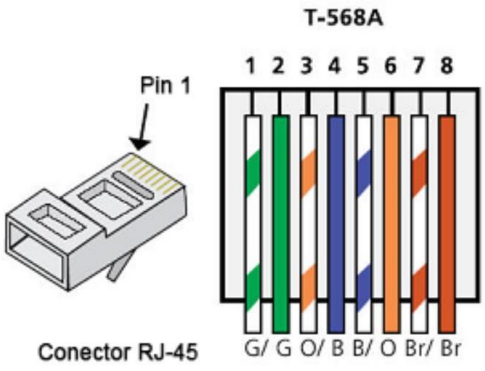
En la tabla y los diagramas siguientes, se muestran el esquema de colores y el diagrama de pines, así como la función de los cuatro pares de hilos que se utilizan para el estándar 568-A.

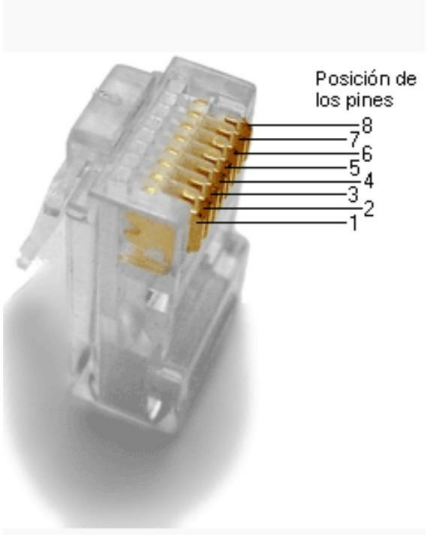
Nota: en las instalaciones de LAN que utilizan 100Base-T (100 Mb/s), se usan solo dos de los cuatro pares.

Ethernet 10/100/1000Base-TX conforme al estándar 568-A

Número de pin	Número de par	Color de hilo	Señal 10Base-T Señal 100Base-TX	Señal 1000Base-T
1	2	Blanco/Verde	Transmitir	BI_DA+
2	2	Verde	Transmitir	BI_DA-
3	3	Blanco/Naranja	Recibir	BI_DB+
4	1	Azul	No se utiliza	BI_DC+
5	1	Blanco/Azul	No se utiliza	BI_DC-
6	3	Naranja	Recibir	BI_DB-
7	4	Blanco/Marrón	No se utiliza	BI_DD+
8	4	Marrón	No se utiliza	BI_DD-

En los diagramas siguientes, se muestra la forma en que el color del hilo y el diagrama de pines se alinean con un conector RJ-45 conforme al estándar 568-A.



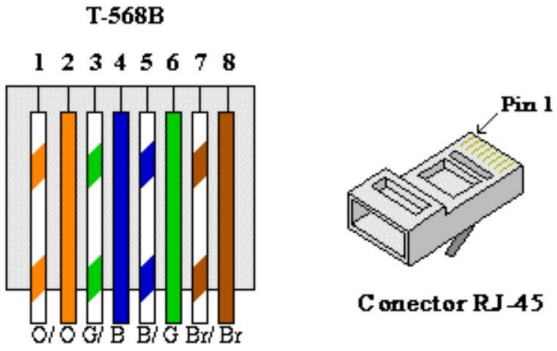


Paso 2: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-B.

En la tabla y el diagrama siguientes, se muestran el esquema de colores y el diagrama de pines conforme al estándar 568-B.

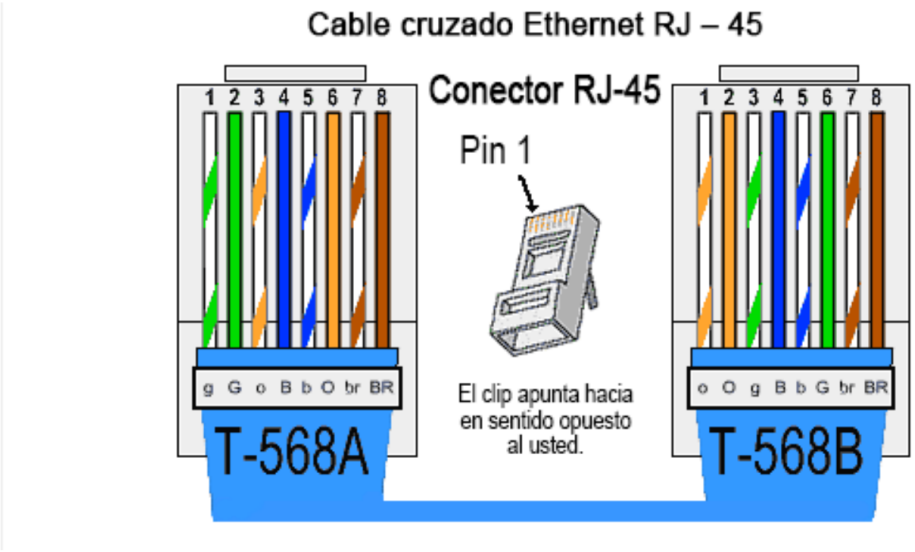
Ethernet 10/100/1000-BaseTX conforme al estándar 568-B

Número de pin	Número de par	Color de hilo	Señal 10Base-T Señal 100Base-TX	Señal 1000Base-T
1	2	Blanco/Naranja	Transmitir	BI_DA+
2	2	Naranja	Transmitir	BI_DA-
3	3	Blanco/Verde	Recibir	BI_DB+
4	1	Azul	No se utiliza	BI_DC+
5	1	Blanco/Azul	No se utiliza	BI_DC-
6	3	Verde	Recibir	BI_DB-
7	4	Blanco/Marrón	No se utiliza	BI_DD+
8	4	Marrón	No se utiliza	BI_DD-



Parte 2: Armar un cable cruzado Ethernet

Un cable cruzado tiene el segundo par y el tercer par del conector RJ-45 en un extremo, invertido en el otro extremo (consulte la tabla de la parte 1, paso 2). Los diagramas de pines de los cables se realizan conforme al estándar 568-A en un extremo y al estándar 568-B en el otro extremo. Los diagramas que siguen ilustran este concepto.



Paso 1: Armar y conectar un extremo del cable TIA/EIA 568-A.

a. Determine la longitud de cable requerida. (El instructor le informará la longitud de cable que debe armar).

   Nota: si estuviera armando un cable en un ambiente de producción, la pauta general indica agregar otras 12 in (30,48 cm) a la longitud.

b. Corte un trozo de cable de la longitud deseada y, con un pelacables, retire 5,08 cm (2 in) del revestimiento de ambos extremos del cable.

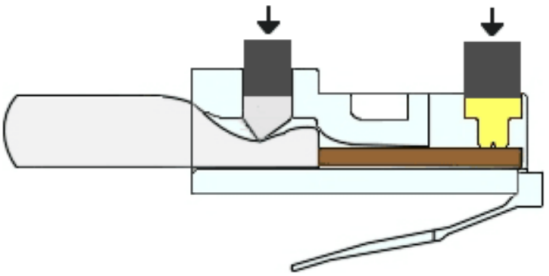
c. Sujete con firmeza los cuatro pares de cables trenzados donde se cortó el revestimiento. Reorganice los pares de cables en el orden que indica el estándar de cableado 568-A. Consulte los diagramas, si es necesario. Tome todas las precauciones posibles para mantener las torsiones del cable, a fin de proporcionar anulación de ruidos.

d. Aplane, enderece y alinee los hilos con los dedos pulgar e índice.

e. Los hilos de los cables deben estar en el orden correcto conforme al estándar 568-A. Utilice el alicate para cortar los cuatro pares en línea recta de 1,25 cm a 1,9 cm (de 1/2 in a 3/4 in).

f. Coloque un conector RJ-45 en el extremo del cable, con la punta de la parte inferior hacia abajo. Inserte con firmeza los hilos en el conector RJ-45. Todos los hilos se deben poder ver en el extremo del conector en la posición correcta. Si los hilos no se extienden hacia el extremo del conector, retire el cable, vuelva a organizar los hilos según sea necesario y vuelva a insertarlos en el conector RJ-45.

g. Si todo está bien, inserte el conector RJ-45 con el cable en la engarzadora. Engarce con fuerza para que los contactos del conector RJ-45 pasen a través del material aislante de los hilos y, de ese modo, completen el camino conductor. Consulte el diagrama siguiente para obtener un ejemplo.



Paso 2: Armar y conectar un extremo del cable TIA/EIA 568-B.

Repita los pasos 1a a 1g utilizando el esquema de colores de hilos establecido en el estándar 568-B para el otro extremo.

Parte 3: Probar un cable cruzado Ethernet

Paso 1: Probar el cable

Muchos comprobadores de cables permiten probar la longitud y el trazado de los hilos. Si el comprobador de cables tiene una característica de trazado, permite comprobar qué pines de un extremo del cable están conectados a qué pines del otro extremo.

Si el instructor tiene un comprobador de cables, pruebe el cable cruzado para corroborar la funcionalidad. Si falla, corrobore primero con el instructor si debe volver a conectar los extremos de los cables y vuelva a probarlos.

Paso 2: Conectar dos PC mediante NIC utilizando el cable cruzado Ethernet

a. Trabaje con un compañero para configurar la PC en una de las direcciones IP que aparecen en la tabla de direccionamiento (consulte la página 1). Por ejemplo, si la PC es la **PC-A**, la dirección IP debe configurarse en **192.168.10.1** con una **máscara de subred de 24 bits**. La dirección IP de su compañero debe ser **192.168.10.2**. La dirección de gateway predeterminado puede dejarse en blanco.

b. Utilice el cable cruzado que armó y conecte las dos PC con las NIC.

c. En el símbolo del sistema de la PC-A, haga ping a la dirección IP de la PC-B.

Nota: es posible que el Firewall de Windows tenga que deshabilitarse temporalmente para que los pings sean correctos. Si el firewall se deshabilita, vuelva a habilitarlo al final de esta práctica de laboratorio.

d. Repita el proceso y haga ping de la PC-B a la PC-A.

Si el direccionamiento IP y el firewall no son un problema, los pings deben ser correctos si los cables se armaron como corresponde.

Reflexión

1. ¿Qué parte del armado de cables le pareció más difícil?

2. ¿Por qué tiene que aprender a armar un cable si puede comprar cables ya armados?

3.4.10.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.10.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.10.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.11 Práctica 11 Conexión de una LAN por cable y una LAN inalámbrica

3.4.11.1 Objetivo

Parte 1: Conectarse a la nube

Parte 2: Conectar el Router0

Parte 3: Conectar los dispositivos restantes

Parte 4: Verificar las conexiones

Parte 5: Examinar la topología física

3.4.11.2 Introducción

Al trabajar en Packet Tracer (un entorno de laboratorio o un contexto empresarial), debe saber cómo seleccionar el cable adecuado y como conectar correctamente los dispositivos. En esta actividad se analizarán configuraciones de dispositivos en el Packet Tracer, se seleccionarán los cables adecuados según la configuración y se conectarán los dispositivos. Esta actividad también explorará la vista física de la red en el Packet Tracer.

3.4.11.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

2.1 Modelo de Comunicación OSI y 2.2 Modelo de Comunicación TCP/IP

3.4.11.4 Material Y Equipo Necesario

- Equipo De Cómputo.
- Conexión A Internet.
- Packet Tracer

3.4.11.5 Metodología

Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0

a. En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las **conexiones** disponibles.

b. Elija el cable adecuado para conectar la **interfaz Fa0/0 del Router0** a la **interfaz Eth6 de la nube**. La **nube** es un tipo de switch, de modo que debe usar una conexión por **cable de cobre de conexión directa**. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar la nube al módem por cable

Elija el cable adecuado para conectar la **interfaz Coax7 de la nube** al **Puerto0 del módem**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

Elija el cable adecuado para conectar la **interfaz Ser0/0/0 del Router0** a la **interfaz Ser0/0 del Router1**. Use uno de los cables **seriales** disponibles.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar el Router0 a netacad.pka

Elija el cable adecuado para conectar la **interfaz Fa0/1 del Router0** a la **interfaz Fa0 de netacad.pka**. Los routers y las PC tradicionalmente utilizan los mismos cables para transmitir (1 y 2) y recibir (3 y 6). El cable adecuado que se debe elegir consta de cables cruzados. Si bien muchas NIC ahora pueden detectar automáticamente qué par se utiliza para transmitir y recibir, el **Router0** y **netacad.pka** no tienen NIC con detección automática.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 3: Conectar el Router0 a la terminal de configuración

Elija el cable adecuado para conectar la **consola** del **Router0** a la **terminal de configuración RS232**. Este cable no proporciona acceso a la red a la **terminal de configuración**, pero le permite configurar el **Router0** a través de su terminal.

Si conectó el cable correcto, las luces de enlace del cable cambian a color negro.

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

Elija el cable adecuado para conectar la **interfaz Fa1/0 del Router1** a la **interfaz Fa0/1 del switch**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde. Deje que transcurran unos segundos para que la luz cambie de color ámbar a verde.

Paso 2: Conectar el módem por cable al router inalámbrico

Elija el cable adecuado para conectar el **Puerto1** del **módem** al puerto de **Internet del router inalámbrico**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 3: Conectar el router inalámbrico a la PC familiar

Elija el cable adecuado para conectar la **interfaz Ethernet 1 del router inalámbrico** a la **PC familiar**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka

a. Abra el símbolo del sistema de la **PC familiar** y haga ping a **netacad.pka**.

b. Abra el **explorador Web** e introduzca dirección Web **http://netacad.pka**.

Paso 2: Hacer ping al switch desde la PC doméstica

Abra el símbolo del sistema de la **PC doméstica** y haga ping a la dirección IP del **switch** para verificar la conexión.

Paso 3: Abrir el Router0 desde la terminal de configuración

a. Abra la **terminal** de la **terminal de configuración** y acepte la configuración predeterminada.

b. Presione **Entrar** para ver el símbolo del sistema del **Router0**.

c. Escriba **show ip interface brief** para ver el estado de las interfaces.

Parte 5: Examinar la topología física

Paso 1: Examinar la nube

a. Haga clic en la ficha **Physical Workspace** (Área de trabajo física) o presione **Mayús** + **P** y **Mayús** + **L** para alternar entre las áreas de trabajo lógicas y físicas.

b. Haga clic en el ícono **Home City** (Ciudad de residencia).

c. Haga clic en el ícono **Cloud** (Nube). ¿Cuántos cables están conectados al switch en el bastidor azul?

d. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

Paso 2: Examinar la red principal

a. Haga clic en el ícono **Primary Network** (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul?

b. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

Paso 3: Examinar la red secundaria

a. Haga clic en el ícono **Secondary Network** (Red secundaria). Mantenga el puntero del mouse sobre los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo?

b. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

Paso 4: Examinar la red doméstica

a. ¿Por qué hay una malla ovalada que cubre la red doméstica?

b. Haga clic en el ícono **Home Network** (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo?

c. Haga clic en la ficha **Logical Workspace** (Área de trabajo lógica) para volver a la topología lógica.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 5: Examinar la topología física	Paso 1c	4	
	Paso 2a	4	
	Paso 3a	4	
	Paso 4a	4	
	Paso 4b	4	
Total de la parte 5		**20**	
Puntuación de Packet Tracer		**80**	
Puntuación total		**100**	

3.4.11.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.11.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.11.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.12 Práctica 12 Identificación de direcciones MAC y direcciones IP

3.4.12.1 Objetivo

Parte 1: Recopilar información de la PDU

Parte 2: Preguntas de reflexión

3.4.12.2 Introducción

Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

3.4.12.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

2.1 Modelo de Comunicación OSI y 2.2 Modelo de Comunicación TCP/IP

3.4.12.4 Material Y Equipo Necesario

1. Equipo De Cómputo.
2. Conexión A Internet.
3. Packet Tracer

3.4.12.5 Metodología

Parte 1: Recopilar información de la PDU

Nota: revise las preguntas de reflexión de la parte 2 antes de continuar con la parte 1. Le darán una idea de los tipos de información que debe recopilar.

Paso 1: Recopilar información de la PDU mientras un paquete se transfiere de 172.16.31.2 a 10.10.10.3

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

b. Introduzca el comando **ping 10.10.10.3**.

c. Cambie al modo de simulación y repita el comando **ping 10.10.10.3**. Aparece una PDU junto a **172.16.31.2**.

d. Haga clic en la PDU y observe la siguiente información en la ficha **Outbound PDU Layer** (Capa de PDU saliente):

- Dirección MAC de destino: 00D0:BA8E:741A
- Dirección MAC de origen: 000C:85CC:1DA7

- Dirección IP de origen: 172.16.31.2
- Dirección IP de destino: 10.10.10.3
- En el dispositivo: PC

e. Haga **clic en Capture/Forward (Capturar/reenviar)** para mover la PDU al siguiente dispositivo. Recopile la misma información del paso 1d. Repita este proceso hasta que la PDU llegue al destino. Registre la información que recopiló de la PDU en una hoja de cálculo con un formato como el de la tabla que se muestra a continuación:

Formato de hoja de cálculo de ejemplo

Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Punto de acceso	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

Paso 2: Recopilar información adicional de la PDU de otros ping

Repita el proceso del paso 1 y recopile información para las pruebas siguientes:

- Ping de 10.10.10.2 a 10.10.10.3
- Ping de 172.16.31.2 a 172.16.31.3
- Ping de 172.16.31.4 a 172.16.31.5
- Ping de 172.16.31.4 a 10.10.10.2
- Ping de 172.16.31.3 a 10.10.10.2

Parte 2: Preguntas de reflexión

Responda las siguientes preguntas relacionadas con la información reunida:

1. ¿Se utilizaron diferentes tipos de cables para conectar los dispositivos?
2. ¿Los cables cambiaron el manejo de la PDU de alguna forma?
3. ¿El **hub** perdió la información que se le entregó?
4. ¿Qué hace el **hub** con las direcciones MAC y las direcciones IP?
5. ¿El **punto de acceso inalámbrico** hizo algo con la información que se le entregó?

6. ¿Se perdió alguna dirección MAC o IP durante la transferencia inalámbrica?
7. ¿Cuál fue la capa OSI más alta que utilizaron el **hub** y el **punto de acceso**?

3.4.12.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.12.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.12.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.13 Práctica 13 Configuración de una dirección de administración del switch

3.4.13.1 Objetivo

Parte 1: Examinar una solicitud de ARP

Parte 2: Examinar una tabla de direcciones MAC del switch

Parte 3: Examinar el proceso de ARP en comunicaciones remotas.

3.4.13.2 Introducción

Esta actividad esta optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una seria de preguntas sobre los datos que obtenga.

3.4.13.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

2.1 Modelo de Comunicación OS y 2.2 Modelo de Comunicación TCP/IP

3.4.13.4 Material Y Equipo Necesario

4. Equipo De Cómputo.
5. Conexión A Internet.
6. Packet Tracer

3.4.13.5 Metodología

Parte 1: Examinar una solicitud de ARP

Paso 1: Generar solicitudes de ARP haciendo ping a 172.16.31.3 desde 172.16.31.2

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

b. Introduzca el comando **arp -d** para borrar la tabla ARP.

c. Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3**. Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.

d. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. La PDU ARP mueve el **Switch1**, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior?

e. Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**?

f. ¿Cuál es la dirección IP del dispositivo que aceptó la PDU?

g. Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino?

h. Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP?

Paso 2: Revisar la tabla ARP

a. Observe que vuelve a aparecer el paquete ICMP. Abra la PDU y revise las direcciones MAC. ¿Las direcciones MAC de origen y destino coinciden con sus direcciones IP?

b. Vuelva a cambiar al modo **Realtime** (Tiempo real), y el ping se completa.

c. Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC?

d. En general, ¿cuándo emite un dispositivo final una solicitud de ARP?

Parte 2: Examinar una tabla de direcciones MAC del switch

Paso 1: Generar tráfico adicional para completar la tabla de direcciones MAC del switch

a. En **172.16.31.2**, introduzca el comando **ping 172.16.31.4**.

b. Haga clic en **10.10.10.2** y abra el **símbolo del sistema**.

c. Introduzca el comando **ping 10.10.10.3**. ¿Cuántas respuestas se enviaron y se recibieron?

Paso 2: Examinar la tabla de direcciones MAC en los switches

a. Haga clic en **Switch1** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla anterior?

b. Haga clic en **Switch0** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla anterior?

c. ¿Por qué hay dos direcciones MAC asociadas a un puerto?

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

b. Introduzca el comando **ping 10.10.10.1**.

c. Escriba **arp -a**. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP?

d. Introduzca el comando **arp -d** para borrar la tabla ARP y volver a cambiar al modo de **simulación**.

e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen?

f. Haga clic en **Capture/Forward** (Capturar/avanzar). Haga clic en la PDU que ahora se encuentra en el **Switch1**. ¿Cuál es la dirección IP de destino de la solicitud de ARP?

g. La dirección IP de destino no es 10.10.10.1. ¿Por qué?

Paso 2: Examinar la tabla ARP en el Router1

a. Cambie al modo **Realtime**. Haga clic en **Router1** y, a continuación, en la ficha **CLI**.

b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué?

c. Introduzca el comando **show arp**. ¿Figura una entrada para **172.16.31.2**?

d. ¿Qué sucede con el primer ping en una situación en la que el router responde a la solicitud de ARP?

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar una solicitud de ARP	Paso 1	10	
	Paso 2	15	
	Total de la parte 1	**25**	
Parte 2: Examinar una tabla de direcciones MAC del switch	Paso 1	5	
	Paso 2	20	
	Total de la parte 2	**25**	
Parte 3: Examinar el proceso de ARP en comunicaciones remotas	Paso 1	25	
	Paso 2	25	
	Total de la parte 3	**50**	
	Puntuación total	**100**	

3.4.13.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.13.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.13.8 Bibliografías

Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.14 Práctica 14. Configuración de switches de capa 3

3.4.14.1 Objetivo

Parte 1: Documentar la configuración actual de la red

Parte 2: Configurar, implementar y probar el nuevo switch multicapa

3.4.14.2 Introducción

Configurar switches de capa 3 implica habilitar capacidades de enrutamiento en un switch, lo que le permite tomar decisiones de enrutamiento y enrutar tráfico IP entre diferentes redes. A continuación, se muestra una guía básica para configurar un switch de capa 3. Ten en cuenta que los comandos y la sintaxis pueden variar según la marca y el modelo del switch. En este ejemplo, se asume que estás utilizando un switch Cisco como referencia.

3.4.14.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.14.4 Material Y Equipo Necesario

7. Equipo De Cómputo.
8. Conexión A Internet.
9. Packet Tracer

3.4.14.5 Metodología

Parte 1: Documentar la configuración actual de la red

Nota: por lo general, un router de producción tendría muchas más configuraciones que simplemente el direccionamiento IP de las interfaces. Sin embargo, para agilizar esta actividad, se configuró solo el direccionamiento IP de interfaces en **R1**.

a. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**.

b. Utilice los comandos disponibles para recopilar información sobre el direccionamiento de interfaces.

c. Registre la información en la **tabla de direccionamiento**.

Parte 2: Configurar, implementar y probar el nuevo switch multicapa

Paso 1: Configurar MLSw1 para utilizar el esquema de direccionamiento de R1

a. Haga clic en **MLSw1** y, a continuación, en la ficha **CLI**.

b. Ingrese al modo de configuración de interfaz para **GigabitEthernet 0/1**.

c. Cambie el puerto al modo de enrutamiento introduciendo el comando **no switchport**.

d. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/1** y active el puerto.

e. Ingrese al modo de configuración de interfaz para **interface VLAN1**.

f. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/0** y active el puerto.

g. Guarde la configuración.

Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

Nota: por lo general, los siguientes pasos se llevarían a cabo después del horario laboral o cuando el tráfico en la red de producción está en su volumen más bajo. Para minimizar el tiempo de inactividad, el nuevo equipo debe estar totalmente configurado y listo para implementar.

a. Haga clic en un área vacía de la pantalla para anular la selección de todos los dispositivos.

b. Use la herramienta **Delete** (Eliminar) para eliminar todas las conexiones o simplemente elimine **R1**, **S1** y **S2**.

c. Seleccione los cables adecuados para completar lo siguiente:

- Conectar **MLSw1 GigabitEthernet 0/1** a **Edge GigabitEthernet 0/0**.
- Conectar las PC a los puertos Fast Ethernet en **MLSw1**.

d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.

Nota: espere hasta que las luces de enlace anaranjadas cambien a color verde.

3.4.14.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.14.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.14.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.15 Práctica 15. Exploración de dispositivos de internetworking

3.4.15.1 Objetivo

Parte 1: Identificar las características físicas de los dispositivos de internetworking.

Parte 2: Seleccionar los módulos correctos para la conectividad.

Parte 3: Conectar los dispositivos.

3.4.15.2 Introducción

En esta actividad, explorará las diversas opciones disponibles de internetworking. También deberá determinar que opciones proporcionan la conectividad necesaria al conectar varios dispositivos. Finalmente, agregará los módulos correctos y conectará los dispositivos.

3.4.15.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.4.15.4 Material Y Equipo Necesario

10. Equipo De Cómputo.
11. Conexión A Internet.
12. Packet Tracer

3.4.15.5 Metodología

Parte 1: Identificar las características físicas de los dispositivos de internetworking

Paso 1: Identificar los puertos de administración de un router Cisco

a. Haga clic en el router **East** (Este). La ficha **Physical** (Capa física) debe estar activa.

b. Acerque el elemento y expanda la ventana para ver todo el router.

c. ¿Qué puertos de administración se encuentran disponibles?

Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay?

b. Haga clic en la ficha **CLI** e introduzca los siguientes comandos:

```
East> show ip interface brief
```

El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican?

c. Introduzca los siguientes comandos:

```
East> show interface gigabitethernet 0/0
```

¿Cuál es el ancho de banda predeterminado de esta interfaz?

```
East> show interface serial 0/0/0
```

¿Cuál es el ancho de banda predeterminado de esta interfaz?

Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

Paso 3: Identificar las ranuras de expansión de módulos en los switches

a. ¿Cuántas ranuras de expansión se encuentran disponibles para agregar más módulos al router **East**?

b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles?

Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

a. Haga clic en **East** y, a continuación, haga clic en la ficha **Physical**. En el lado izquierdo, debajo de la etiqueta **Modules** (Módulos), se ven las opciones disponibles para expandir las capacidades del router. Haga clic en cada módulo. Se muestra una imagen y una descripción en la parte inferior. Familiarícese con estas opciones.

1) Debe conectar las PC 1, 2 y 3 al router **East**, pero no cuenta con los fondos necesarios para adquirir un nuevo switch. ¿Qué módulo puede usar para conectar las tres PC al router **East**?

2) ¿Cuántos hosts puede conectar al router mediante este módulo?

b. Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**?

Paso 2: Agregar los módulos correctos y encender los dispositivos

a. Haga clic en **East** e intente insertar el módulo adecuado del paso 1a.

b. Debe aparecer el mensaje `Cannot add a module when the power is on` (No se puede agregar un módulo cuando el dispositivo está encendido). Las interfaces para este modelo de router no son intercambiables en caliente. Se debe apagar el dispositivo. Haga clic en el interruptor de alimentación que se encuentra a la derecha del logotipo de Cisco para apagar **East**. Inserte el módulo adecuado del paso 1a. Cuando haya terminado, haga clic en el interruptor de alimentación para encender **East**.

Nota: si inserta el módulo incorrecto y debe quitarlo, arrastre el módulo hasta su imagen en la esquina inferior derecha y suelte el botón del mouse.

c. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo.

¿En qué ranura se insertó?

e. Haga clic en el router **West** (Oeste). La ficha **Physical** (Capa física) debe estar activa. Instale el módulo adecuado que agregará una interfaz serial a la ranura para tarjetas de interfaz WAN de alta velocidad mejoradas (**EHWIC 0**) de la derecha. Puede cubrir las ranuras sin utilizar para evitar que ingrese polvo al router (optativo).

f. Use el comando adecuado para verificar que se hayan instalado las nuevas interfaces seriales.

Parte 3: Conectar los dispositivos

Esta puede ser la primera actividad que realiza en la que se le solicita conectar dispositivos. Si bien es posible que no conozca el propósito de los distintos tipos de cables, use la tabla que se encuentra a continuación y siga estas pautas para conectar correctamente todos los dispositivos:

a. Seleccione el tipo de cable adecuado.

b. Haga clic en el primer dispositivo y seleccione la interfaz especificada.

c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.

d. Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

Ejemplo: para conectar **East** al **Switch1**, seleccione el tipo de cable de **cobre de conexión directa**. Haga clic en **East** y elija **GigabitEthernet0/0**. Luego, haga clic en **Switch1** y elija **GigabitEthernet1/1**. Su puntuación ahora debe ser de 4/52.

Nota: a los efectos de esta actividad, se deshabilitaron las luces de enlace. Los dispositivos no están configurados con ningún direccionamiento IP, de modo que no puede probar la conectividad.

Dispositivo	Interfaz	Tipo de cable	Dispositivo	Interfaz
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet1/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet1/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0
Switch1	FastEthernet0/1	Cable de cobre de conexión directa	PC4	FastEthernet0
Switch1	FastEthernet0/2	Cable de cobre de conexión directa	PC5	FastEthernet0
Switch1	FastEthernet0/3	Cable de cobre de conexión directa	PC6	FastEthernet0
Switch4	GigabitEthernet1/2	Cross-Over de cobre	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fibra	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Cable de cobre de conexión directa	PC7	FastEthernet0
Switch2	FastEthernet1/1	Cable de cobre de conexión directa	PC8	FastEthernet0
Switch2	FastEthernet2/1	Cable de cobre de conexión directa	PC9	FastEthernet0
East	Serial0/0/0	DCE serial (conectar primero a East)	West	Serial0/0/0

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Identificar las características físicas de los dispositivos de internetworking	Paso 1c	4	
	Paso 2a	4	
	Paso 2b	4	
	Paso 2c, pregunta 1	4	
	Paso 2c, pregunta 2	4	
	Paso 3a	4	
	Paso 3b	4	
Total de la parte 1		**28**	
Parte 2: Seleccionar los módulos correctos para la conectividad	Paso 1a, pregunta 1	5	
	Paso 1a, pregunta 2	5	
	Paso 1b	5	
	Paso 2d	5	
Total de la parte 2		**20**	
Puntuación de Packet Tracer		**52**	
Puntuación total		**100**	

3.4.15.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.15.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.15.8 Bibliografías

Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.16 Práctica 16 Configuración inicial del router

3.4.16.1 Objetivo

Parte 1: Verificar la configuración predeterminada del router.

Parte 2: Configurar y verificar la configuración inicial del router.

Parte 3: Guardar el archivo de configuración en ejecución.

3.4.16.2 Introducción

En esta actividad, configurará los parámetros básicos del router. Proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También configurará mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten a los usuarios no autorizados que el acceso está prohibido. Finalmente, verificará y guardará la configuración en ejecución.

3.4.16.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.16.4 Material Y Equipo Necesario

13. Equipo De Cómputo.
14. Conexión A Internet.
15. Packet Tracer

3.4.16.5 Metodología

Parte 1: Verificar la configuración predeterminada del router

Paso 1: Establecer una conexión de consola al R1

a. Elija un cable de **consola** de las conexiones disponibles.

b. Haga clic en **PCA** y seleccione **RS 232**.

c. Haga clic en **R1** y seleccione **Console** (Consola).

d. Haga clic en **PCA** > ficha **Desktop** (Escritorio) > **Terminal**.

e. Haga clic en **OK** (Aceptar) y presione **Entrar**. Ahora puede configurar **R1**.

Paso 2: Ingresar al modo privilegiado y examinar la configuración actual

Puede acceder a todos los comandos del router en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

a. Introduzca el modo EXEC privilegiado introduciendo el comando **enable.**

```
Router> enable
Router#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

b. Introduzca el comando **show running-config**:

```
Router# show running-config
```

c. Responda las siguientes preguntas:

¿Cuál es el nombre de host del router?

¿Cuántas interfaces Fast Ethernet tiene el router?

¿Cuántas interfaces Gigabit Ethernet tiene el router? _____

¿Cuántas interfaces seriales tiene el router?

¿Cuál es el rango de valores que se muestra para las líneas vty?

d. Muestre el contenido actual de la NVRAM.

```
Router# show startup-config
startup-config is not present
```

¿Por qué el router responde con el mensaje `startup-config is not present`?

Parte 2: Configurar y verificar la configuración inicial del router

Para configurar los parámetros de un router, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el router.

Paso 1: Configurar los parámetros iniciales de R1

Nota: si tiene dificultad para recordar los comandos, consulte el contenido de este tema. Los comandos son los mismos que configuró en un switch.

a. Establezca **R1** como nombre de host.

b. Utilice las siguientes contraseñas:

1) Consola: **letmein**

2) EXEC privilegiado, sin encriptar: **cisco**

3) EXEC privilegiado, encriptado: **itsasecret**

c. Encripte todas las contraseñas de texto no cifrado.

d. Texto del mensaje del día: `Unauthorized access is strictly prohibited` (El acceso no autorizado queda terminantemente prohibido).

Paso 2: Verificar los parámetros iniciales de R1

a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza?

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:

```
R1 con0 is now available

Press RETURN to get started.
```

c. Presione **Entrar**; debería ver el siguiente mensaje:

```
Unauthorized access is strictly prohibited.

User Access Verification
```

```
Password:
```

¿Por qué todos los routers deben tener un mensaje del día (MOTD)?

Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?

d. Introduzca las contraseñas necesarias para regresar al modo EXEC privilegiado.

¿Por qué la contraseña **secreta de enable** permitiría el acceso al modo EXEC privilegiado y **la contraseña de enable** dejaría de ser válida?

Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique.

Parte 3: Guardar el archivo de configuración en ejecución

Paso 1: Guarde el archivo de configuración en la NVRAM.

a. Configuró los parámetros iniciales de **R1**. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM?

¿Cuál es la versión más corta e inequívoca de este comando?

¿Qué comando muestra el contenido de la NVRAM?

b. Verifique que todos los parámetros configurados estén registrados. Si no fuera así, analice el resultado y determine qué comandos no se introdujeron o se introdujeron incorrectamente. También puede hacer clic en **Check Results** (Verificar resultados) en la ventana de instrucción.

Paso 2: Puntos extra optativos: guarde el archivo de configuración de inicio en la memoria flash.

Aunque aprenderá más sobre la administración del almacenamiento flash de un router en los siguientes capítulos, le puede interesar saber ahora que puede guardar el archivo de configuración de inicio en la memoria flash como procedimiento de respaldo adicional. De manera predeterminada, el router seguirá cargando la configuración de inicio desde la NVRAM, pero si esta se daña, puede restablecer la configuración de inicio copiándola de la memoria flash.

Complete los siguientes pasos para guardar la configuración de inicio en la memoria flash.

a. Examine el contenido de la memoria flash mediante el comando **show flash**:

```
R1# show flash
```

¿Cuántos archivos hay almacenados actualmente en la memoria flash?

¿Cuál de estos archivos cree que es la imagen de IOS?

¿Por qué cree que este archivo es la imagen de IOS?

Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

```
R1# copy startup-config flash
Destination filename [startup-config]
```

El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione **Entrar**; de lo contrario, escriba un nombre adecuado y presione la tecla **Entrar**.

b. Utilice el comando **show flash** para verificar que el archivo de configuración de inicio esté almacenado en la memoria flash.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Verificar la configuración predeterminada del router	Paso 2c	10	
	Paso 2d	2	
Total de la parte 1		**12**	
Parte 2: Configurar y verificar la configuración inicial del router	Paso 2a	2	
	Paso 2c	5	
	Paso 2d	6	
Total de la parte 2		**13**	
Parte 3: Guardar el archivo de configuración en ejecución	Paso 1a	5	
	Paso 2a (puntos extra)	5	
Total de la parte 3		**10**	
Puntuación de Packet Tracer		**80**	
Puntuación total (con los puntos extra)		**105**	

3.4.16.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.16.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.16.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.17 Práctica 17. Conexión de un router a una LAN

3.4.17.1 Objetivo

Parte 1: Mostrar la información del router

Parte 2: Configurar las interfaces del router

Parte 3: Verificar la configuración

3.4.17.2 Introducción

En esta actividad, utiliza diversos comandos show para mostrar el estado actual del router. Después utilizará la Tabla de direccionamiento para configurar las interfaces Ethernet del router. Finalmente, utilizará comandos para verificar y probar las configuraciones.

3.4.17.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

5.1 Memoria técnica

5.2 Análisis de necesidades y requerimientos.

3.4.17.4 Material Y Equipo Necesario

16. Equipo De Cómputo.
17. Conexión A Internet.
18. Packet Tracer

3.4.17.5 Metodología

Parte 1: Mostrar la información del router

Paso 1: Mostrar la información de la interfaz en el R1.

Nota: haga clic en un dispositivo y, a continuación, en la ficha **CLI** para acceder a la línea de comandos directamente. La contraseña de consola es **cisco**. La contraseña de EXEC privilegiado es **class**.

a. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router?

b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0?

c. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

   1) ¿Cuál es la dirección IP configurada en el **R1**?

   2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0?

d. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:

   1) ¿Cuál es la dirección IP en el **R1**?

   2) ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0?

   3) ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0?

Paso 2: Mostrar una lista de resumen de las interfaces en el R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas?

b. Introduzca el comando en cada router y responda las siguientes preguntas:

   1) ¿Cuántas interfaces seriales hay en **R1** y **R2**?

   2) ¿Cuántas interfaces Ethernet hay en **R1** y **R2**?

   3) ¿Son iguales todas las interfaces Ethernet en el **R1**? Si no es así, explique las diferencias.

Paso 3: Mostrar la tabla de enrutamiento en el R1

a. ¿Qué comando muestra el contenido de la tabla de enrutamiento?

b. Introduzca el comando en el **R1** y responda las siguientes preguntas:

   1) ¿Cuántas rutas conectadas hay (utilizan el código C)?

   2) ¿Qué ruta se indica?

3) ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento?

Parte 2: Configurar las interfaces del router

Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1

a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
```

b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.

```
R1(config-if)# description LAN connection to S1
```

c. Ahora, el **R1** debe poder hacer ping a la PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

a. Utilice la información en la Addressing Table para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:

1) Introduzca la dirección IP y active la interfaz.

2) Configure una descripción apropiada.

b. Verifique las configuraciones de las interfaces.

Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM

Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó?

Parte 3: Verificar la configuración

Paso 1: Utilizar los comandos de verificación para revisar la configuración de la interfaz

a. Utilice el comando **show ip interface brief** en **R1** y **R2** para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.

¿Cuántas interfaces en **R1** y **R2** están configuradas con direcciones IP y tienen el estado "up/up" (activa/activa)?

¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando?

¿Qué comandos puede utilizar para verificar esta parte de la configuración?

b. Utilice el comando **show ip route** en **R1** y **R2** para ver las tablas de enrutamiento actuales y responda las siguientes preguntas:

1) ¿Cuántas rutas conectadas (utilizan el código **C**) ve en cada router?
2) ¿Cuántas rutas EIGRP (utilizan el código **D**) ve en cada router?
3) Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y de rutas descubiertas dinámicamente (EIGRP) debe ser igual a la cantidad total de LAN y WAN. ¿Cuántas LAN y WAN hay en la topología?
4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento?

Nota: si su respuesta es "no", falta una configuración necesaria. Revise los pasos de la parte 2.

Paso 2: Probar la conectividad de extremo a extremo a través de la red

Ahora debería poder hacer ping desde cualquier PC a cualquier otra PC en la red. Además, debería poder hacer ping a las interfaces activas de los routers. Por ejemplo, las siguientes pruebas deberían realizarse correctamente:

- Desde la línea de comandos en la PC1, haga ping a la PC4.
- Desde la línea de comandos en el R2, haga ping a la PC2.

Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Mostrar la información del router	Paso 1a	2	
	Paso 1b	2	
	Paso 1c	4	
	Paso 1d	6	
	Paso 2a	2	
	Paso 2b	6	
	Paso 3a	2	
	Paso 3b	6	
Total de la parte 1		**30**	
Paso 2: Configurar las interfaces del router	Paso 3	2	
Total de la parte 2		**2**	
Paso 3: Verificar la configuración	Paso 1a	6	
	Paso 1b	8	
Total de la parte 3		**14**	
Puntuación de Packet Tracer		**54**	
Puntuación total (con los puntos extra)		**100**	

3.4.17.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.17.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.17.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.18 Práctica 18. Armado de una red de switch y router

3.4.18.1 Objetivo

Parte 1: Establecer la topología e inicializar los dispositivos

Parte 2: Configurar dispositivos y verificar la conectividad

Parte 3: Mostrar información del dispositivo

3.4.18.2 Introducción

Esta es una práctica de laboratorio exhaustiva para repasar los comandos del IOS que se abarcaron anteriormente. En este practica de laboratorio, conectará el equipo tal como se muestra en el diagrama de topología. Luego, configurará los dispositivos según la tabla de direccionamiento. Cuando se haya guardado la configuración, la verificará probando la conectividad de red.

Una vez que los dispositivos estén configurados y que se haya verificado la conectividad de red, utilizará los comandos del IOS para recuperar la información de los dispositivos y responder preguntas sobre los equipos de red.

En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos reales necesarios para configurar el router. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento intentando configurar los dispositivos sin consultar el apéndice.

3.4.18.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.18.4 Material Y Equipo Necesario

19. Equipo De Cómputo.
20. Conexión A Internet.

21. Packet Tracer

3.4.18.5 Metodología

Parte 1: Establecer la topología e inicializar los dispositivos

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

a. Conecte los dispositivos que se muestran en el diagrama de topología y tienda el cableado, según sea necesario.

b. Encienda todos los dispositivos de la topología.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos. Para obtener información sobre cómo inicializar y volver a cargar estos dispositivos, consulte el apéndice B.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará la topología de la red y los parámetros básicos, como direcciones IP de la interfaz, el acceso a dispositivos y contraseñas. ConsulteTopology yAddressing Table al principio de esta práctica de laboratorio para obtener información sobre nombres de dispositivos y direcciones.

Nota: en el apéndice A, se proporcionan detalles de configuración para los pasos de la parte 2. Antes de consultar el apéndice, intente completar la parte 2.

Paso 1: Asignar información de IP estática a las interfaces de la PC.

a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.

b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.

c. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.

¿Por qué los pings no fueron correctos?

Paso 2: Configurar el router.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Asigne un nombre de dispositivo al router.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

f. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

g. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

j. Configure y active las dos interfaces en el router.

k. Configure una descripción de interfaz para cada interfaz e indique qué dispositivo está conectado.

l. Guarde la configuración en ejecución en el archivo de configuración de inicio.

m. Configure el reloj en el router.

Nota: utilice el signo de interrogación (**?**) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar este comando.

n. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.

¿Tuvieron éxito los pings? ¿Por qué?

Parte 3: Mostrar información del dispositivo

En la parte 3, utilizará los comandos **show** para recuperar información del router y el switch.

Paso 1: Recuperar información del hardware y del software de los dispositivos de red.

a. Utilice el comando **show version** para responder las siguientes preguntas sobre el router.

¿Cuál es el nombre de la imagen del IOS que el router está ejecutando?

¿Cuánta memoria DRAM tiene el router?

¿Cuánta memoria NVRAM tiene el router?

¿Cuánta memoria flash tiene el router?

b. Utilice el comando **show version** para responder las siguientes preguntas sobre el switch.

¿Cuál es el nombre de la imagen del IOS que el switch está ejecutando?

¿Cuánta memoria de acceso aleatorio dinámica (DRAM) tiene el switch?

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el switch?

¿Cuál es el número de modelo del switch?

Paso 2: Mostrar la tabla de enrutamiento en el router

Utilice el comando **show ip route** en el router para responder las preguntas siguientes.

¿Qué código se utiliza en la tabla de enrutamiento para indicar una red conectada directamente? _____

¿Cuántas entradas de ruta están codificadas con un código C en la tabla de enrutamiento? _____

¿Qué tipos de interfaces están asociadas a las rutas con código C?

Paso 3: Mostrar información de la interfaz en el router.

Utilice el comando **show interface g0/1** para responder las preguntas siguientes.

¿Cuál es el estado operativo de la interfaz G0/1?

¿Cuál es la dirección de control de acceso al medio (MAC) de la interfaz G0/1?

¿Cómo se muestra la dirección de Internet en este comando?

Paso 4: Mostrar una lista de resumen de las interfaces del router y del switch.

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. Uno de los más útiles es el comando **show ip interface brief**. El resultado del comando muestra una lista resumida de las interfaces en el dispositivo e informa de inmediato el estado de cada interfaz.

a. Introduzca el comando **show ip interface brief** en el router.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         192.168.0.1     YES manual up                    up
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
R1#
```

b. Introduzca el comando **show ip interface brief** en el switch.

```
Switch# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Switch#
```

Reflexión

1. Si la interfaz G0/1 se mostrara administrativamente inactiva, ¿qué comando de configuración de interfaz usaría para activar la interfaz?

2. ¿Qué ocurriría si hubiera configurado incorrectamente la interfaz G0/1 en el router con una dirección IP 192.168.1.2?

Tabla de resumen de interfaces del router

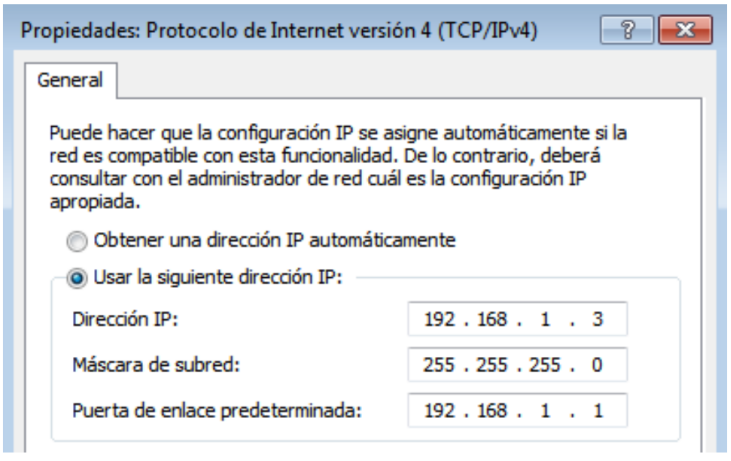
Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet #2**	**Interfaz serial #1**	**Interfaz serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

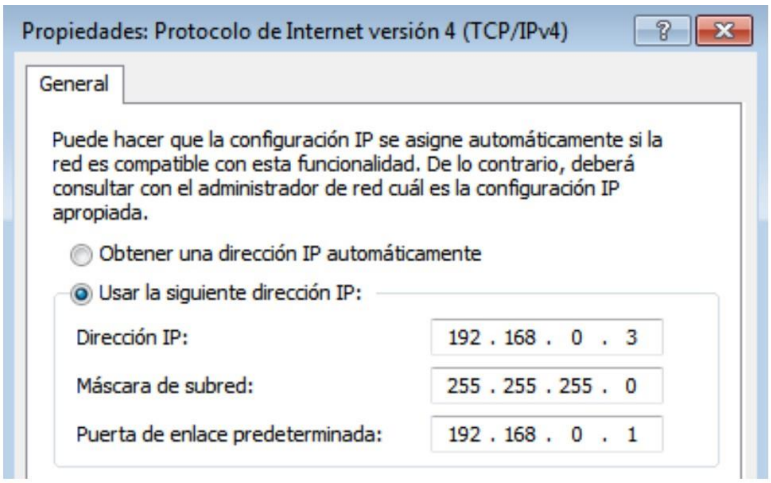
Apéndice A: Detalles de configuración para los pasos de la parte 2

Paso 1: Configure las interfaces de la PC.

a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.



b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.



c. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>
```

Paso 2: Configurar el router.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
Router#
```

b. Entre al modo de configuración.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

c. Asigne un nombre de dispositivo al router.

```
Router(config)# hostname R1
```

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

```
R1(config)# no ip domain-lookup
```

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

```
R1(config)# enable secret class
```

f. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

```
R1(config-line)# exit
R1(config)#
```

g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

h. Encripte las contraseñas de texto no cifrado.

```
R1(config)# service password-encryption
```

i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd #
Enter TEXT message.  End with the character '#'.
  Unauthorized access prohibited!
#
R1(config)#
```

j. Configure y active las dos interfaces en el router.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B.
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)#
*Nov 29 23:49:44.195: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
down
*Nov 29 23:49:47.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
up
*Nov 29 23:49:48.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1.
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# exit
*Nov 29 23:50:15.283: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
*Nov 29 23:50:18.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Nov 29 23:50:19.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1#
```

k. Guarde la configuración en ejecución en el archivo de inicio.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
```

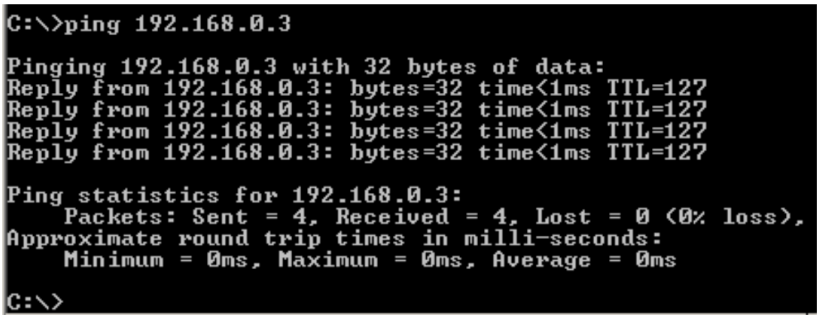
```
Building configuration...
[OK]
R1#
```

l. Configure el reloj en el router.

```
R1# clock set 17:00:00 29 Nov 2012
R1#
*Nov 29 17:00:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:55:46
UTC Thu Nov 29 2012 to 17:00:00 UTC Thu Nov 29 2012, configured from console by
console.
R1#
```

Nota: utilice el signo de interrogación (**?**) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar este comando.

m. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.



Apéndice B: Inicialización y recarga de un router y un switch

Parte 1: Inicializar el router y volver a cargar

Paso 1: Conéctese al router.

Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando **enable**.

```
Router> enable
Router#
```

Paso 2: Elimine el archivo de configuración de inicio de la NVRAM.

Escriba el comando **erase startup-config** para eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM, non-volatile random-access memory).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Paso 3: Recargue el router.

Emita el comando **reload** para eliminar una antigua configuración de la memoria. Cuando reciba el mensaje Proceed with reload (Continuar con la recarga), presione Entrar para confirmar la recarga. Si se presiona cualquier otra tecla, se anula la recarga.

```
Router# reload
Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 4: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Paso 5: Finalice el programa de instalación automática.

Se le solicitará que finalice el programa de instalación automática. Responda **yes** (sí) y, luego, presione Entrar.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Parte 2: Inicializar el switch y volver a cargar

Paso 1: Conéctese al switch.

Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Paso 2: Determine si se crearon redes de área local virtuales (VLAN, Virtual Local-Area Networks).

Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Paso 3: Elimine el archivo VLAN.

a. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Entrar si introdujo el nombre de manera correcta.

b. Cuando se le pregunte sobre la eliminación de este archivo, presione Entrar para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Paso 4: Borre el archivo de configuración de inicio.

Utilice el comando **erase startup-config** para borrar el archivo de configuración de inicio de la NVRAM. Cuando se le pregunte sobre la eliminación del archivo de configuración, presione Entrar para confirmar el borrado. (Si se presiona cualquier otra tecla, se anula la operación).

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Paso 5: Recargar el switch.

Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Cuando se le pregunte sobre la recarga del switch, presione Entrar para continuar con la recarga. (Si se presiona cualquier otra tecla, se anula la recarga).

```
Switch# reload
Proceed with reload? [confirm]
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 6: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Escriba **no** en la petición de entrada y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

3.4.18.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.18.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.18.8 Bibliografías

Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.19 Práctica 19. Comunicaciones TCP y UDP

3.4.19.1 Objetivo

Parte 1: Generar tráfico de red en modo de simulación

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

3.4.19.2 Introducción

El objetivo de esta actividad de simulación es proporcionar una base para comprender en detalle los protocolos TCP y UDP. El modo de simulación permite ver la funcionalidad de los diferentes protocolos.

A medida que los datos se trasladan por la red, se dividen en parte más pequeñas y se identifican de forma tal que se puedan volver a juntar. A cada de una de estas partes de le asigna un nombre especifico (Unidad de datos del protocolo [PDU, protocolo data unit]) y se le asocia a una capa especifica. El modo de simulación de Packet Tracer le permite al usuario ver cada uno de los protocolos y las PDU asociadas. Los pasos que se detallan a continuación guían al usuario en el proceso de solicitud de servicios mediante diversas aplicaciones disponibles en una PC cliente.

Esta actividad proporciona la oportunidad de explorar la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función que cumplen los números de puerto para determinar que aplicación local solicita o envía los datos.

3.4.19.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

5.1 Memoria técnica

5.2 Análisis de necesidades y requerimientos.

3.4.19.4 Material Y Equipo Necesario

22. Equipo De Cómputo.
23. Conexión A Internet.
24. Packet Tracer

3.4.19.5 Metodología

Parte 1: Generar tráfico de red en modo de simulación

Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

Para reducir la cantidad de tráfico de red que se ve en la simulación, realice lo siguiente:

a. Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ping 192.168.1.255**. Esto toma unos segundos, ya que todos los dispositivos en la red responden a **MultiServer**.

c. Cierre la ventana de **MultiServer**.

Paso 2: Genere tráfico web (HTTP).

a. Cambie a modo de simulación.

b. Haga clic en **HTTP Client** (Cliente HTTP) y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Explorador Web).

c. En el campo de dirección URL, introduzca **192.168.1.254** y haga clic en **Go** (Ir). En la ventana de simulación, aparecerán sobres (PDU).

d. Minimice (pero no cierre) la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP

a. Haga clic en **FTP Client** (Cliente FTP) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

b. Introduzca el comando **ftp 192.168.1.254**. En la ventana de simulación, aparecerán PDU.

c. Minimice (pero no cierre) la ventana de configuración de **FTP Client**.

Paso 4: Generar tráfico DNS

a. Haga clic en **DNS Client** (Cliente DNS) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

b. Introduzca el comando **nslookup multiserver.pt.ptu**. En la ventana de simulación, aparecerá una PDU.

c. Minimice (pero no cierre) la ventana de configuración de **DNS Client**.

Paso 5: Generar tráfico de correo electrónico

a. Haga clic en **E-Mail Client** (Cliente de correo electrónico) y, a continuación, haga clic en la ficha **Desktop** y seleccione la herramienta **E Mail** (Correo electrónico).

b. Haga clic en **Compose** (Redactar) e introduzca la siguiente información:

1) **To:** (Para:) usuario@multiserver.pt.ptu.

2) **Subject:** (Asunto:) personalice el campo de asunto.

3) **E-Mail Body:** (Cuerpo del correo electrónico:) personalice el correo electrónico.

c. Haga clic en **Send** (Enviar).

d. Minimice (pero no cierre) la ventana de configuración de **E-Mail Client**.

Paso 6: Verifique que se haya generado tráfico y que esté preparado para la simulación.

Cada equipo cliente debe tener PDU enumeradas en el panel de simulación.

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Paso 1: Examinar la multiplexación a medida que el tráfico cruza la red

Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

a. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.

b. Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?

c. Haga clic en **Capture/Forward** seis veces. Todos los clientes deberían haber recibido una respuesta. Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado.

¿Cómo se denomina este proceso?

d. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?

e. Haga clic en **Back** ocho veces. Esto restablecerá la simulación.

NOTA: no haga clic en **Reset Simulation** (Restablecer simulación) en ningún momento durante esta actividad; si lo hace, deberá repetir los pasos de la parte 1.

Paso 2: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor

a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**:

   1) Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrar todos/ninguno).

   2) Seleccione **HTTP** y **TCP**. Haga clic en cualquier lugar fuera del cuadro Edit Filters (Editar filtros) para ocultarlo. En Visible Events (Eventos visibles), ahora solo se deberían mostrar las PDU de **HTTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en **HTTP Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

   ¿Estas comunicaciones se consideran confiables?

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **HTTP Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

g. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación HTTP. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).

h. ¿Qué información se indica ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?

i. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 3: Examine el tráfico FTP cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **FTP Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

¿Estas comunicaciones se consideran confiables?

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

h. Cierre la PDU y haga clic en **Capture/Forward** hasta que una segunda PDU vuelva a **FTP Client**. La PDU es de un color diferente.

i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?

j. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 4: Examine el tráfico DNS cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS** y **UDP**.

b. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

¿Estas comunicaciones se consideran confiables?

d. Registre los valores de **SRC PORT** (Puerto de origen) y **DEST PORT** (Puerto de destino). ¿Por qué no hay números de secuencia ni de acuse de recibo?

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

g. ¿Cómo se llama la última sección de la **PDU**?

h. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 5: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **E-mail Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico?

¿Estas comunicaciones se consideran confiables?

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva a **E-Mail Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

h. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).

i. ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos **PDU** anteriores?

j. ¿Qué protocolo de correo electrónico se relaciona con el puerto TCP 25? ¿Qué protocolo se relaciona con el puerto TCP 110?

k. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 6: Examinar el uso de números de puerto del servidor

a. Para ver las sesiones TCP activas, siga estos pasos en una secuencia rápida:

   1) Pase nuevamente al modo **Realtime** (Tiempo real).

   2) Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **netstat**. ¿Qué protocolos se indican en la columna izquierda?

   ¿Qué números de puerto utiliza el servidor?

c. ¿En qué estados están las sesiones?

d. Repita el comando **netstat** varias veces hasta que vea solo una sola sesión con el estado ESTABLISHED. ¿Para qué servicio aún está abierta la conexión?

   ¿Por qué esta sesión no se cierra como las otras tres? (Sugerencia: revise los clientes minimizados)

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP	Paso 1	15	
	Paso 2	15	
	Paso 3	15	
	Paso 4	15	
	Paso 5	15	
	Paso 6	25	
Puntuación total		**100**	

3.4.19.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.19.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.19.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.20 Práctica 20 Uso de la calculadora de Windows con direcciones de red

3.4.20.1 Objetivo

Parte 1: Acceder a la calculadora de Windows.

Parte 2: Convertir entre sistemas de numeración.

Parte 3: Convertir direcciones de host y máscaras de subred IPv4 al sistema binario.

Parte 4: Determinar la cantidad de hots en una red mediante potencias de 2.

Parte 5: Convertir direcciones MAC y direcciones IPv6 al sistema binario.

3.4.20.2 Introducción

Los técnicos de red usan números binarios, decimales y hexadecimales cuando trabajan con PC y dispositivos de red. Microsoft proporciona la aplicación Calculadora incorporada como parte del sistema operativo. La versión de Windows 7 de la calculadora incluye una vista estándar que se puede utilizar para realizar tareas básicas de aritmética, como suma, resta, multiplicación y división. La aplicación Calculadora también tiene capacidades avanzadas de programación, calculadora científica y estadística.

En esta práctica de laboratorio, utilizara la vista Programador de la aplicación Calculadora de Windows 7 para la conversión entre sistemas numéricos binarios, decimales y hexadecimales. También usara la función de potencia de la vista Científica para determinar la cantidad de hosts que se pueden asignar según la cantidad de bits disponibles.

3.4.20.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.20.4 Material Y Equipo Necesario

25. Equipo De Cómputo.
26. Conexión A Internet.
27. Packet Tracer

3.4.20.5 Metodología

Parte 1: Acceder a la calculadora de Windows.

En la parte 1, se familiarizará con la aplicación Calculadora incorporada de Microsoft Windows y verá los modos disponibles.

Paso 1: Haga clic en el botón Inicio de Windows y seleccione Todos los programas.

Paso 2: Haga clic en la carpeta Accesorios y seleccione Calculadora.

Paso 3: Una vez que se abra la calculadora, haga clic en el menú Ver.

¿Cuáles son los cuatro modos disponibles?

Nota: en esta práctica de laboratorio, se utilizan los modos Programador y Científica.

Parte 2: Convertir entre sistemas de numeración

En la vista Programador de la calculadora de Windows, se encuentran disponibles varios modos de sistemas de numeración: Hex (hexadecimal o de base 16), Dec (decimal o de base 10), Oct (octal o de base 8) y Bin (binario o de base 2).

Estamos acostumbrados a usar el sistema de numeración decimal que emplea los dígitos del 0 al 9. El sistema de numeración decimal se utiliza en la vida diaria para todas las transacciones contables, de dinero y financieras. Las PC y otros dispositivos electrónicos utilizan el sistema de numeración binario con los dígitos 0 y 1 únicamente para el almacenamiento de datos, la transmisión de datos y los cálculos numéricos. Todos los cálculos de las PC se realizan, en última instancia, internamente en forma binaria (digital), independientemente de cómo aparecen.

Una desventaja de los números binarios es que el equivalente en números binarios de un número decimal grande puede ser muy largo. Esto dificulta su lectura y escritura. Una manera de solucionar este problema es ordenar los números binarios en grupos de cuatro, como números hexadecimales. Los números hexadecimales son de base 16, y se usa una combinación de números del 0 al 9 y de letras de la A a la F para representar el equivalente binario o decimal. Los caracteres hexadecimales se utilizan cuando se escriben o se muestran direcciones IPv6 y MAC.

El sistema de numeración octal es muy similar en principio al hexadecimal. Los números octales representan números binarios en grupos de tres. Este sistema de numeración utiliza los dígitos del 0 al 7. Usar números octales también es una manera práctica de representar un número binario grande en grupos más pequeños, pero este sistema de numeración no es muy común.

En esta práctica de laboratorio, se utiliza la calculadora de Windows 7 para realizar conversiones entre distintos sistemas de numeración en el modo Programador.

a. Haga clic en el menú **Ver** y seleccione **Programador** para cambiar al modo de programador.

Nota: en Windows XP y Windows Vista, solo hay dos modos disponibles: Estándar y Científica. Si utiliza uno de estos sistemas operativos, puede utilizar el modo Científica para realizar esta práctica de laboratorio.

¿Qué sistema numérico está activo?

¿Qué números del teclado numérico están activos en el modo decimal?

b. Haga clic en el botón de opción **Bin** (Binario). ¿Qué números están activos ahora en el teclado numérico?

¿Por qué considera que los otros números se muestran en color gris?

c. Haga clic en el botón de opción **Hex** (Hexadecimal). ¿Qué caracteres están activos ahora en el teclado numérico?

d. Haga clic en el botón de opción **Dec** (Decimal) Con el mouse, haga clic en el número **1** y luego en el número **5** del teclado numérico. Se introdujo el número decimal 15.

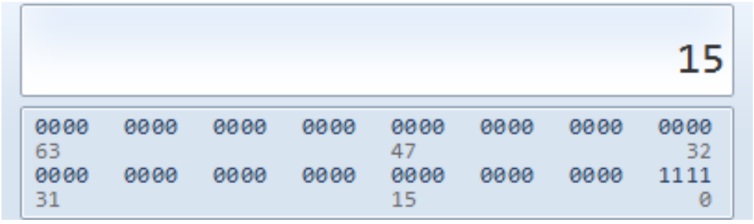
Nota: también se pueden usar los números y las letras del teclado para introducir los valores. Si utiliza el teclado numérico, escriba el número **15**. Si el número no se introduce en la calculadora, presione la tecla **Bloq Num** para habilitar el teclado numérico.

Haga clic en el botón de opción **Bin** (Binario). ¿Qué sucedió con el número 15?

e. Los números se convierten de un sistema de numeración a otro al seleccionar el modo de numeración deseado. Vuelva a hacer clic en el botón de opción **Dec**. El número vuelve a convertirse a decimal.

f. Haga clic en el botón de opción **Hex** para cambiar al modo hexadecimal. ¿Qué carácter hexadecimal (del 0 al 9 o de la A a la F) representa el 15 decimal?

g. Al cambiar entre los sistemas de numeración, es posible que haya observado que el número binario 1111 se mostraba durante la conversión. Esto lo ayuda a relacionar los dígitos binarios con otros valores del sistema de numeración. Cada conjunto de 4 bits representa un carácter hexadecimal o varios caracteres decimales potencialmente.



h. Haga clic en la **C** que está encima del número 9 en el teclado de la calculadora para borrar los valores de la ventana. Convierta los siguientes números entre los sistemas de numeración binario, decimal y hexadecimal.

Decimal	Binario	Hexadecimal
86		
175		
204		
	0001 0011	
	0100 1101	
	0010 1010	
		38
		93
		E4

i. A medida que registra los valores en la tabla anterior, ¿observa un patrón entre los números binarios y hexadecimales?

Parte 3: Convertir direcciones de host y máscaras de subred IPv4 al sistema binario

Las direcciones del protocolo de Internet versión 4 (IPv4) y las máscaras de subred se representan en un formato decimal punteado (cuatro octetos), por ejemplo, 192.168.1.10 y 255.255.255.0, respectivamente. Esto permite que estas direcciones sean más fáciles de leer para los usuarios. Cada uno de los octetos decimales de la dirección o de una máscara se puede convertir en 8 bits binarios. Un octeto equivale siempre a 8 bits binarios. Si los 4 octetos se convirtieran al sistema binario, ¿cuántos bits habría?

a. Utilice la aplicación Calculadora de Windows para convertir la dirección IP 192.168.1.10 a número binario y registre los números binarios en la tabla siguiente:

Decimal	Binario
192	
168	
1	
10	

b. Las máscaras de subred, como 255.255.255.0, también están representadas en formato decimal punteado. Una máscara de subred siempre consta de cuatro octetos de 8 bits, cada uno representado como un número decimal. Con la calculadora de Windows, convierta los 8 valores posibles de octetos de la máscara de subred decimal a números binarios y registre dichos números en la tabla siguiente:

Decimal	Binario
0	
128	
192	
224	
240	
248	
252	
254	
255	

c. Con la combinación de la dirección IPv4 y la máscara de subred, se puede determinar la porción de red y también se puede calcular la cantidad de hosts disponibles en una subred IPv4 determinada. El proceso se examina en la parte 4.

Parte 4: Determinar la cantidad de hosts en una red mediante potencias de 2

Dada una dirección de red IPv4 y una máscara de subred, se puede determinar la porción de red junto con la cantidad de hosts disponibles en la red.

a. Para calcular la cantidad de hosts en una red, debe determinar la porción de red y de host de la dirección.

Si se aplica el ejemplo de 192.168.1.10 con una subred 255.255.248.0, la dirección y la máscara de subred se convierten a números binarios. Alinee los bits a medida que registra las conversiones a números binarios.

Dirección IP y máscara de subred decimales	Dirección IP y máscara de subred binarias
192.168.1.10	
255.255.248.0	

Dado que los primeros 21 bits en la máscara de subred son números 1 consecutivos, los primeros 21 bits correspondientes en la dirección IP en sistema binario son 11000000101010000000, que representan la porción de red de la dirección. Los 11 bits restantes son 00100001010 y representan la porción de host de la dirección.

¿Cuál es el número de red decimal y binario para esta dirección?

¿Cuál es la porción de host decimal y binaria para esta dirección?

Dado que el número de red y la dirección de broadcast utilizan dos direcciones fuera de la subred, la fórmula para determinar la cantidad de hosts disponibles en una subred IPv4 es el número 2 elevado a la cantidad de bits de hosts disponibles, menos 2:

$$\text{Cantidad de hosts disponibles} = 2^{(\text{cantidad de bits de hosts})} - 2$$

b. Con la aplicación Calculadora de Windows, cambie al modo Científica; para eso, haga clic en el menú **Ver** y, a continuación, seleccione **Científica**.

c. Introduzca **2.** Haga clic en la tecla $\mathbf{x^y}$. Esta tecla eleva un número a una potencia.

d. Introduzca **11.** Haga clic en **=** o presione Entrar en el teclado para obtener la respuesta.

e. Utilice la calculadora, si lo desea, para restar **2** a la respuesta.

f. En este ejemplo, hay 2046 hosts disponibles en esta red (2^{11} -2).

g. Dada la cantidad de bits de hosts, determine la cantidad de hosts disponibles y registre el número en la tabla siguiente.

Cantidad de bits de host disponibles	Cantidad de hosts disponibles
5	
14	
24	
10	

h. Para una máscara de subred dada, determine la cantidad de hosts disponibles y registre la respuesta en la tabla siguiente.

Máscara de subred	Máscara de subred binaria	Cantidad de bits de host disponibles	Cantidad de hosts disponibles
255.255.255.0	11111111.11111111.11111111.00000000		
255.255.240.0	11111111.11111111.11110000.00000000		
255.255.255.128	11111111.11111111.11111111.10000000		
255.255.255.252	11111111.11111111.11111111.11111100		
255.255.0.0	11111111.11111111.00000000.00000000		

Parte 5: Convertir direcciones MAC y direcciones IPv6 al sistema binario

Tanto las direcciones de control de acceso al medio (MAC) y del protocolo de Internet versión 6 (IPv6) se representan como dígitos hexadecimales para facilitar la lectura. Sin embargo, las PC solo comprenden los dígitos binarios y los utilizan para los cálculos. En esta parte, convertirá estas direcciones hexadecimales a direcciones binarias.

Paso 1: Convertir direcciones MAC a dígitos binarios

a. La dirección MAC o física normalmente se representa como 12 caracteres hexadecimales, agrupados en pares y separados por guiones (-). Las direcciones físicas en un equipo Windows se muestran en un formato xx-xx-xx-xx-xx-xx, donde cada x es un número del 0 al 9 o una letra de la A a la F. Cada uno de los caracteres hexadecimales en la dirección puede convertirse en 4 bits binarios, que es lo que la PC comprende. Si los 12 caracteres hexadecimales se convirtieran al sistema binario, ¿cuántos bits habría?

b. Registre la dirección MAC de la PC.

c. Convierta la dirección MAC a dígitos binarios mediante la aplicación Calculadora de Windows.

Paso 2: Convertir una dirección IPv6 a dígitos binarios

Las direcciones IPv6 también se escriben en caracteres hexadecimales por cuestiones de practicidad. Estas direcciones IPv6 pueden convertirse a números binarios para el uso de la PC.

a. Las direcciones IPv6 son números binarios representados en notaciones legibles para los usuarios: 2001:0DB8:ACAD:0001:0000:0000:0000:0001 o en un formato más corto: 2001:DB8:ACAD:1::1.

b. Las direcciones IPv6 tienen una longitud de 128 bits. Utilice la aplicación Calculadora de Windows para convertir la dirección IPv6 del ejemplo a números binarios y regístrela en la tabla siguiente.

Hexadecimal	Binario
2001	
0DB8	
ACAD	
0001	
0000	
0000	
0000	
0001	

Reflexión

1. ¿Puede realizar todas las conversiones sin la ayuda de la calculadora? ¿Qué puede hacer para lograrlo?

2. Para la mayoría de las direcciones IPv6, la porción de red de la dirección suele ser de 64 bits. ¿Cuántos hosts están disponibles en una subred donde los primeros 64 bits representan la red? Sugerencia: todas las direcciones host están disponibles en la subred para los hosts.

3.4.20.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.20.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.20.8 Bibliografías

Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.21 Práctica 21. Conversión de direcciones IPv4 al sistema binario

3.4.21.1 Objetivo

Parte 1: Convertir direcciones IPv4 de formato decimal punteado a binario.

Parte 2: Utilizar la operación AND bit a bit para determinar las direcciones de red.

Parte 3: Aplicar los cálculos de direcciones de red.

3.4.21.2 Introducción

Cada dirección IPv4 consta de dos partes: una porción de red y una porción de host. La porción de red de una dirección es la misma para todos los dispositivos que residen en la misma red. La porción de host identifica un host especifico dentro de una red determinada. La máscara de subred se utiliza para determinar la porción de red de una dirección IP. Los dispositivos en la misma red pueden comunicarse directamente; los dispositivos en redes diferentes requieren un dispositivo intermediario de capa 3, como un router, para comunicarse.

Para comprender el funcionamiento de los dispositivos en una red, debemos ver las direcciones de la manera en que lo hacen los dispositivos; en notación binaria. Para ello, debemos convertir el formato decimal punteado de una dirección IP y la máscara de subred a notación binaria. Después de hacerlo, podremos usar la operación AND bit a bit para determinar la dirección de red.

En esta práctica de laboratorio, se proporcionan instrucciones acerca de cómo determinar la porción de red y la porción de host de direcciones IP convirtiendo las direcciones y las máscaras de subred de la forma decimal punteada a la forma binaria y luego utilizando la operación AND bit a bit. Luego aplicará esta información para identificar las direcciones en la red.

3.4.21.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.21.4 Material Y Equipo Necesario

28. Equipo De Cómputo.
29. Conexión A Internet.
30. Packet Tracer

3.4.21.5 Metodología

Parte 1: Convertir direcciones IPv4 de formato decimal punteado a binaria

En la parte 1, convertirá números decimales a su equivalente binario. Después de dominar esta actividad, convertirá direcciones IPv4 y máscaras de subred del formato decimal punteado al formato binario.

Paso 1: Convertir números decimales a su equivalente binario

Complete la tabla siguiente convirtiendo el número decimal a un número binario de 8 bits. El primer número se completó a modo de referencia. Recuerde que los ocho valores de bits binarios en un octeto están basados en las potencias de 2 y, de izquierda a derecha, son 128, 64, 32, 16, 8, 4, 2 y 1.

Decimal	Binario
192	11000000
168	
10	
255	
2	

Paso 2: Convertir las direcciones IPv4 a su equivalente binario

Una dirección IPv4 se puede convertir utilizando la misma técnica que se usó anteriormente. Complete la tabla siguiente con el equivalente binario de las direcciones proporcionadas. Para que las respuestas sean más fáciles de leer, separe los octetos binarios con un punto.

Decimal	Binario
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	
172.16.18.183	
10.86.252.17	
255.255.255.128	
255.255.192.0	

Parte 2: Utilizar la operación AND bit a bit para determinar las direcciones de red

En la parte 2, utilizará la operación AND bit a bit para calcular la dirección de red para las direcciones de host proporcionadas. Primero, deberá convertir una dirección decimal IPv4 y una máscara de subred a su equivalente binario. Una vez que tenga la forma binaria de la dirección de red, conviértala a su forma decimal.

Nota: el proceso de aplicación de AND compara el valor binario en cada posición de bit de la dirección IP del host de 32 bits con la posición correspondiente en la máscara de subred de 32 bits. Si hay dos 0 o un 0 y un 1, el resultado de la aplicación de AND es 0. Si hay dos 1, el resultado es un 1, como se muestra en el ejemplo siguiente.

Paso 1: Determinar la cantidad de bits que se utilizarán para calcular la dirección de red

Descripción	Decimal	Binario
Dirección IP	192.168.10.131	11000000.10101000.00001010.10000011
Máscara de subred	255.255.255.192	11111111.11111111.11111111.11000000
Dirección de red	192.168.10.128	11000000.10101000.00001010.10000000

¿Cómo se determina qué bits deben utilizarse para calcular la dirección de red?

.

En el ejemplo anterior, ¿cuántos bits se utilizan para calcular la dirección de red?

.

Paso 2: Utilizar la operación AND para determinar la dirección de red

a. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	172.16.145.29	
Máscara de subred	255.255.0.0	
Dirección de red		

b. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	192.168.10.10	
Máscara de subred	255.255.255.0	
Dirección de red		

c. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	192.168.68.210	
Máscara de subred	255.255.255.128	
Dirección de red		

d. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	172.16.188.15	
Máscara de subred	255.255.240.0	
Dirección de red		

e. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	10.172.2.8	
Máscara de subred	255.224.0.0	
Dirección de red		

Parte 3: Aplicar los cálculos de direcciones de red

En la parte 3, debe calcular la dirección de red para las direcciones IP y las máscaras de subred dadas. Una vez que tenga la dirección de red, debe poder determinar las respuestas para completar la práctica de laboratorio.

Paso 1: Determinar si las direcciones IP están en la misma red

a. Está configurando dos PC para su red. A la PC-A se le asigna la dirección IP 192.168.1.18 y a la PC-B se le asigna la dirección IP 192.168.1.33. Las dos PC reciben una máscara de subred 255.255.255.240.

¿Cuál es la dirección de red para la PC-A?

¿Cuál es la dirección de red para la PC-B?

¿Estas PC podrán comunicarse directamente entre sí?

¿Cuál es la dirección más alta que se puede asignar a la PC-B que le permita estar en la misma red que la PC-A?

b. Está configurando dos PC para su red. A la PC-A se le asigna la dirección IP 10.0.0.16 y a la PC-B se le asigna la dirección IP 10.1.14.68. Las dos PC reciben la máscara de subred 255.254.0.0

¿Cuál es la dirección de red para la PC-A?

¿Cuál es la dirección de red para la PC-B?

¿Estas PC podrán comunicarse directamente entre sí?

¿Cuál es la dirección más baja que se puede asignar a la PC-B que le permita estar en la misma red que la PC-A?

Paso 2: Identificar la dirección de gateway predeterminado

a. Su empresa tiene una política para utilizar la primera dirección IP de una red como la dirección de gateway predeterminado. Un host en la red de área local (LAN) tiene una dirección IP 172.16.140.24 y una máscara de subred 255.255.192.0.

¿Cuál es la dirección de red para esta red?

¿Cuál es la dirección de gateway predeterminado para este host?

b. Su empresa tiene una política para utilizar la primera dirección IP de una red como la dirección de gateway predeterminado. Se le indicó configurar un servidor nuevo con una dirección IP 192.168.184.227 y una máscara de subred 255.255.255.248.

¿Cuál es la dirección de red para esta red?

¿Cuál es el gateway predeterminado para este servidor?

Reflexión

¿Por qué la máscara de subred es importante para determinar la dirección de red?

3.4.21.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.21.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando

detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.21.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.22 Practica 22. Identificación de direcciones IPv4

3.4.22.1 Objetivo

Parte 1: Identificar las direcciones IPv4.

Parte 2: Clasificar direcciones IPv4.

3.4.22.2 Introducción

El direccionamiento es una función importante de los protocolos de la capa de red, porque permite la comunicación de datos entre hosts en la misma red o en redes diferentes. En esta práctica de laboratorio, examinará la estructura de las direcciones del protocolo de internet versión 4. Identificará a los diversos tipos de direcciones IPv4 y los componentes que ayudan a formar la dirección, la porción de red, la porción de host y la máscara de subred. Entre los tipos de direcciones que se abarcan, se incluyen los siguientes: pública, unicast y muticast.

3.4.22.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.1 Dispositivos de capa física y 3.2 Dispositivos de capa de enlace.

3.4.22.4 Material Y Equipo Necesario

31. Equipo De Cómputo.
32. Conexión A Internet.
33. Packet Tracer

3.4.22.5 Metodología

Parte 1: Identificar direcciones IPv4

En la parte 1, se le proporcionarán varios ejemplos de direcciones IPv4, y deberá completar las tablas con la información apropiada.

Paso 1: Analizar la tabla que se muestra a continuación e identificar la porción de red y la porción de host de las direcciones IPv4 dadas

En las dos primeras filas, se muestran ejemplos de la forma en que debe completarse la tabla.

Referencias para la tabla:

N = los 8 bits de un octeto están en la porción de red de la dirección

n = un bit en la porción de red de la dirección

H = los 8 bits de un octeto están en la porción de host de la dirección

h = un bit en la porción de host de la dirección

Dirección/prefijo IP	Red/host N, n = red H, h = host	Máscara de subred	Dirección de red
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Paso 2: Analizar la tabla siguiente e indicar el rango de direcciones de host y de broadcast, dado un par de máscara de red y prefijo

En la primera fila, se muestra un ejemplo de cómo se debe completar.

Dirección/prefijo IP	Primera dirección de host	Última dirección de host	Dirección de broadcast
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Parte 2: Clasificar direcciones IPv4

En la parte 2, identificará y clasificará varios ejemplos de direcciones IPv4.

Paso 1: Analizar la tabla siguiente e identificar el tipo de dirección (dirección de red, de host, multicast o broadcast)

En la primera fila, se muestra un ejemplo de cómo se debe completar.

Dirección IP	Máscara de subred	Tipo de dirección
10.1.1.1	255.255.255.252	direcciones
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

Paso 2: Analizar la tabla siguiente e identificar la dirección como pública o privada

Dirección/prefijo IP	Pública o privada
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Paso 3: Analizar la tabla siguiente e identificar si el par dirección/prefijo es una dirección de host válida

Dirección/prefijo IP	¿La dirección de host es válida?	Motivo
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

Reflexión

¿Por qué debemos seguir estudiando y aprendiendo sobre el direccionamiento IPv4 si el espacio de direcciones IPv4 disponible está agotado?

3.4.22.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.22.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.22.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.23 Configuración de direccionamiento IPv6

3.4.23.1 Objetivo

Parte 1: Configurar el direccionamiento IPv6 en el router.

Parte 2: Configurar el direccionamiento IPv6 en los servidores.

Parte 3: Configurar el direccionamiento IPv6 en los clientes.

Parte 4: Probar y verificar la conectividad de red.

3.4.23.2 Introducción

En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación de las direcciones IPv6.

3.4.23.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares y 4.2 Componentes y herramientas de Instalación.

3.4.23.4 Material Y Equipo Necesario

34. Equipo De Cómputo.
35. Conexión A Internet.
36. Packet Tracer

3.4.23.5 Metodología

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

a. Introduzca el comando de configuración global ipv6 unicast-routing. Este comando se debe configurar para habilitar el router para que reenvíe paquetes IPv6. Este comando se analizará en otro semestre.

```
R1(config)# ipv6 unicast-routing
```

Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

a. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **Entrar**.

b. Ingrese al modo EXEC privilegiado.

c. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/0.

d. Configure la dirección IPv6 con el siguiente comando:

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

e. Configure la dirección IPv6 link-local con el siguiente comando:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

f. Active la interfaz.

Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/1.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.

c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Paso 4: Configurar el direccionamiento IPv6 en Serial0/0/0

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para Serial0/0/0.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.

c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Parte 2: Configurar el direccionamiento IPv6 en los servidores

Paso 1: Configurar el direccionamiento IPv6 en el servidor de contabilidad

a. Haga clic en **Accounting** (Contabilidad) y, a continuación, en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

b. Establezca la **dirección IPv6 2001:DB8:1:1::4** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

Paso 2: Configurar el direccionamiento IPv6 en el servidor CAD

Repita los pasos 1a a 1c para el servidor **CAD**. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Parte 3: Configurar el direccionamiento IPv6 en los clientes

Paso 1: Configurar el direccionamiento IPv6 en los clientes de ventas y facturación

a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:1::3** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

d. Repita los pasos 1a a 1c para **Sales** (Ventas). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:2::3** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

d. Repita los pasos 1a a 1c para **Design** (Diseño). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Parte 4: Probar y verificar la conectividad de la red

Paso 1: Abrir las páginas Web del servidor de los clientes

a. Haga clic en **Sales** y, a continuación, en la ficha **Desktop**. Si es necesario, cierre la ventana **IP Configuration**.

b. Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.

c. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.

d. Repita los pasos 1a a 1d para el resto de los clientes.

Paso 2: Hacer ping al ISP

a. Abra una ventana de configuración de cualquier equipo cliente haciendo clic en el ícono.

b. Haga clic en la ficha **Desktop** > **Command Prompt** (Símbolo del sistema).

c. Pruebe la conectividad al ISP con el siguiente comando:

```
PC> ping 2001:DB8:1:A001::1
```

d. Repita el comando **ping** con otros clientes hasta que se haya verificado la conectividad completa.

3.4.23.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.23.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.23.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.24 Práctica 24 Configuración inicial del router

3.4.24.1 Objetivo

Parte 1: Conectar la red.

Parte 2: Utilizar el comando ping para realizar pruebas de red básicas.

Parte 3: Utilizar los comandos tracert y traceroute para realizar pruebas de red básicas.

3.4.24.2 Introducción

Ping y traceroute son dos herramientas imprescindibles para probar la conectividad de red TCP/IP. Ping es una utilidad de administración de red que se utiliza para probar la posibilidad de conexión de un dispositivo en una red IP. Esta utilidad también mide el tiempo de ida y vuelta para los mensajes que se envían desde el host de origen hasta una PC de destino. La utilidad ping está disponible en Windows, en sistemas operativos (OS) del estilo de Unix y en el Sistema operativo Internetwork (IOS) de Cisco.

La utilidad de traceroute es una herramienta de diagnóstico de red para mostrar la ruta y medir las demoras en el tránsito de los paquetes que viajan por una red IP. La utilidad tracert está disponible en Windows y una utilidad similar, traceroute, está disponible en OS del estilo de Unix y en Cisco IOS.

3.4.24.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.24.4 Material Y Equipo Necesario

37. Equipo De Cómputo.
38. Conexión A Internet.
39. Packet Tracer

3.4.24.5 Metodología

Parte 1: Armar y configurar la red

En la parte 1, configurará la red en la topología y configurará las PC y los dispositivos Cisco. Como referencia, se proporcionan las configuraciones iniciales para los routers y switches. En esta topología, el EIGRP se utiliza para enrutar paquetes entre redes.

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

Paso 2: Borrar las configuraciones en los routers y switches, y volver a cargar los dispositivos

Paso 3: Configurar las direcciones IP de las PC y los gateways predeterminados según la tabla de direccionamiento

Paso 4: Configurar los routers LOCAL, ISP y REMOTE mediante las configuraciones iniciales que se detallan a continuación

En la petición de entrada del modo de configuración global del switch o el router, copie y pegue la configuración para cada dispositivo. Guarde la configuración en startup-config.

Configuraciones iniciales para el router LOCAL:

```
hostname LOCAL
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 56000
 no shutdown
interface g0/1
```

```
 ip add 192.168.1.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Configuraciones iniciales para el router ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface s0/0/1
 ip add 10.2.2.2 255.255.255.252
 clock rate 56000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 no auto-summary
end
```

Configuraciones iniciales para el router REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.3.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Paso 5: Configurar los switches S1 y S3 con las configuraciones iniciales

Configuraciones iniciales para el S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.11 255.255.255.0
 no shutdown
 exit
```

```
ip default-gateway 192.168.1.1
end
```

Configuraciones iniciales para el S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
 ip add 192.168.3.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.3.1
end
```

Paso 6: Configurar una tabla de hosts IP en el router LOCAL

La tabla de hosts IP le permite utilizar un nombre de host para conectarse a un dispositivo remoto en lugar de una dirección IP. La tabla de hosts proporciona la resolución de nombres para el dispositivo con las siguientes configuraciones. Copie y pegue las siguientes configuraciones para el router LOCAL. Estas configuraciones le permitirán usar los nombres de host para los comandos **ping** y **traceroute** en el router LOCAL.

```
ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end
```

Parte 2: Utilizar el comando ping para realizar pruebas de red básicas

En la parte 2 de esta práctica de laboratorio, utilice el comando **ping** para verificar la conectividad de extremo a extremo. Ping opera mediante el envío de paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al host de destino y la espera de una respuesta del ICMP. Puede registrar el tiempo de ida y vuelta y la pérdida de paquetes.

Inspeccionará los resultados con el comando **ping** y las opciones de ping adicionales que están disponibles en las PC con Windows y en los dispositivos Cisco.

Paso 1: Probar la conectividad de red desde la red LOCAL por medio de la PC-A

Todos los pings de la PC-A a otros dispositivos en la topología deben realizarse correctamente. De lo contrario, revise la topología y el cableado, así como la configuración de los dispositivos Cisco y las PC.

a. Haga ping de la PC-A al gateway predeterminado (la interfaz GigabitEthernet 0/1 del router LOCAL).

```
C:\Users\User1> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En este ejemplo, se enviaron cuatro (4) solicitudes de ICMP, de 32 bytes cada una, y las respuestas se recibieron en menos de un milisegundo sin pérdida de paquetes. El tiempo de transmisión y respuesta aumenta a medida que se procesan las solicitudes y respuestas de ICMP a través de más dispositivos en el trayecto hasta el destino final y desde este.

b. Desde la PC-A, haga ping a las direcciones que se indican en la tabla siguiente y registre el tiempo de ida y vuelta promedio y el tiempo de vida (TTL).

Destino	Tiempo promedio de ida y vuelta (ms)	TTL
192.168.1.1 (LOCAL)		
192.168.1.11 (S1)		
10.1.1.1 (LOCAL)		
10.1.1.2 (ISP)		
10.2.2.2 (ISP)		
10.2.2.1 (REMOTE)		
192.168.3.1 (REMOTE)		
192.168.3.11 (S3)		
192.168.3.3 (PC-C)		

Observe el viaje promedio de ida y vuelta para 192.168.3.3 (PC-C). El tiempo aumentó porque las solicitudes de ICMP fueron procesadas por tres routers antes de que la PC-A recibiera la respuesta de la PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Paso 2: Utilizar los comandos de ping extendido en una PC

El comando **ping** predeterminado envía cuatro solicitudes a 32 bytes cada una. Espera la devolución de cada respuesta 4000 milisegundos (cuatro segundos) y luego muestra el mensaje “Tiempo de espera agotado”. El comando **ping** se puede ajustar para resolver los problemas de una red.

a. En el símbolo del sistema, escriba **ping** y presione Entrar.

```
C:\Users\User1> ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

```
Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

b. Mediante la opción **–t**, haga ping a la PC-C para verificar que haya posibilidad de conexión con ella.

```
C:\Users\User1> ping -t 192.168.3.3
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

Para ilustrar los resultados cuando no hay posibilidad de conexión a un host, desconecte el cable entre el router REMOTE y el switch S3 o desactive la interfaz GigabitEthernet 0/1 en el router REMOTE.

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
```

Mientras la red funciona correctamente, el comando **ping** puede determinar si el destino respondió y cuánto tardó en recibir una respuesta del destino. Si existe un problema de conectividad de red, el comando **ping** muestra un mensaje de error.

c. Vuelva a conectar el cable Ethernet o habilite la interfaz GigabitEthernet en el router REMOTE (mediante el comando **no shutdown**) antes de continuar con el paso siguiente. Después de 30 segundos, el ping debe volver a ser correcto.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

d. Presione **Ctrl+C** para detener el comando ping.

Paso 3: Probar la conectividad de red desde la red LOCAL por medio de dispositivos Cisco

El comando **ping** también está disponible en los dispositivos Cisco. En este paso, el comando **ping** se examina por medio del router LOCAL y el switch S1.

a. Haga ping a la PC-C en la red REMOTE utilizando la dirección IP 192.168.3.3 desde el router LOCAL.

```
LOCAL# ping 192.168.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

El signo de exclamación (!) indica que el ping desde el router LOCAL hasta la PC-C se realizó correctamente. El tiempo promedio de ida y vuelta es de 64 ms sin pérdida de paquetes, según lo indica la tasa de éxito del 100%.

b. Dado que se configuró una tabla de hosts locales en el router LOCAL, puede hacer ping a la PC-C en la red REMOTE utilizando el nombre de host configurado desde el router LOCAL.

```
LOCAL# ping PC-C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

c. Hay más opciones disponibles para el comando **ping**. En la CLI, escriba **ping** y presione Entrar. Introduzca **192.168.3.3** o **PC-C** para Target IP address (Dirección IP de destino). Presione Entrar para aceptar el valor predeterminado para otras opciones.

```
LOCAL# ping
Protocol [ip]:
Target IP address: PC-C
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

d. Puede utilizar un ping extendido para tareas de observación cuando hay un problema de red. Inicie el comando **ping** a 192.168.3.3 con un conteo de repetición de 500. Luego, desconecte el cable entre el router REMOTE y el switch S3 o desactive la interfaz GigabitEthernet 0/1 en el router REMOTE.

Vuelva a conectar el cable Ethernet o habilite la interfaz GigabitEthernet en el router REMOTE después de reemplazar los signos de exclamación (!) por la letra U y puntos (.). Después de 30 segundos, el ping debe volver a ser correcto. Si lo desea, presione **Ctrl+Mayús+6** para detener el comando **ping**.

```
LOCAL# ping
Protocol [ip]:
Target IP address: 192.168.3.3
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

```
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!U.............
....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/63/72 ms
```

La letra U en los resultados indica que no hay posibilidad de conexión a un destino. El router LOCAL recibió una unidad de datos del protocolo (PDU) de error. Cada punto (.) en el resultado indica que el tiempo de espera del ping se agotó mientras se esperaba una respuesta de la PC-C. En este ejemplo, se perdió el 5% de los paquetes durante la interrupción de red simulada.

Nota: también puede utilizar el comando siguiente para obtener los mismos resultados:

```
LOCAL# ping 192.168.3.3 repeat 500
```

o

```
LOCAL# ping PC-C repeat 500
```

e. También puede probar la conectividad de red con un switch. En este ejemplo, el switch S1 hace ping al switch S3 en la red REMOTE.

```
S1# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/67/68 ms
```

El comando **ping** es extremadamente útil al resolver problemas en la conectividad de red. Sin embargo, no puede indicar la ubicación del problema cuando un ping no se realiza correctamente. El comando **tracert** (o **traceroute**) puede mostrar la latencia de red e información sobre la ruta.

Parte 3: Utilizar los comandos tracert y traceroute para realizar pruebas de red básicas

En las PC y los dispositivos de red, existen comandos para rastrear las rutas. En las PC con Windows, el comando **tracert** utiliza mensajes de ICMP para rastrear la ruta hacia el destino final. En dispositivos Cisco y PC del estilo de Unix, el comando **traceroute** utiliza los datagramas del protocolo de datagramas de usuario (UDP) para rastrear las rutas hacia el destino final.

En la parte 3, examinará los comandos traceroute y determinará la ruta de un paquete hasta el destino final. Utilizará el comando **tracert** en las PC con Windows y el comando **traceroute** en los dispositivos Cisco. También analizará las opciones disponibles para ajustar los resultados de traceroute.

Paso 1: Utilizar el comando tracert de la PC-A a la PC-C

a. En el símbolo del sistema, escriba **tracert 192.168.3.3**.

```
C:\Users\User1> tracert 192.168.3.3
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:
```

```
  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]

Trace complete.
```

Los resultados de tracert indican que la ruta de la PC-A a la PC-C va de la PC-A a LOCAL, a ISP, a REMOTE y a la PC-C. La ruta a la PC-C pasó por tres saltos de router hasta llegar el destino final en la PC-C.

Paso 2: Explorar opciones adicionales para el comando tracert

a. En el símbolo del sistema, escriba **tracert** y presione Entrar.

```
C:\Users\User1> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

b. Utilice la opción **-d**. Observe que la dirección IP 192.168.3.3 no se resolvió como PC-C.

```
C:\Users\User1> tracert -d 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    192.168.3.3

Trace complete.
```

Paso 3: Utilizar el comando traceroute del router LOCAL a la PC-C

a. En la petición de entrada de comandos del router local, escriba **traceroute 192.168.3.3** o **traceroute PC-C**. Los nombres de host se resuelven porque se configuró una tabla de hosts IP locales en el router LOCAL.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec
```

```
LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Paso 4: Utilizar el comando traceroute del switch S1 a la PC-C

a. En el switch S1, escriba **traceroute 192.168.3.3**. Los nombres de host no se muestran en los resultados del comando traceroute porque no se configuró una tabla de hosts IP locales en este switch.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 1007 msec 0 msec 0 msec
  2 10.1.1.2 17 msec 17 msec 16 msec
  3 10.2.2.1 34 msec 33 msec 26 msec
  4 192.168.3.3 33 msec 34 msec 33 msec
```

El comando **traceroute** tiene opciones adicionales. Puede utilizar **?** o simplemente presionar Entrar después de escribir **traceroute** en la petición de entrada para explorar estas opciones.

El enlace siguiente proporciona más información acerca de los comandos **ping** y **traceroute** para dispositivos Cisco:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Parte 4: Resolver problemas de la topología

Paso 1: Borrar las configuraciones en el router REMOTE

Paso 2: Volver a cargar el router REMOTE

Paso 3: Copiar y pegar la siguiente configuración en el router REMOTE

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.8.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Paso 4: Desde la red LOCAL, utilizar los comandos ping y tracert o traceroute para resolver y corregir problemas en la red REMOTE

a. Utilice los comandos **ping** y **tracert** desde la PC-A.

Puede utilizar el comando **tracert** para determinar la conectividad de red de extremo a extremo. Este resultado de tracert indica que la PC-A puede conectarse a su gateway predeterminado 192.168.1.1, pero no tiene conectividad de red con la PC-C.

```
C:\Users\User1> tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2  192.168.1.1  reports: Destination host unreachable.

Trace complete.
```

Una manera de localizar el problema de la red es hacer ping a cada salto en la red hacia la PC-C. Determine primero si la PC-A tiene posibilidad de conexión a la interfaz Serial 0/0/1 del router ISP con la dirección IP 10.2.2.2.

```
C:\Users\Utraser1> ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

El ping se realizó correctamente para el router ISP. El salto siguiente en la red es el router REMOTE. Haga ping a la interfaz Serial 0/0/1 del router REMOTE con la dirección IP 10.2.2.1.

```
C:\Users\User1> ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

La PC-A tiene posibilidad de conexión al router REMOTE. Según los resultados correctos del ping de la PC-A al router REMOTE, el problema de conectividad de red es con la red 192.168.3.0/24. Haga ping al gateway predeterminado de la PC-C, que es la interfaz GigabitEthernet 0/1 del router REMOTE.

```
C:\Users\User1> ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

La PC-A no tiene posibilidad de conexión a la interfaz GigabitEthernet 0/1 del router REMOTE, tal como lo muestran los resultados del comando **ping**.

También se puede hacer ping al switch S3 desde la PC-A para verificar la ubicación del problema de conectividad de red escribiendo **ping 192.168.3.11** en el símbolo del sistema. Dado que la PC-A no tiene posibilidad de conexión a la interfaz GigabitEthernet 0/1 del router REMOTE, es probable que la PC-A no pueda hacer ping al switch S3 correctamente, como lo indican los siguientes resultados.

```
C:\Users\User1> ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Mediante los resultados de tracert y ping, se concluye que la PC-A tiene posibilidad de conexión a los routers LOCAL, ISP y REMOTE, pero no a la PC-C, el switch S3 ni el gateway predeterminado para la PC-C.

b. Utilice los comandos **show** para examinar las configuraciones en ejecución del router REMOTE.

```
REMOTE# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.8.1     YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up

REMOTE# show run
<resultado omitido>
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.8.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
<resultado omitido>
```

Los resultados de los comandos **show run** y **show ip interface brief** indican que el estado de la interfaz GigabitEthernet 0/1 es up/up (activo/activo), pero se configuró con una dirección IP incorrecta.

c. Corrija la dirección IP para GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

d. Verifique que la PC-A pueda hacer ping y tracert a la PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 44ms, Average = 41ms

C:\Users\User1> tracert 192.168.3.3

Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]

Trace complete.
```

Nota: esto también se puede lograr mediante los comandos **ping** y **traceroute** desde la CLI en el router LOCAL y el switch S1 después de verificar que no haya problemas de conectividad de red en la red 192.168.1.0/24.

Reflexión

1. ¿Qué podría evitar que las respuestas de los comandos ping o traceroute lleguen al dispositivo de origen, además de problemas de conectividad de red?

2. Si hace ping a una dirección inexistente en la red remota, como 192.168.3.4, ¿qué mensaje mostrará el comando **ping**? ¿Qué significa esto? Si hace ping a una dirección de host válida y recibe esta respuesta, ¿qué debe revisar?

3. Si hace ping a una dirección que no existe en ninguna red de la topología, como 192.168.5.3, desde una PC con Windows, qué mensaje que mostrará el comando **ping**? ¿Qué significa este mensaje?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

3.4.24.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.24.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando

detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.24.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.25 Practica 25. Cálculo de subredes IPv4

3.4.25.1 Objetivo

Parte 1: Determinar la división en subredes de la dirección IPv4.

Parte 2: Calcular la división en subredes de la dirección IPv4.

3.4.25.2 Introducción

La capacidad de trabajar con subredes IPv4 y de determinar la información de red y host sobre la base de una dirección IP y una máscara de subred determinadas es fundamental para comprender la forma en que funcionan las redes IPv4. La primera parte de diseñó para reforzar el conocimiento de la forma de calcular la información de dirección IP de una red a partir de una dirección IP y una máscara de subred determinadas. Al tener una dirección IP y una máscara de subred específicas, podrá determinar información adicional sobre la subred, por ejemplo:

- Dirección de red
- Dirección de broadcast
- Cantidad total de bits de host
- Cantidad de host por subred

3.4.25.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.25.4 Material Y Equipo Necesario

40. Equipo De Cómputo.
41. Conexión A Internet.
42. Packet Tracer

3.4.25.5 Metodología

Parte 1: Determinar la división en subredes de la dirección IPv4

En la parte 1, determinará las direcciones de red y de broadcast, así como la cantidad de hosts, dada una dirección IPv4 y una máscara de subred.

REPASO: para determinar la dirección de red, realice la operación AND binaria en la dirección IPv4 utilizando la máscara de subred que se proporciona. El resultado será la dirección de red. Sugerencia: si la máscara de subred tiene el valor decimal 255 en un octeto, el resultado SIEMPRE será el valor original de ese octeto. Si la máscara de subred tiene el valor decimal 0 en un octeto, el resultado SIEMPRE será 0 para ese octeto.

Ejemplo:

Dirección IP	192.168.10.10
Máscara de subred	255.255.255.0
	==========
Resultado (red)	192.168.10.0

Al saber esto, es posible que solo tenga que realizar una operación AND binaria en un octeto que no tenga 255 o 0 en la porción de máscara de subred.

Ejemplo:

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0

Al analizar este ejemplo, puede ver que solo tiene que realizar la operación AND binaria en el tercer octeto. El resultado de los dos primeros octetos será 172.30, debido a la máscara de subred. El resultado del cuarto octeto será 0, debido a la máscara de subred.

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0
	==========
Resultado (red)	172.30.**?**.0

Realice la operación AND binaria en el tercer octeto.

	Decimal	**Binario**
	239	11101111
	192	11000000
		=======
Resultado	**192**	11000000

Si se vuelve a analizar este ejemplo, el resultado será el siguiente:

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0
	==========
Resultado (red)	172.30.192.0

Con este mismo ejemplo, para calcular la cantidad de hosts por red puede analizarse la máscara de subred. La máscara de subred estará representada en formato decimal punteado, como 255.255.192.0, o en formato de prefijo de red, como /18. Las direcciones IPv4 siempre tienen 32 bits. Restar la cantidad de bits utilizados para la porción de red (representada por la máscara de subred) da como resultado la cantidad de bits utilizados para los hosts.

Con el ejemplo anterior, la máscara de subred 255.255.192.0 equivale a /18 en notación de prefijo. Restar 18 bits de red de 32 bits da como resultado 14 bits para la porción de host. A partir de allí, es un cálculo simple:

$2^{(\text{cantidad de bits del host})} - 2 = \text{cantidad de hosts}$

$2^{14} = 16\,384 - 2 = 16\,382$ hosts

Determine las direcciones de red y broadcast y la cantidad de bits de host y hosts para las direcciones IPv4 y los prefijos dados en la siguiente tabla.

Dirección IPv4/prefijo	Dirección de red	Dirección de broadcast	Cantidad total de bits de host	Cantidad total de hosts
192.168.100.25/28				
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

Parte 2: Calcular la división en subredes de la dirección IPv4

Dada una dirección IPv4, la máscara de subred original y la nueva máscara de subred, podrá determinar lo siguiente:

- Dirección de red de esta subred
- Dirección de broadcast de esta subred
- Rango de direcciones de host de esta subred
- Cantidad de subredes creadas
- Cantidad de hosts por subred

A continuación, se muestra un problema de ejemplo junto con la solución:

Dado:	
Dirección IP del host:	172.16.77.120
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.240.0
Encontrar:	
Cantidad de bits de subred	4
Cantidad de subredes creadas	16
Cantidad de bits de host por subred	12
Cantidad de hosts por subred	4,094
Dirección de red de esta subred	172.16.64.0
Dirección IPv4 del primer host en esta subred	172.16.64.1
Dirección IPv4 del último host en esta subred	172.16.79.254
Dirección de broadcast IPv4 en esta subred	172.16.79.255

Analicemos cómo se completó esta tabla.

La máscara de subred original era 255.255.0.0 o /16. La nueva máscara de subred es 255.255.240.0 o /20. La diferencia resultante es 4 bits. Como se tomaron prestados 4 bits, podemos determinar que se crearon 16 subredes, ya que $2^4 = 16$.

La nueva máscara 255.255.240.0 o /20 deja 12 bits para los hosts. Con 12 bits para los hosts, utilizamos la siguiente fórmula: $2^{12} = 4096 – 2 = 4094$ hosts por subred.

La operación AND binaria lo ayudará a determinar la subred de este problema, que da como resultado la red 172.16.64.0.

Finalmente, necesita determinar el primer host, el último host y la dirección de broadcast para cada subred. Un método para determinar el rango de hosts es aplicar cálculos binarios para la porción de host de la dirección. En el ejemplo, los últimos 12 bits de la dirección corresponden a la porción de host. El primer host tendría todos los bits significativos establecidos en cero y el bit menos significativo establecido en 1. El último host tendría todos los bits significativos establecidos en 1 y el bit menos significativo establecido en 0. En este ejemplo, la porción de host de la dirección reside en el tercero y el cuarto octetos.

Descripción	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto	Descripción
Red/host	**nnnnnnnn**	**nnnnnnnn**	**nnnn**hhhh	hhhhhhhh	Máscara de subred
Binario	**10101100**	**00010000**	**0100**0000	00000001	Primer host
Decimal	172	16	64	1	Primer host
Binario	**10101100**	**00010000**	**0100**1111	11111110	Último host
Decimal	172	16	79	254	Último host
Binario	**10101100**	**00010000**	**0100**1111	11111111	Broadcast
Decimal	172	16	79	255	Broadcast

Paso 1: Complete las tablas siguientes con las respuestas correspondientes dadas la dirección IPv4, la máscara de subred original y la nueva máscara de subred.

a. **Problema 1**:

Dado:	
Dirección IP del host:	192.168.200.139
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.224
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

b. **Problema 2**:

Dado:	
Dirección IP del host:	10.101.99.228
Máscara de subred original	255.0.0.0
Máscara de subred nueva:	255.255.128.0
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

c. **Problema 3**:

Dado:	
Dirección IP del host:	172.22.32.12
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.224.0
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

d. **Problema 4**:

Dado:	
Dirección IP del host:	192.168.1.245
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.252
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

e. **Problema 5**:

Dado:	
Dirección IP del host:	128.107.0.55
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.255.0
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

f. **Problema 6**:

Dado:	
Dirección IP del host:	192.135.250.180
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.248
Encontrar:	
Cantidad de bits de subred	
Cantidad de subredes creadas	
Cantidad de bits de host por subred	
Cantidad de hosts por subred	
Dirección de red de esta subred	
Dirección IPv4 del primer host en esta subred	
Dirección IPv4 del último host en esta subred	
Dirección de broadcast IPv4 en esta subred	

Reflexión

¿Por qué la máscara de subred es tan importante cuando se analiza una dirección IPv4?

3.4.25.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.25.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.25.8 Bibliografías

Cisco Networking Academy: Learn Cybersecurity, Python & more. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.26. Practica 26. División de topologías de red en subredes

3.4.26.1 Objetivo

De la parte 1 a la 5, para todas las topologías de red:

- Determinar la cantidad de subredes.
- Diseñar un esquema de direccionamiento adecuado.
- Asignar direcciones y pares de máscaras de subred a las interfaces del dispositivo.
- Examinar el uso del espacio de direcciones de red disponible y el crecimiento potencial futuro.

3.4.26.2 Introducción

Ante una topología de la red, es importante poder determinar la cantidad de subredes necesarias. En esta práctica de laboratorio, se proporcionarán varias situaciones de topologías, junto con una máscara y una dirección de red base. Dividirá la dirección de red en subredes y proporcionaran un esquema de direccionamiento IP que admitirá la cantidad de subredes que se muestra en el diagrama de topología. Deberá determinar la cantidad de bits que se deben tomar prestados, la cantidad de hosts por subred y el potencial de crecimiento según lo especificado en las instrucciones.

3.4.26.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.4.26.4 Material Y Equipo Necesario

43. Equipo De Cómputo.

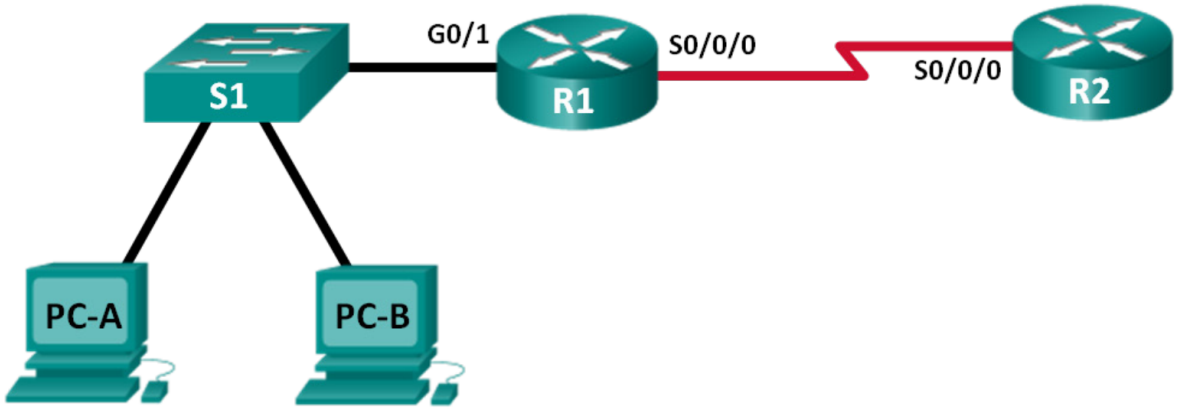
44. Conexión A Internet.

45. Packet Tracer

3.4.26.5 Metodología

Parte 1: Topología de la red A

En la parte 1, se otorgó la dirección de red 192.168.10.0/24 a la subred, con la siguiente topología. Determine la cantidad de redes necesarias y luego diseñe un esquema de direccionamiento adecuado.



Paso 1: Determine la cantidad de subredes en la topología de la red A.

a. ¿Cuántas subredes hay?

b. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas?

c. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?

d. ¿Cuál es la máscara de subred nueva en formato decimal punteado?

e. ¿Cuántas subredes quedan disponibles para usar en el futuro?

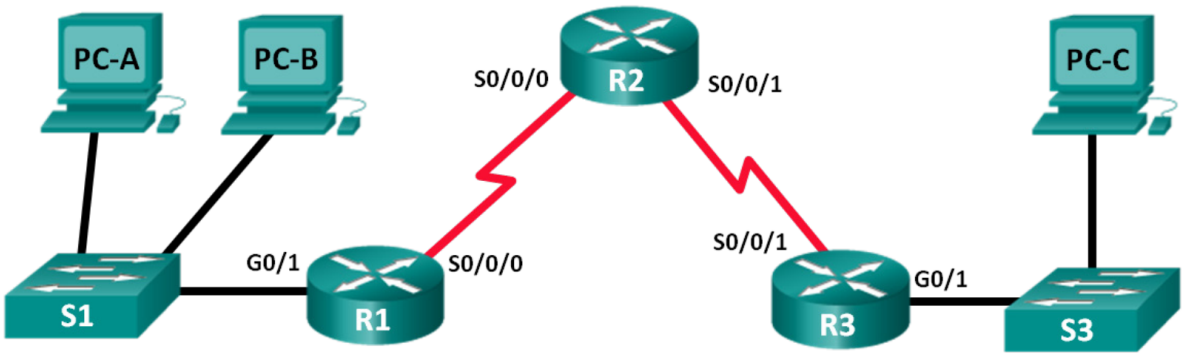
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				

Parte 2: Topología de la red B

La topología de la red de la parte 1 se expandió para admitir el agregado del router R3 y la red complementaria, como se ilustra en la topología siguiente. Utilice la dirección de red 192.168.10.0/24 para proporcionar direcciones a los dispositivos de red y luego diseñe un nuevo esquema de direccionamiento para admitir el requisito de red adicional.



Paso 1: Determine la cantidad de subredes en la topología de la red B.

a. ¿Cuántas subredes hay?

b. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas?

c. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?

d. ¿Cuál es la máscara de subred nueva en formato decimal punteado?

e. ¿Cuántas subredes quedan disponibles para usar en el futuro?

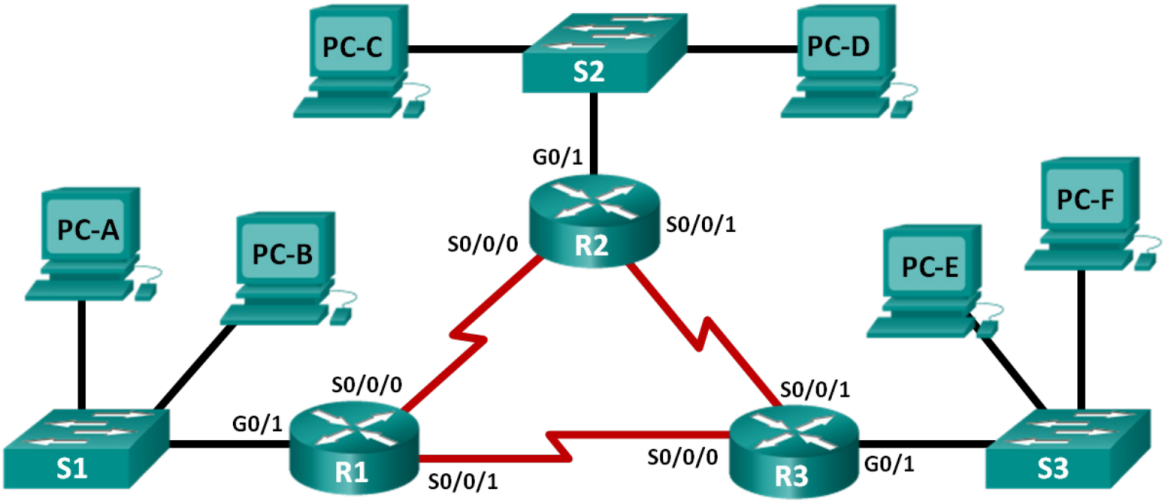
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				

Parte 3: Topología de la red C

La topología volvió a cambiar con una LAN nueva agregada al R2 y un enlace redundante entre R1 y R3. Utilice la dirección de red 192.168.10.0/24 para proporcionar direcciones a los dispositivos de red. También proporcione un esquema de direcciones IP que admita estos dispositivos adicionales. Para esta topología, asigne una subred a cada red.



Paso 1: Determine la cantidad de subredes en la topología de la red C.

a. ¿Cuántas subredes hay?

b. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas?

c. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?

d. ¿Cuál es la máscara de subred nueva en formato decimal punteado?

e. ¿Cuántas subredes quedan disponibles para usar en el futuro?

Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Paso 3: Asignar direcciones a los dispositivos de red en las subredes

a. Complete la siguiente tabla con las direcciones IP y las máscaras de subred para las interfaces del router:

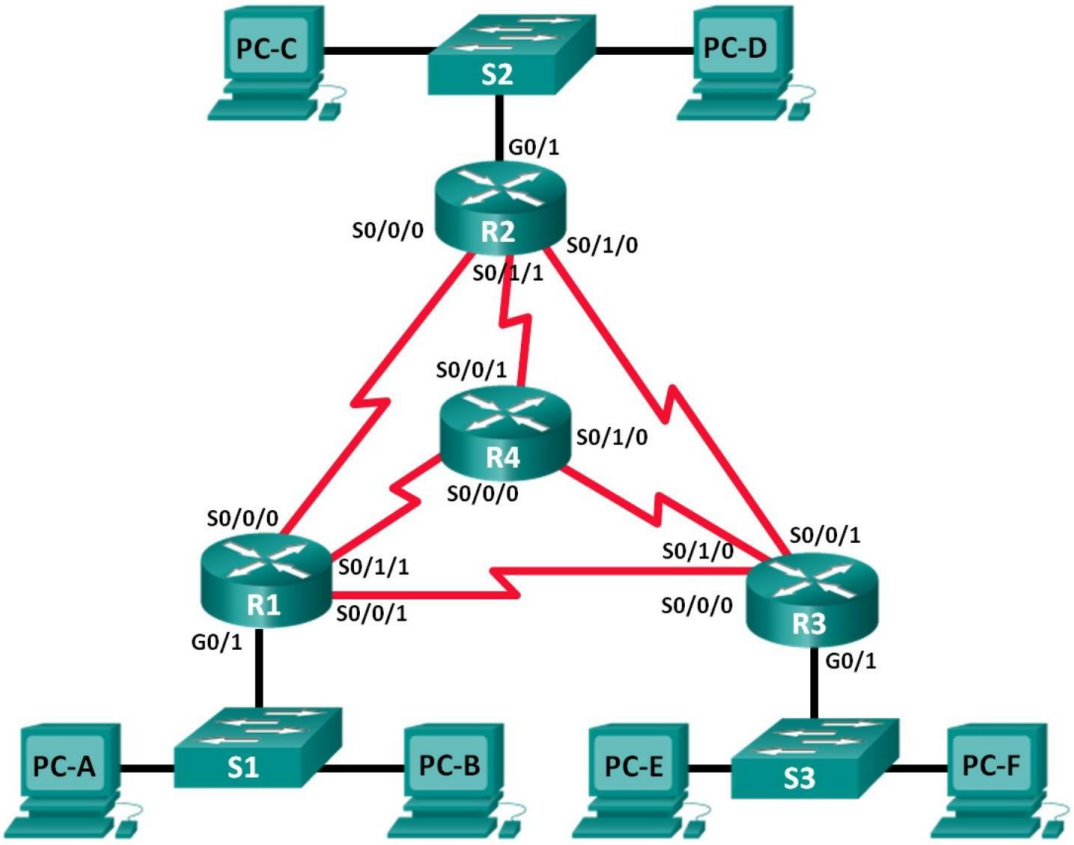
Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R2	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R3	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		

b. Complete la tabla siguiente con las direcciones IP y las máscaras de subred para los dispositivos en la LAN, como se muestra en la topología.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC-A	NIC			
PC-B	NIC			
S1	VLAN 1			
PC-C	NIC			
PC-D	NIC			
S2	VLAN 1			
PC-E	NIC			
PC-F	NIC			
S3	VLAN 1			

Parte 4: Topología de la red D

La red se modificó para admitir cambios en la organización. Se utiliza la dirección de red 192.168.10.0/24 para proporcionar las direcciones en la red.



Paso 1: Determine la cantidad de subredes en la topología de la red D.

a. ¿Cuántas subredes hay?

b. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas?

c. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?

d. ¿Cuál es la máscara de subred nueva en formato decimal punteado?

e. ¿Cuántas subredes quedan disponibles para usar en el futuro?

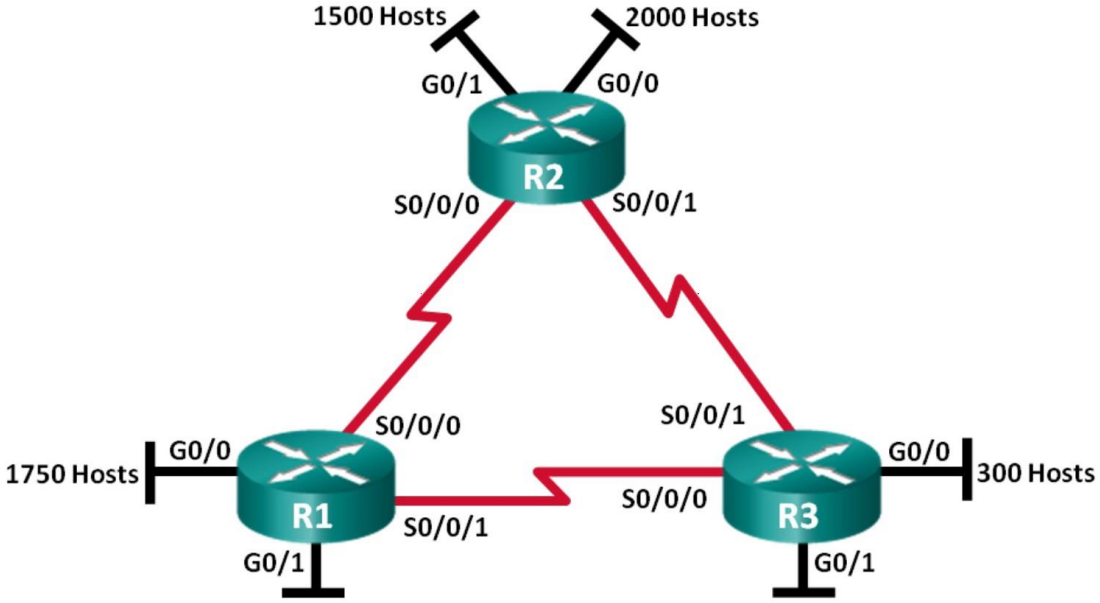
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Parte 5: Topología de la red E

La organización tiene una dirección de red 172.16.128.0/17 que se dividirá como se ilustra en la topología siguiente. Debe elegir un esquema de direccionamiento que pueda admitir la cantidad de redes y hosts en la topología.



Paso 1: Determine la cantidad de subredes en la topología de la red E.

a. ¿Cuántas subredes hay?

b. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas?

c. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?

d. ¿Cuál es la máscara de subred nueva en formato decimal punteado?

e. ¿Cuántas subredes quedan disponibles para usar en el futuro?

Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Paso 3: Asignar direcciones a los dispositivos de red en las subredes

a. Complete la siguiente tabla con las direcciones IP y las máscaras de subred para las interfaces del router:

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	GigabitEthernet 0/0		
	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R2	GigabitEthernet 0/0		
	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R3	GigabitEthernet 0/0		
	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		

Reflexión

1. ¿Qué información es necesaria cuando debe determinar un esquema de direccionamiento adecuado para una red?

2. Una vez asignadas las subredes, ¿se utilizarán todas las direcciones de host en cada subred?

3.4.26.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.26.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.26.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.27 Práctica 27. Diseño e implementación de un esquema de direccionamiento IPv4 dividido en subredes

3.4.27.1 Objetivo

Parte 1: Diseñar un esquema de división en subredes

Parte 2: Configurar los dispositivos

Parte 3: Probar la red y resolver los problemas encontrados

3.4.27.2 Introducción

En esta práctica de laboratorio, a partir de una sola dirección de red y una máscara de red, dividirá la red en varias subredes. El esquema de división en subredes se basará en la cantidad de equipos host necesarios en cada subred, así como en otras consideraciones de redes, como la futura expansión de hosts de la red.

Después de crear un esquema de división en subredes y completar el diagrama de red con las direcciones IP de hosts e interfaces, configurará las PC host y las interfaces del router, incluidas las interfaces loopback. Las interfaces loopback se crean para simular LAN adicionales conectadas al router R1.

Una vez configurados los dispositivos de red y las PC host, utilizará el comando ping para probar la conectividad de red.

En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos reales necesarios para configurar el router. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento intentando configurar los dispositivos sin consultar el apéndice.

3.4.27.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.27.4 Material Y Equipo Necesario

46. Equipo De Cómputo.
47. Conexión A Internet.
48. Packet Tracer

3.4.27.5 Metodología

Parte 1: Diseñar un esquema de división en subredes

Paso 1: Crear un esquema de división en subredes que cumpla con la cantidad requerida de subredes y de direcciones de host

En esta situación, usted es un administrador de red para una pequeña subdivisión de una compañía más grande. Debe crear varias subredes a partir del espacio de direcciones de red 192.168.0.0/24 para cumplir los siguientes requisitos:

- La primera subred es la red de los empleados. Necesita un mínimo de 25 direcciones IP de host.
- La segunda subred es la red de administración. Necesita un mínimo de 10 direcciones IP.
- La tercera y la cuarta subredes están reservadas como redes virtuales en las interfaces virtuales del router loopback 0 y loopback 1. Estas interfaces virtuales del router simulan LAN conectadas al R1.
- También necesita dos subredes adicionales sin utilizar para la futura expansión de la red.

Nota: no se usarán máscaras de subred de longitud variable. Todas las máscaras de subred de los dispositivos tendrán la misma longitud.

Responda las siguientes preguntas para poder crear un esquema de división en subredes que cumpla con los requisitos de red mencionados:

1) ¿Cuántas direcciones de host se necesitan en la subred requerida más grande?
2) ¿Cuál es la cantidad mínima de subredes necesaria?
3) La red que se le asignó para la división en subredes es 192.168.0.0/24. ¿Cómo es la máscara de subred /24 en formato binario?

4) La máscara de subred consta de dos partes: la porción de red y la porción de host. En sistema binario, esto se representa mediante unos y ceros en la máscara de subred.

   En la máscara de red, ¿qué representan los unos?

   En la máscara de red, ¿qué representan los ceros?

5) Para dividir una red en subredes, los bits de la porción de host de la máscara de red original cambian por bits de subred. La cantidad de bits de subred define la cantidad de subredes. Dada cada una de las posibles máscaras de subred presentadas a continuación en formato binario, ¿cuántas subredes y cuántos hosts se crean en cada ejemplo?

   Sugerencia: recuerde que la cantidad de bits de host (en potencia de 2) define la cantidad de hosts por subred (menos 2), y que la cantidad de bits de subred (en potencia de 2) define la cantidad de subredes. Los bits de subred (representados en negrita) son los bits que se tomaron prestados más allá de la máscara de red original /24. /24 es la notación de prefijo de barra y corresponde a la máscara decimal punteada 255.255.255.0.

   (/25) 11111111.11111111.11111111.**1**0000000

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

   (/26) 11111111.11111111.11111111.**11**000000

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

   (/27) 11111111.11111111.11111111.**111**00000

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

   (/28) 11111111.11111111.11111111.**1111**0000

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

   (/29) 11111111.11111111.11111111.**11111**000

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

   (/30) 11111111.11111111.11111111.**111111**00

   Equivalente decimal punteado de la máscara de subred:

   ¿Cantidad de subredes? ¿Cantidad de hosts?

6) Sobre la base de sus respuestas, ¿qué máscaras de subred cumplen con la cantidad mínima requerida de direcciones de host?

7) Sobre la base de sus respuestas, ¿qué máscaras de subred cumplen con la cantidad mínima requerida de subredes?

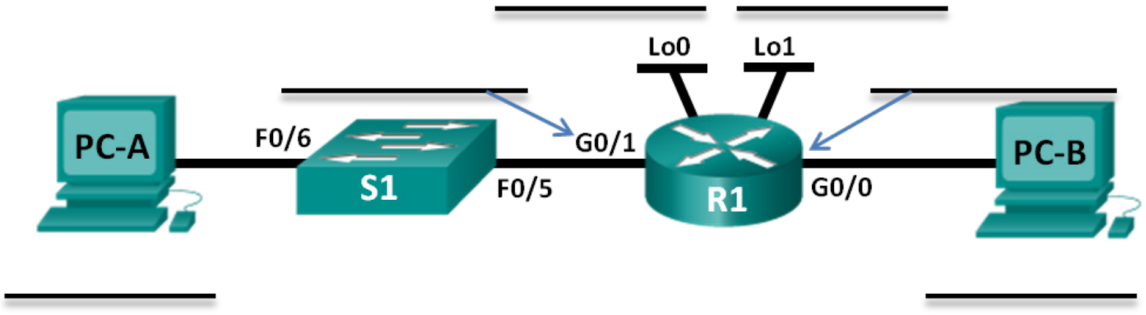
8) Sobre la base de sus respuestas, ¿qué máscara de subred cumple con la cantidad mínima requerida de hosts y también con la cantidad mínima requerida de subredes?

9) Cuando haya determinado qué máscara de subred cumple con todos los requisitos de red mencionados, derivará cada una de las subredes a partir de la dirección de red original. Indique las subredes desde la primera hasta la última a continuación. Recuerde que la primera subred es 192.168.0.0, con la máscara de subred recién adquirida.

Dirección de subred	/ Prefijo	Máscara de subred (decimal punteada)
	/	
	/	
	/	
	/	
	/	
	/	
	/	
	/	
	/	
	/	

Paso 2: Completar el diagrama para mostrar dónde se aplicarán las direcciones IP de host

En las líneas siguientes, complete las direcciones IP y las máscaras de subred en notación de prefijo de barra. En el router, utilice la primera dirección utilizable en cada subred para cada una de las interfaces: Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 y loopback 1. Complete una dirección IP para la PC-A y la PC-B. También introduzca esta información en la tabla de direccionamiento de la página 1.



Parte 2: Configurar los dispositivos

En la parte 2, establecerá la topología de la red y configurará los parámetros básicos en las PC y el router, como las direcciones IP de la interfaz Gigabit Ethernet del router y las direcciones IP, las máscaras de subred y los gateways predeterminados de las PC. Consulte la tabla de direccionamiento para obtener los nombres e información de dirección de los dispositivos.

Nota: en el apéndice A, se proporcionan detalles de configuración para los pasos de la parte 2. Antes de consultar el apéndice A, intente completar la parte 2.

Paso 1: Configurar el router.

a. Ingrese al modo EXEC privilegiado y, luego, al modo de configuración global.

b. Asigne **R1** como nombre de host para el router.

c. Configure las interfaces **G0/0** y **G0/1** con direcciones IP y máscaras de subred y, luego, habilítelas.

d. Las interfaces loopback se crean para simular LAN adicionales en el router R1. Configure las interfaces loopback con direcciones IP y máscaras de subred. Una vez que se crean, las interfaces loopback se habilitan de manera predeterminada. (Para crear las direcciones de loopback, introduzca el comando **interface loopback 0** en el modo de configuración global).

   Nota: si lo desea, puede crear varios loopbacks adicionales para probar con diferentes esquemas de direccionamiento.

e. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 2: Configure las interfaces de la PC.

a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.

b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.

Parte 3: Probar la red y resolver los problemas encontrados

En la parte 3, utilizará el comando **ping** para probar la conectividad de red.

a. Pruebe si la PC-A puede comunicarse con el gateway predeterminado. En la PC-A, abra un símbolo del sistema y haga ping a la dirección IP de la interfaz Gigabit Ethernet 0/1 del router. ¿Obtiene una respuesta?

b. Pruebe si la PC-B puede comunicarse con el gateway predeterminado. En la PC-B, abra un símbolo del sistema y haga ping a la dirección IP de la interfaz Gigabit Ethernet 0/0 del router. ¿Obtiene una respuesta?

c. Pruebe si la PC-A puede comunicarse con la PC-B. En la PC-A, abra un símbolo del sistema y haga ping a la dirección IP de la PC-B. ¿Obtiene una respuesta?

d. Si alguna de sus respuestas a las preguntas anteriores fue negativa, debe revisar todas las configuraciones de dirección IP y máscara de subred, y asegurarse de que los gateways predeterminados estén configurados correctamente en la PC-A y la PC-B.

e. Si verifica que todas las configuraciones son correctas y aún no puede hacer ping correctamente, hay algunos otros factores que pueden bloquear los pings de ICMP. En Windows, en la PC-A y la PC-B, asegúrese de que el Firewall de Windows esté desactivado para las redes de trabajo, doméstica y pública.

f. Experimente configurando a propósito la dirección del gateway de manera incorrecta en la PC-A como 10.0.0.1. ¿Qué sucede cuando intenta hacer ping de la PC-B a la PC-A? ¿Recibe una respuesta?

Reflexión

1. Dividir una red grande en subredes más pequeñas brinda mayor flexibilidad y seguridad en el diseño de redes. Sin embargo, ¿cuáles piensa que son algunas en las desventajas cuando las subredes están limitadas a tener el mismo tamaño?

2. ¿Por qué piensa que la dirección IP del gateway o del router es generalmente la primera dirección IP utilizable en la red?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

Apéndice A: Detalles de configuración para los pasos de la parte 2

Paso 1: Configurar el router.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
Router#
```

b. Entre al modo de configuración.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

c. Asigne un nombre de dispositivo al router.

```
Router(config)# hostname R1
R1(config)#
```

d. Configure las interfaces **G0/0** y **G0/1** con direcciones IP y máscaras de subred, y habilítelas.

```
R1(config)# interface g0/0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
```

e. Las interfaces loopback se crean para simular LAN adicionales fuera del router R1. Configure las interfaces loopback con direcciones IP y máscaras de subred. Cuando se crean, las interfaces loopback se habilitan de manera predeterminada.

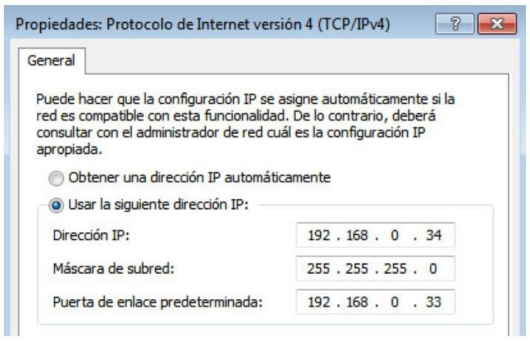
```
R1(config)# interface loopback 0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# interface loopback 1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# end
```

f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

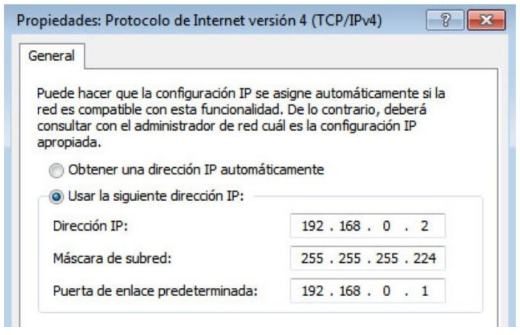
```
R1# copy running-config startup-config
```

Paso 2: Configure las interfaces de la PC.

a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.



b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.



3.4.27.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.27.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.27.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.28 Práctica 28. Diseño e implementación de un esquema de direccionamiento VLSM

3.4.28.1 Objetivo

Parte 1: Examinar los requisitos de la red

Parte 2: Diseñar el esquema de direcciones VLSM

Parte 3: Cablear y configurar la red IPv4

3.4.28.2 Introducción

La máscara de subred de longitud variables (VLSM) se diseñó para evitar el desperdicio de direcciones IP con VLSM, una red se divide en subredes y luego se vuelve a dividir en subredes. Este proceso se puede repetir varias veces para crear subredes de diversos tamaños según la cantidad de hosts necesarios en cada subred. El uso eficaz de VLSM requiere la planificación de direcciones.

En esta práctica de laboratorio, utilice la dirección de red 172.16.128.0/17 para desarrollar un esquema de direcciones para la red que se muestra en el diagrama de topología VLSM se utiliza para cumplir con los requisitos de direccionamiento IPv4. Después de diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información de direcciones IP correspondiente.

3.4.28.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.28.4 Material Y Equipo Necesario

49. Equipo De Cómputo.

50. Conexión A Internet.

51. Packet Tracer

3.4.28.5 Metodología

Parte 1: Examinar los requisitos de la red

En la parte 1, examinará los requisitos de la red para desarrollar un esquema de direcciones VLSM para la red que se muestra en el diagrama de topología utilizando la dirección de red 172.16.128.0/17.

Nota: para obtener ayuda con los cálculos, puede utilizar la aplicación de calculadora de Windows y la calculadora de subredes IP de www.ipcalc.org.

Paso 1: Determinar cuántas direcciones de host y cuántas subredes hay disponibles

¿Cuántas direcciones de host hay disponibles en una red /17?

¿Cuál es la cantidad total de direcciones de host necesarias en el diagrama de topología?

¿Cuántas subredes se necesitan en la topología de la red?

Paso 2: Determinar la subred más grande

¿Cuál es la descripción de la subred (p. ej., enlace BR1 G0/1 LAN o BR1-HQ WAN)?

¿Cuántas direcciones IP se requieren en la subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede dividir la dirección de red 172.16.128.0/17 en subredes para admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 3: Determinar la segunda subred más grande

¿Cuál es la descripción de la subred?

¿Cuántas direcciones IP se requieren para la segunda subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 4: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred?

¿Cuántas direcciones IP se requieren para la siguiente subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 5: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred?

¿Cuántas direcciones IP se requieren para la siguiente subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 6: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred?

¿Cuántas direcciones IP se requieren para la siguiente subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 7: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred?

¿Cuántas direcciones IP se requieren para la siguiente subred más grande?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

¿Cuántas direcciones de host totales puede admitir esa máscara de subred?

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred?

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

Utilice la primera dirección de red para esta subred.

Paso 8: Determinar las subredes necesarias para admitir los enlaces seriales

¿Cuántas direcciones de host se requieren para cada enlace serial de subred?

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

a. Continúe subdividiendo la primera subred de cada subred nueva hasta que tenga cuatro subredes /30. Escriba las tres primeras direcciones de red de estas subredes /30 a continuación.

b. Introduzca las descripciones de subred para estas tres subredes a continuación.

Parte 2: Diseñar el esquema de direcciones VLSM

Paso 1: Calcular la información de subred

Utilice la información que obtuvo en la parte 1 para completar la siguiente tabla.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red /CIDR	Primera dirección de host	Dirección de broadcast
HQ G0/0	16 000			
HQ G0/1	8 000			
BR1 G0/1	4 000			
BR1 G0/0	2 000			
BR2 G0/1	1000			
BR2 G0/0	500			
HQ S0/0/0 – BR1 S0/0/1	2			
HQ S0/0/1 – BR2 S0/0/1	2			
BR1 S0/0/1 – BR2 S0/0/0	2			

Paso 2: Completar la tabla de direcciones de interfaces de dispositivos

Asigne la primera dirección de host en la subred a las interfaces Ethernet. A HQ se le debe asignar la primera dirección de host en los enlaces seriales a BR1 y BR2. A BR1 se le debe asignar la primera dirección de host para el enlace serial a BR2.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Interfaz de dispositivo
HQ	G0/0			LAN de 16 000 hosts
	G0/1			LAN de 8000 hosts
	S0/0/0			BR1 S0/0/0
	S0/0/1			BR2 S0/0/1
BR1	G0/0			LAN de 2000 hosts
	G0/1			LAN de 4000 hosts
	S0/0/0			HQ S0/0/0
	S0/0/1			BR2 S0/0/0
BR2	G0/0			LAN de 500 hosts
	G0/1			LAN de 1000 hosts
	S0/0/0			BR1 S0/0/1
	S0/0/1			HQ S0/0/1

Parte 3: Cablear y configurar la red IPv4

En la parte 3, realizará el cableado de la topología de la red y configurará los tres routers mediante el esquema de direcciones VLSM que desarrolló en la parte 2.

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

Paso 2: Configurar los parámetros básicos en cada router

a. Asigne el nombre de dispositivo al router.

b. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

c. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

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

e. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

f. Encripte las contraseñas de texto no cifrado.

g. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

Paso 3: Configurar las interfaces en cada router

a. Asigne una dirección IP y una máscara de subred a cada interfaz por medio de la tabla que completó en la parte 2.

b. Configure una descripción de la interfaz para cada interfaz.

c. Establezca la velocidad del reloj de todas las interfaces seriales DCE en 128000.

```
HQ(config-if)# clock rate 128000
```

d. Active las interfaces.

Paso 4: Guardar la configuración en todos los dispositivos

Paso 5: Probar la conectividad

a. En HQ, haga ping a la dirección de la interfaz S0/0/0 de BR1.

b. En HQ, haga ping a la dirección de la interfaz S0/0/1 de BR2.

c. En BR1, haga ping a la dirección de la interfaz S0/0/0 de BR2.

d. Si los pings no se realizaron correctamente, resuelva los problemas de conectividad.

Nota: los pings a las interfaces GigabitEthernet en otros routers no se realizarán correctamente. Las LAN definidas para las interfaces GigabitEthernet son simuladas. Dado que no hay dispositivos conectados a estas LAN, el estado será down/down (inactivo/inactivo). Debe haber un protocolo de enrutamiento implementado para que los otros dispositivos adviertan esas subredes. Las interfaces GigabitEthernet también deben tener un estado up/up (activo/activo) para que un protocolo de enrutamiento pueda agregar las subredes a la tabla de enrutamiento. Estas interfaces permanecerán en un estado down/down hasta que se conecte un dispositivo al otro extremo del cable de la interfaz Ethernet. Esta práctica de laboratorio se centra en VLSM y en la configuración de las interfaces.

Reflexión

¿Puede pensar en un atajo para calcular las direcciones de red de las subredes /30 consecutivas?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

3.4.28.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.28.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.28.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.29 Práctica 29. Servidores Web y de correo electrónico

3.4.29.1 Objetivo

Parte 1: Configurar y verificar los servicios Web

Parte 2: Configurar y verificar los servicios de correo electrónico

3.4.29.2 Introducción

En esta actividad, configurará los servicios HTTP y de correo electrónico mediante el servidor simulado de Packet Tracer. Luego, configurará clientes para que accedan a los servicios HTTP y de correo electrónico.

3.4.29.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.29.4 Material Y Equipo Necesario

52. Equipo De Cómputo.
53. Conexión A Internet.
54. Packet Tracer

3.4.29.5 Metodología

Parte 1: Configurar y verificar los servicios Web

Paso 1: Configurar servicios Web en CentralServer y BranchServer

a. Haga clic en **CentralServer** y, a continuación, haga clic en la ficha **Config** > **HTTP**.

b. Haga clic en **On** (Activar) para habilitar HTTP y HTTP seguro (HTTPS).

c. Optativo: personalice el código HTML.

d. Repita desde el paso 1a hasta el paso 1c en **BranchServer**.

Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web

Existen muchos dispositivos terminales en esta red, pero para este paso, use **PC3**.

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Escritorio > Explorador Web).

b. En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.

c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.

d. En el cuadro de dirección URL, introduzca **centralserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **CentralServer**.

e. En el cuadro de dirección URL, introduzca **branchserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.

f. ¿Qué protocolo traduce los nombres **centralserver.pt.pka** y **branchserver.pt.pka** por direcciones IP?

Parte 2: Configurar y verificar los servicios de correo electrónico en los servidores

Paso 1: Configurar CentralServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **CentralServer** y, a continuación, seleccione la ficha **Config**, seguida del botón **EMAIL** (Correo electrónico).

b. Haga clic en **On** para habilitar SMTP y POP3.

c. Establezca el nombre de dominio **centralserver.pt.pka** y haga clic en **Set** (Establecer).

d. Cree un usuario denominado **usuario-de-central** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.

Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **BranchServer** y, a continuación, haga clic en la ficha **Config** > **EMAIL**.

b. Haga clic en **On** para habilitar SMTP y POP3**.**

c. Establezca el nombre de dominio **branchserver.pt.pka** y haga clic en **Set**.

d. Cree un usuario denominado **usuario-de-sucursal** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.

Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **E Mail** (Correo electrónico).

b. Introduzca los siguientes valores en los campos correspondientes:

   1) Your Name (Su nombre): **Usuario de central**

   2) Email Address (Dirección de correo electrónico): **usuario-de-central@centralserver.pt.pka**

   3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**

   4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**

   5) User Name (Nombre de usuario): **usuario-de-central**

   6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).

Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

a. Haga clic en **Sales** (Ventas) y, a continuación, haga clic en la ficha **Desktop** > **E Mail**.

b. Introduzca los siguientes valores en los campos correspondientes:

   1) Your Name (Su nombre): **Usuario de sucursal**

   2) Email Address (Dirección de correo electrónico): **usuario-de-sucursal@branchserver.pt.pka**

   3) Incoming Mail Server (Servidor de correo entrante): **172.16.0.3**

   4) Outgoing Mail Server (Servidor de correo saliente): **172.16.0.3**

   5) User Name (Nombre de usuario): **usuario-de-sucursal**

   6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).

e. Esta actividad debe completarse en un 100%. No cierre la ventana de configuración de Sales ni la ventana del explorador de correo.

Paso 5: Envíe un correo electrónico desde el cliente Sales y el cliente PC3.

a. Desde la ventana del **explorador de correo** de **Sales**, haga clic en **Compose** (Redactar).

b. Introduzca los siguientes valores en los campos correspondientes:

   1) To (Para): **usuario-de-central@centralserver.pt.pka**

   2) Subject (Asunto): *Personalice el asunto*.

   3) **Email** body (Cuerpo del correo electrónico): *Personalice el correo electrónico*.

c. Haga clic en **Send** (Enviar).

d. Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

e. Haga clic en **Receive** (Recibir). Aparece un correo electrónico proveniente de Sales. Haga doble clic en el correo electrónico.

f. Haga clic en **Reply** (Responder), personalice una respuesta y haga clic en **Send**.

g. Verifique que **Sales** haya recibido la respuesta.

3.4.29.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.29.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.29.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.30 Practica 30. Servidores de DHCP y servidores DNS

3.4.30.1 Objetivo

Parte 1: Configurar el direccionamiento IPv4 estático

Parte 2: Configurar y verificar los registros DNS

3.4.30.2 Introducción

En esta actividad, configurará y verificará el direccionamiento IP estático y el direccionamiento DHCP. A continuación, configurará un servidor DNS para que asigne direcciones IP a los nombres de sitios Web.

3.4.30.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.30.4 Material Y Equipo Necesario

55. Equipo De Cómputo.

56. Conexión A Internet.

57. Packet Tracer

3.4.30.5 Metodología
Parte 1: Configurar el direccionamiento IPv4 estático

Paso 1: Configurar la impresora de inyección de tinta con direccionamiento IPv4 estático

Las PC de oficinas domésticas necesitan conocer la dirección IPv4 de una impresora para enviarle información. Por lo tanto, la impresora debe utilizar una dirección IPv4 estática (invariable).

a. Haga clic en **Inkjet** (Inyección de tinta) y, a continuación, haga clic en la ficha **Config**, en la que se muestran los parámetros de Global Settings (Configuración global).

b. Asigne de manera estática la dirección de gateway **192.168.0.1** y la dirección de servidor DNS **64.100.8.8**.

c. Haga clic en **FastEthernet0** y asigne de manera estática la dirección IP **192.168.0.2** y la dirección de máscara de subred **255.255.255.0**.

d. Cierre la ventana Inkjet.

Paso 2: Configurar WRS para que proporcione servicios de DHCP

a. Haga clic en **WRS** y, a continuación, haga clic en la ficha **GUI** y maximice la ventana.

b. Se muestra la ventana Basic Setup (Configuración básica) de manera predeterminada. Configure los siguientes parámetros en la sección Network Setup (Configuración de red):

   1) Cambie la Dirección IP a **192.168.0.1**.

   2) Establezca la máscara de subred **255.255.255.0**.

   3) Habilite el servidor de DHCP.

   4) Establezca la dirección DNS estática 1 **64.100.8.8**.

   5) Desplácese hasta la parte inferior y haga clic en **Save** (Guardar).

c. Cierre la ventana **WRS**.

Paso 3: Solicitar direccionamiento DHCP para la computadora portátil doméstica

Esta actividad se centra en la oficina doméstica. Los clientes que configurará con DHCP son **Home Laptop** (Computadora portátil doméstica) y **Tablet PC**.

a. Haga clic en **Home Laptop** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

c. Ahora, **Home Laptop** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

d. Cierre la ventana IP Configuration y, a continuación, cierre la ventana **Home Laptop**.

Paso 4: Solicitar direccionamiento DHCP para la tablet PC

a. Haga clic en **Tablet** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration**.

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

Paso 5: Probar el acceso a sitios Web

a. Cierre la ventana **IP Configuration** y, a continuación, haga clic en Web Browser (Explorador Web).

b. En el cuadro de dirección URL, escriba **10.10.10.2** (para el sitio Web de **CentralServer**) o **64.100.200.1** (para el sitio web de **BranchServer**) y haga clic en **Go** (Ir). Deben aparecer ambos sitios Web.

c. Vuelva a abrir el explorador Web. Pruebe los nombres para esos mismos sitios Web mediante la introducción de **centralserver.pt.pka** y **branchserver.pt.pka**. Haga clic en **Fast Forward Time** (Adelantar el tiempo) en la barra amarilla que se encuentra debajo de la topología, a fin de acelerar el proceso.

Parte 2: Configurar los registros en el servidor DNS

Paso 1: Configurar famous.dns.pka con registros para CentralServer y BranchServer.

En general, los registros DNS se realizan ante compañías, pero en esta actividad, usted controla el servidor **famous.dns.pka** en Internet.

a. Haga clic en la nube de **Internet**. Se muestra una nueva red.

b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config** > **DNS**.

c. Agregue los siguientes registros del recurso:

Nombre de registro del recurso	Dirección
centralserver.pt.pka	10.10.10.2.
branchserver.pt.pka	64.100.200.1

d. Cierre la ventana famous.dns.pka.

e. Haga clic en **Back** (Atrás) para salir de la nube de **Internet**.

Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

Ahora que configuró los registros DNS, **Home Laptop** y **Tablet** deben ser capaces de acceder a los sitios Web mediante los nombres en lugar de las direcciones IP. Primero, compruebe que el cliente DNS funcione correctamente y, a continuación, verifique el acceso al sitio Web.

a. Haga clic en **Home Laptop** o **Tablet**.

b. Si el explorador Web está abierto, ciérrelo y seleccione **Command Prompt** (Símbolo del sistema).

c. Verifique el direccionamiento IPv4 mediante la introducción del comando **`ipconfig /all`**. Debe ver la dirección IP del servidor DNS.

d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.

Nota: es posible que los primeros dos o tres pings fallen, ya que Packet Tracer simula los distintos procesos que deben ocurrir para que la conectividad a un recurso remoto sea correcta.

e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos **`nslookup centralserver.pt.pka`** y **`nslookup branchserver.pt.pka`**. Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.

f. Cierre la ventana Command Prompt y haga clic en **Web Browser**. Verifique que **Home Laptop** o **Tablet** puedan acceder ahora a las páginas Web de **CentralServer** y **BranchServer**.

3.4.30.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.30.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.30.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.31 Práctica 31. Servidores FTP

3.4.31.1 Objetivo

Parte 1: Configurar servicios FTP en los servidores

Parte 2: Subir un archivo al servidor FTP

Parte 3: Descargar un archivo del servidor FTP

3.4.31.2 Introducción

En esta actividad, configurará servicios FTP. Luego utilizará FTP para transferir archivos entre los clientes y el servidor.

3.4.31.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

3.4.31.4 Material Y Equipo Necesario

58. Equipo De Cómputo.
59. Conexión A Internet.
60. Packet Tracer

3.4.31.5 Metodología

Parte 1: Configurar servicios FTP en los servidores

Paso 1: Configurar el servicio FTP en CentralServer

a. Haga clic en **CentralServer** > ficha **Config** > **FTP**.

b. Haga clic en **On** (Activar) para habilitar el servicio FTP.

c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario. Haga clic en el botón **+** para agregar la cuenta:

Nombre de usuario	Contraseña	Permisos
anonymous	anonymous	limitado a **Read** (Lectura) y **List** (Lista)
administrator	cisco	permiso total

d. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón **-** para eliminarla. Cierre la ventana de configuración de la CentralServer.

Paso 2: Configurar el servicio FTP en BranchServer

Repita el paso 1 en **BranchServer**.

Parte 2: Subir un archivo al servidor FTP

Paso 1: Transferir el archivo README.txt de la computadora portátil doméstica a CentralServer

Como administrador de red, debe colocar un aviso en los servidores FTP. El documento se creó en la computadora portátil doméstica y se debe subir a los servidores FTP.

a. Haga clic en **Home Laptop** (Computadora portátil doméstica) y, a continuación, haga clic en la ficha **Desktop** > **Text Editor** (Escritorio > Editor de texto).

b. Abra el archivo **README.txt** y revíselo. Cierre **Text Editor** cuando haya terminado.

Nota: no modifique el archivo porque esto afecta la puntuación.

c. En la ficha **Desktop**, abra la ventana del símbolo del sistema y siga estos pasos:

1) Escriba **`ftp centralserver.pt.pka`**. Espere algunos segundos mientras se conecta el cliente.

Nota: dado que Packet Tracer es una simulación, FTP puede tardar hasta 30 segundos en conectarse la primera vez.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **administrator** (administrador).

3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo **`dir`**. Se muestra el directorio de archivos en **CentralServer**.

4) Transfiera el archivo README.txt: en la petición de entrada `ftp>`, escriba **`put README.txt`**. El archivo README.txt se transfiere de la computadora portátil doméstica a **CentralServer**.

5) Para verificar la transferencia del archivo, escriba **`dir`**. El archivo README.txt ahora figura en el directorio de archivos.

6) Cierre el cliente FTP escribiendo **`quit`**. La petición de entrada se revierte a `PC>`.

Paso 2: Transferir el archivo README.txt de la computadora portátil doméstica a BranchServer

a. Repita el paso 1c para transferir el archivo README.txt a **branchserver.pt.pka**.

b. Cierre las ventanas Command Prompt (Símbolo del sistema) y Home Laptop.

Parte 3: Descargar un archivo del servidor FTP

Paso 1: Transferir README.txt de CentralServer a la PC2

a. Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

1) Escriba **`ftp centralserver.pt.pka`**.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **anonymous** (anónimo)

3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo **`dir.`** El archivo README.txt figura en la parte superior de la lista del directorio.

4) Descargue el archivo README.txt: en la petición de entrada ftp>, escriba **`get README.txt`**. El archivo README.txt se transfiere a la **PC2**.

5) Verifique que la cuenta **anonymous** no tenga permiso para escribir archivos en **CentralServer** escribiendo **`put sampleFile.txt`**. Se muestra el siguiente mensaje de error:

```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...

%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

6) Cierre el cliente FTP escribiendo **`quit`**. La petición de entrada se revierte a `PC>`.

7) Para verificar la transferencia del archivo a la PC2, escriba **`dir`**. El archivo README.txt figura en el directorio.

8) Cierre la ventana de línea de comandos.

b. En la ficha **Desktop**, abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.

c. Cierre **Text Editor** y, luego, cierre la ventana de configuración de la PC2.

Paso 2: Transferir el archivo README.txt de BranchServer al smartphone

Repita el paso 1 para **Smart Phone**, excepto la descarga del archivo README.txt desde **branchserver.pt.pka**.

3.4.31.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.31.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.31.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.32. Practica 32. Acceso a dispositivos de red mediante SSH

3.4.32.1 Objetivo

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Configurar el router para el acceso por SSH

Parte 3: Examinar una sesión de Telnet con Wireshark

Parte 4: Examinar una sesión de SSH con Wireshark

Parte 5: Configurar el switch para el acceso por SSH

Parte 6: Ejecutar SSH desde la CLI del switch

3.4.32.2 Introducción

En el pasado, Telnet era el protocolo de red más común utilizado para configurar dispositivos de red de manera remota. Sin embargo, los protocolos como Telnet no autentican ni encriptan la información entre el cliente y el servidor. Estos permiten que un programa detector de redes intercepte contraseñas y la información de configuración.

Shell seguro (SSH) es un protocolo de red que establece una conexión de emulación de terminal segura a un router u otro dispositivo de red, SSh encripta toda la información que atraviesa el enlace de red y proporciona autenticación de la computadora remota, SSH está reemplazando rápidamente a Telnet como la herramienta de conexión remota preferida por los profesionales de red. SSh se utiliza con mayor frecuencia para conectarse a un dispositivo remoto y ejecutar comandos. Sin embargo, también puede transferir archivos mediante los protocolos de transferencia segura de archivos (SFTP) o de copia segura (SCP) asociados.

Para que SSh funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En esta práctica de laboratorio, habilitará el servidor SSH en un router y luego se conectará a ese router mediante una PC con un cliente

SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP.

En esta práctica de laboratorio, configurará un router para que acepte conectividad de SSH y utilizará Wireshark para capturar y ver sesiones Telnet y SSH. Esto para demostrará la importancia de la encriptación con SSH. También se lo desafiará a que configure un switch para que tenga conectividad de SSH.

3.4.32.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.32.4 Material Y Equipo Necesario

61. Equipo De Cómputo.
62. Conexión A Internet.
63. Packet Tracer

3.4.32.5 Metodología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

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

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar el router.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

d. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

e. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

f. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

g. Encripte las contraseñas de texto no cifrado.

h. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

i. Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.

j. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configurar la PC-A

a. Configure la PC-A con una dirección IP y una máscara de subred.

b. Configure un gateway predeterminado para la PC-A.

Paso 5: Verificar la conectividad de la red.

Haga ping a R1 desde PC-A. Si el ping falla, resuelva los problemas en la conexión.

Parte 2: Configurar el router para el acceso por SSH

Usar Telnet para conectarse a un dispositivo de red es un riesgo de seguridad, porque toda la información se transmite en formato de texto no cifrado. SSH encripta los datos de sesión y proporciona autenticación del dispositivo, por lo que se recomienda SSH para las conexiones remotas. En la parte 2, configurará el router para que acepte conexiones SSH por las líneas VTY.

Paso 1: Configurar la autenticación del dispositivo

El nombre del dispositivo y el dominio se utilizan como parte de la clave de encriptación, cuando se genera. Por lo tanto, estos nombres deben introducirse antes de emitir el comando **crypto key**.

a. Configure el nombre del dispositivo.

```
Router(config)# hostname R1
```

b. Configure el dominio para el dispositivo.

```
R1(config)# ip domain-name ccna-lab.com
```

Paso 2: Configurar el método de la clave de encriptación

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Paso 3: Configurar el nombre de usuario de una base de datos local

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

Nota: el nivel de privilegio 15 otorga al usuario derechos de administrador.

Paso 4: Habilitar SSH en las líneas VTY

a. Habilite Telnet y SSH en las líneas VTY entrantes mediante el comando **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

b. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Paso 5: Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Parte 3: Examinar una sesión de Telnet con Wireshark

En la parte 3, utilizará Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder al R1 mediante Telnet, se registrará y luego emitirá el comando show run en el router.

Nota: si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, debe instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) y PuTTy (www.putty.org).

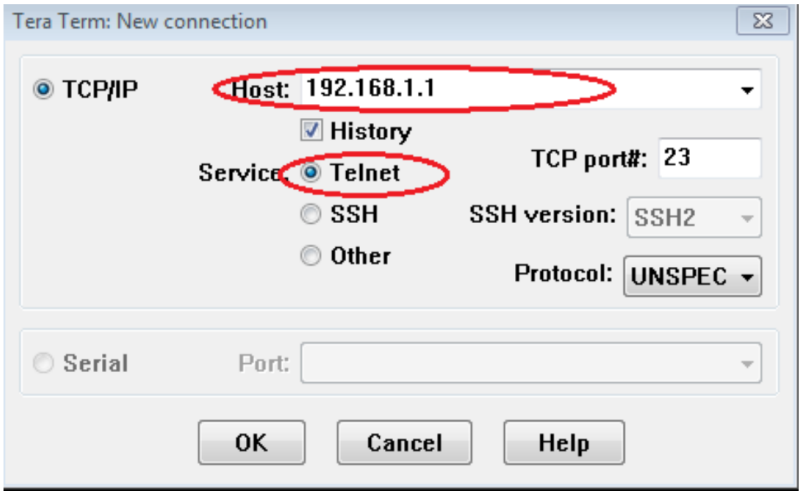
Nota: Telnet no está disponible de manera predeterminada mediante el símbolo del sistema de Windows 7. Para habilitar Telnet a fin de utilizarlo en la ventana del símbolo del sistema, haga clic en **Inicio** > **Panel de control** > **Programas** > **Programas y características** > **Activar o desactivar las características de Windows**. Haga clic en la casilla de verificación **Client Telnet** y, a continuación, haga clic en **Aceptar**.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

Nota: si no puede comenzar la captura en la interfaz LAN, necesitará abrir Wireshark mediante la opción **Run as Administrator** (Ejecutar como administrador).

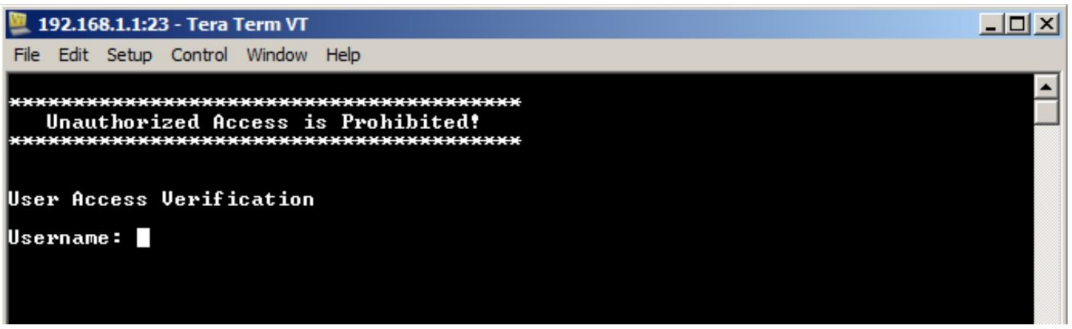
Paso 2: Iniciar una sesión de Telnet en el router

a. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, introduzca **192.168.1.1**.



¿Cuál es el puerto TCP predeterminado para las sesiones de Telnet?

b. En la petición de entrada Username: (Nombre de usuario:), introduzca **admin**, y en la petición de entrada Password: (Contraseña:), introduzca **adminpass**. Estas peticiones de entrada se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando **login local**.



c. Emita el comando **show run**.

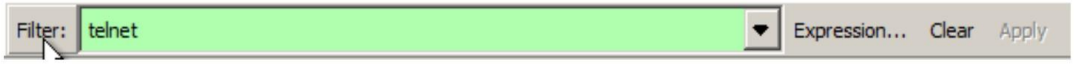
```
R1# show run
```

d. Introduzca **exit** para salir de la sesión de Telnet y de Tera Term.

```
R1# exit
```

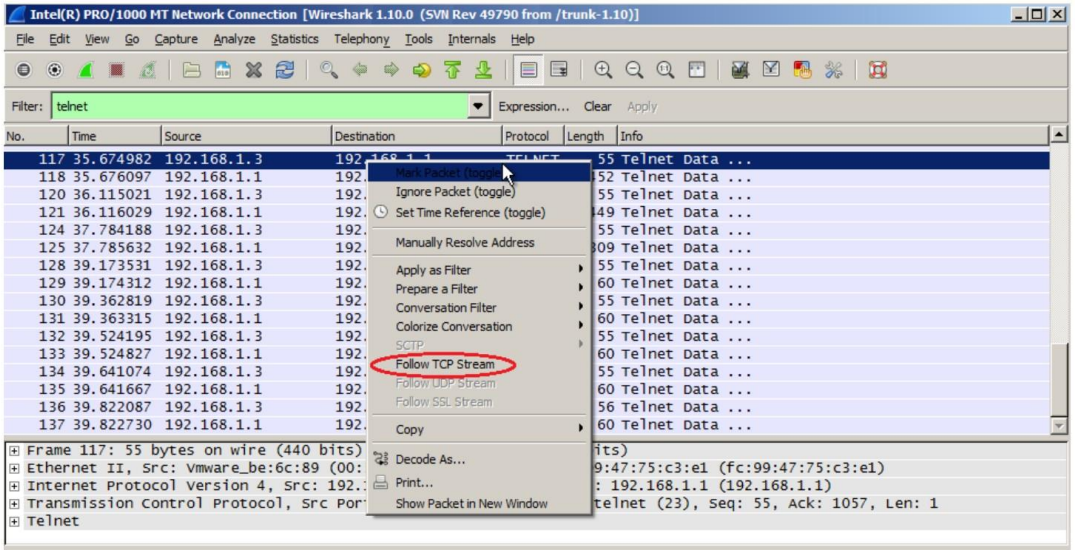
Paso 3: Detener la captura de Wireshark

Paso 4: Aplicar un filtro de Telnet a los datos de captura de Wireshark

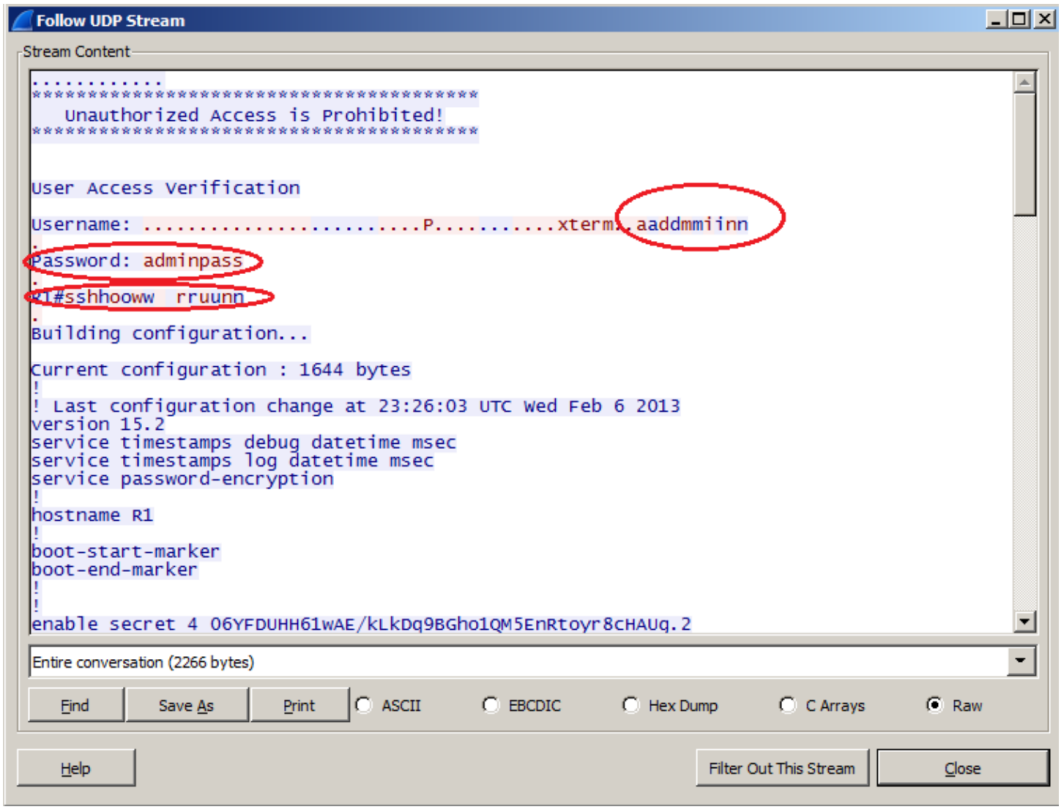


Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón secundario en una de las líneas **Telnet** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).



b. En la ventana Follow TCP Stream, se muestran los datos para su sesión de Telnet con el router. Toda la sesión, incluida la contraseña, se muestra como texto no cifrado. Observe que el nombre de usuario y el comando **show run** que introdujo se muestran con caracteres duplicados. Esto lo causa el ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.



c. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream**, haga clic en **Close** (Cerrar).

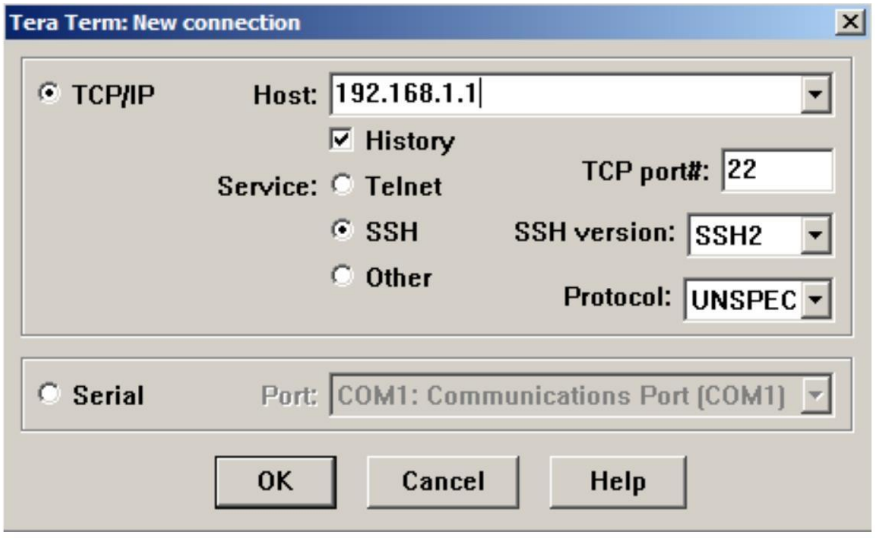
Parte 4: Examinar una sesión de SSH con Wireshark

En la parte 4, utilizará el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

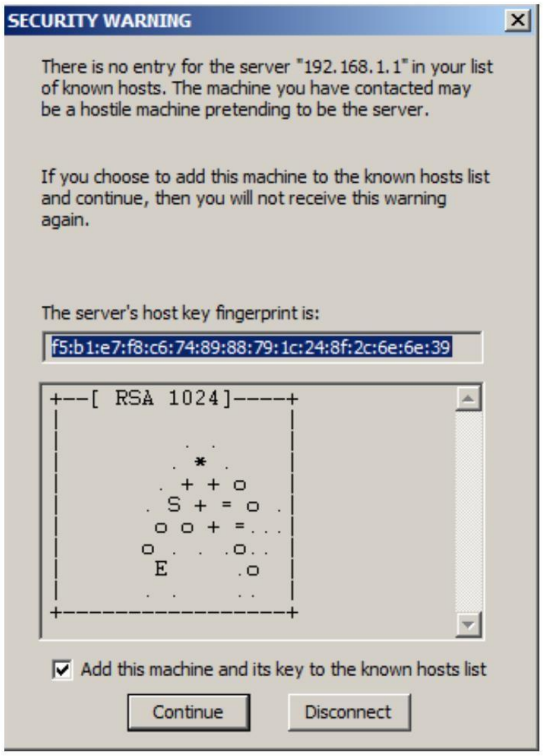
Paso 2: Iniciar una sesión de SSH en el router

a. Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **SSH** esté seleccionado y, a continuación, haga clic en **OK** (Aceptar) para conectarse al router.

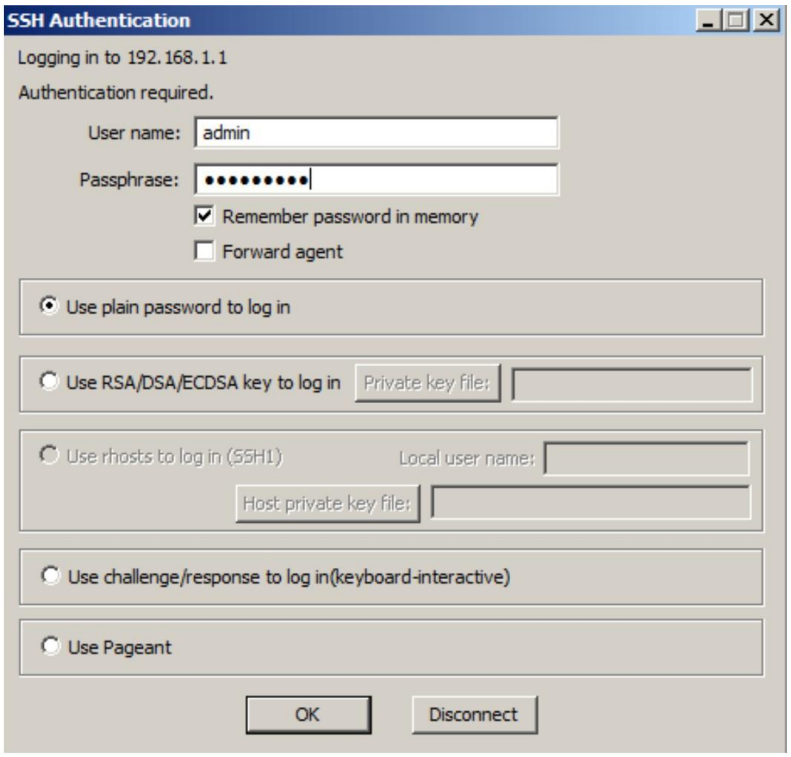


¿Cuál es el puerto TCP predeterminado que se utiliza para las sesiones de SSH?

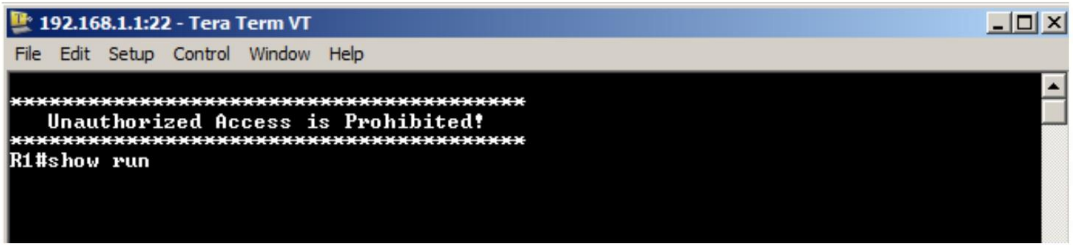
b. La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (ADVERTENCIA DE SEGURIDAD) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y, luego, haga clic en **Continue** (Continuar).



c. En la ventana de la autenticación de SSH, introduzca **admin** en User name (Nombre de usuario) y **adminpass** en Passphrase (Frase de contraseña). Haga clic en **OK** (Aceptar) para registrarse en el router.



d. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En la petición de entrada, emita el comando **show version**.



e. Salga de la sesión de SSH y de Tera Term emitiendo el comando **exit**.

```
R1# exit
```

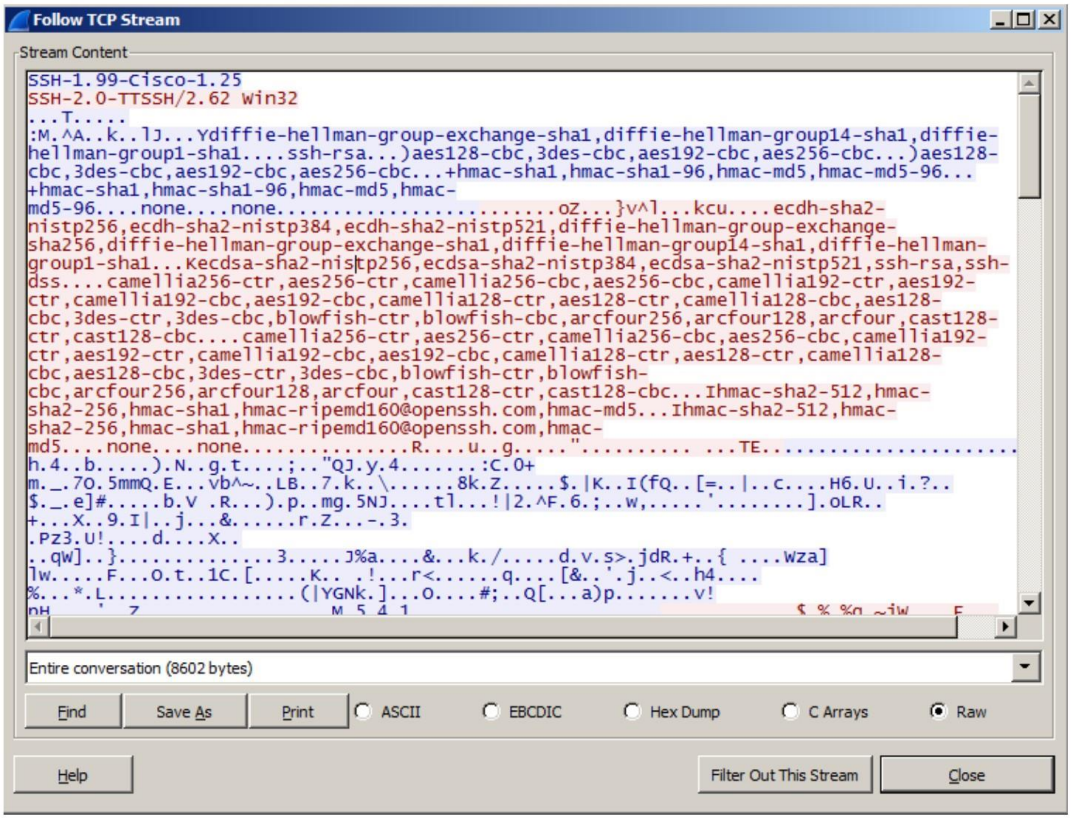
Paso 3: Detener la captura de Wireshark

Paso 4: Aplicar un filtro de SSH a los datos de captura de Wireshark

Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón secundario en una de las líneas **SSHv2** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).

b. Examine la ventana **Follow TCP Stream** de la sesión de SSH. Los datos se encriptaron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.



¿Por qué se prefiere SSH a Telnet para las conexiones remotas?

c. Después de analizar la sesión de SSH, haga clic en **Close** (Cerrar).

d. Cierre Wireshark.

Parte 5: Configurar el switch para el acceso por SSH

En la parte 5, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH en él utilizando Tera Term.

Paso 1: Configurar los parámetros básicos en el switch

Paso 2: Configurar el switch para que tenga conectividad de SSH

A fin de configurar SSH para el switch, utilice los mismos comandos que usó para configurar SSH en el router en la parte 2.

Paso 3: Establecer una conexión SSH al switch

Inicie Tera Term desde la PC-A y, luego, acceda a la interfaz SVI en el S1 mediante SSH.

Paso 4: Resuelva cualquier problema que se presente.

¿Puede establecer una sesión de SSH con el switch?

Parte 6: Ejecutar SSH desde la CLI del switch

El cliente de SSH está incorporado en Cisco IOS y puede ejecutarse desde la CLI. En la parte 6, ejecutará una conexión SSH al router desde la CLI del switch.

Paso 1: Ver los parámetros disponibles para el cliente de SSH de Cisco IOS

Utilice el signo de interrogación (**?**) para mostrar las opciones de parámetros disponibles con el comando **ssh**.

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Paso 2: Acceder al router R1 mediante SSH desde el S1

a. Cuando accede al R1 mediante SSH, debe utilizar la opción **–l admin**. De esta manera, podrá iniciar sesión como usuario **admin**. Cuando se le solicite, introduzca **adminpass** en el campo Password (contraseña).

```
S1# ssh -l admin 192.168.1.1
Password:
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************


R1#
```

b. Para volver al S1 sin cerrar la sesión de SSH para el R1, presione las teclas **Ctrl+Mayús+6.** Suelte las teclas **Ctrl+Mayús+6** y presione **x.** Debería ver la ventana de petición de entrada del modo EXEC privilegiado del switch.

```
R1#
S1#
```

c. Para volver a la sesión de SSH en el R1, presione Entrar en una línea en blanco de la CLI. Es posible que deba presionar Entrar por segunda vez para ver la petición de entrada de la CLI del router.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. Para finalizar la sesión de SSH en el R1, escriba **exit** en la petición de entrada del router.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

¿Qué versiones de SSH se admiten en la CLI?

Reflexión

¿Cómo proporcionaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

3.4.32.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.32.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.32.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.33 Práctica 33. Protección de dispositivos de red

3.4.33.1 Objetivo

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Configurar medidas bacias de seguridad en el router

Parte 3: Configurar medidas básicas de seguridad en el switch

3.4.33.2 Introducción

Se recomienda que todos los dispositivos de red se configuren, al menos, con un conjunto mínimo de comandos de seguridad conforme a las practicas recomendadas. Esto incluye dispositivos para usuarios finales, servidores y dispositivos de red, como routers y switches.

En esta práctica de laboratorio, configurará los dispositivos de red en la topología a fin de que acepten sesiones de SSH para la administración remota. También utilizará la CLI del IOS para configurar medidas de seguridad básicas conforme a las practicas recomendadas. Luego, probará las medidas de seguridad para verificar que estén implementadas de manera apropiada y que funcionen correctamente.

3.4.33.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.33.4 Material Y Equipo Necesario

64. Equipo De Cómputo.

65. Conexión A Internet.

66. Packet Tracer

3.4.33.5 Metodología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

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

Conecte los dispositivos que se muestran en la topología y realice el cableado según sea necesario.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar el router.

Consulte la práctica de laboratorio anterior para obtener ayuda con los comandos necesarios para SSH.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Asigne el nombre R1 al router.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

f. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

j. Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.

k. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configure el switch.

a. Acceda al switch mediante el puerto de consola y habilite al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Asigne el nombre S1 al switch.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

f. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

j. Configure la SVI predeterminada con la información de dirección IP incluida en la tabla de direccionamiento.

k. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Configurar medidas básicas de seguridad en el router

Paso 1: Aportar seguridad a las contraseñas

Un administrador debe asegurar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Entre estas pautas, se podría incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

Nota: las pautas de prácticas recomendadas requieren el uso de contraseñas seguras, como las que se muestran aquí, en ambientes de producción. Sin embargo, las otras prácticas de laboratorio en este curso utilizan las contraseñas cisco y class para facilitar la realización de las prácticas.

a. Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas.

```
R1(config)# enable secret Enablep@55
```

b. Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas.

```
R1(config)# security passwords min-length 10
```

Paso 2: Habilitar conexiones SSH

a. Asigne el nombre **CCNA-lab.com** al dominio.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configure la entrada de transporte para las líneas vty de modo que acepten conexiones SSH, pero no permitan conexiones Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

a. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante el lapso especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra la sesión del usuario en forma automática después de un tiempo especificado. Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. El comando siguiente impide los intentos de inicio de sesión por fuerza bruta. Si alguien falla en dos intentos en un período de 120 segundos, el router bloquea los intentos de inicio de sesión por 30 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
R1(config)# login block-for 30 attempts 2 within 120
```

¿Qué significa **2 within 120** en el comando anterior?

¿Qué significa **block-for 30** en el comando anterior?

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

Los puertos del router están deshabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado administrativamente inactivo. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en el estado administratively down (administrativamente inactivo) se deben deshabilitar por medio del comando **shutdown** en el modo de configuración de interfaz.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

a. Utilice Tera Term para acceder al R1 mediante Telnet.

¿R1 acepta la conexión Telnet?

¿Por qué o por qué no?

b. Utilice Tera Term para acceder al R1 mediante SSH.

¿R1 acepta la conexión SSH?

c. Escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea después de dos intentos.

¿Qué ocurrió después del segundo inicio de sesión fallido?

d. Desde su sesión de consola en el router, emita el comando **show login** para ver el estado de inicio de sesión. En el siguiente ejemplo, el comando **show login** se emitió dentro del período de bloqueo de inicio de sesión de 30 segundos y muestra que el router está en modo silencioso. El router no aceptará ningún intento de inicio de sesión por 14 segundos más.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. Cuando hayan pasado los 30 segundos, vuelva a acceder al R1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.

Una vez que inició sesión correctamente, ¿qué se mostró?

f. Ingrese al modo EXEC privilegiado y utilice la contraseña **Enablep@55**.

Si escribe esta contraseña incorrectamente, ¿se desconectará la sesión de SSH después de dos intentos fallidos en el lapso de 120 segundos?

¿Por qué o por qué no?

g. Emita el comando **show running-config** en la petición de entrada del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Parte 3: Configurar medidas básicas de seguridad en el switch

Paso 1: Aportar seguridad a las contraseñas en el switch

Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas de contraseña segura.

```
S1(config)# enable secret Enablep@55
```

Nota: el comando de seguridad **password min-length** no está disponible en el switch 2960.

Paso 2: Habilitar conexiones SSH

a. Asigne el nombre **CCNA-lab.com** al dominio.

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. Configure la entrada de transporte para las líneas vty para permitir las conexiones SSH, pero no las conexiones Telnet.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

a. Haga que el switch cierre sesión en una línea que haya estado inactiva durante 10 minutos.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Para impedir intentos de inicio de sesión por fuerza bruta, configure el switch para que bloquee el acceso de inicio de sesión por 30 segundos en caso de que haya dos intentos fallidos en un período de 120 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

Los puertos del switch están habilitados de manera predeterminada. Desactive todos los puertos que no estén en uso en el switch.

a. Para verificar el estado de los puertos del switch, utilice el comando **show ip interface brief**.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
```

```
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. Utilice el comando **interface range** para desactivar varias interfaces a la vez.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Verifique que todas las interfaces inactivas tengan un estado administrativamente inactivo.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
```

```
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

a. Verifique que Telnet esté deshabilitado en el switch.

b. Acceda al switch mediante SSH y escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea.

c. Cuando hayan pasado los 30 segundos, vuelva a acceder al S1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.

¿Apareció el anuncio después de iniciar sesión correctamente?

d. Ingrese al modo EXEC privilegiado utilizando la contraseña **Enablep@55**.

e. Emita el comando **show running-config** en la petición de entrada del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Reflexión

1. En la configuración básica de la parte 1, se introdujo el comando **password cisco** para las líneas de consola y vty. ¿Cuándo se utiliza esta contraseña después de haberse aplicado las medidas de seguridad conforme a las prácticas recomendadas?

2. ¿Se vieron afectadas por el comando **security passwords min-length 10** las contraseñas configuradas previamente con menos de 10 caracteres?

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

3.4.33.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.33.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.33.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.34 Práctica 34. Prueba de la conectividad con traceroute

3.4.34.1 Objetivo

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert.

Parte 2: Comparar con el comando traceroute en un router.

3.4.34.2 Introducción

Esta actividad está diseñada para ayudarlo a llevar a cabo la resolución de problemas de conectividad de red utilizando comandos para rastrear la ruta de origen a destino. Debe examinar el resultado de tracert (el comando de Windows) y traceroute (el comando de 1OS) mientras los paquetes atraviesan la red y determinar la causa de un problema de red. Una vez que se corrija el problema, utilice los comandos tracert y traceroute para verificar la finalización.

3.4.34.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.34.4 Material Y Equipo Necesario

- Equipo De Cómputo.
- Conexión A Internet.
- Packet Tracer

3.4.34.5 Metodología

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert.

Paso 1: Enviar un ping de un extremo al otro de la red. Haga clic en PC1 y abra el símbolo del sistema. Haga ping a PC3 en 10.1.0.2. ¿Qué mensaje se muestra como resultado del ping?

Paso 2: Rastrear la ruta de PC1 para determinar dónde falla la conectividad

1. En el símbolo del sistema de la PC1. introduzca el comando tracert 10.1.0.2.
2. Cuando reciba el mensaje Request timed out (Tiempo de espera agotado), presione Ctrl+C. ¿Cuál fue la primera dirección IP indicada en el resultado del comando tracert?
3. Observe los resultados del comando tracert. ¿Cuál es la última dirección que se alcanzó con el comando tracert?

Paso 3: Corregir el problema de red

1. Compare la última dirección que se alcanzó con el comando tracert con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de falla. ¿Qué dispositivos tienen direcciones configuradas para la red donde ocurrió la falla?
2. Haga clic en RouterC y, a continuación, haga clic en la ficha CLI.
3. ¿Cuáles el estado de las interfaces?

4. Compare las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo común?
5. Realice los cambios necesarios para restaurar la conectividad, pero no modifique las subredes. ¿Cuál es la solución?

Paso 4: Verificar que la conectividad de extremo a extremo esté establecida

a. En el símbolo del sistema de la PC4, introduzca el comando tracert 10.1.0.2.

b. Observe el resultado del comando tracert. ¿El comando funcionó correctamente?

Parte 2: Comparar con el comando traceroute en un router

a. Haga clic en RouterA y, a continuación, haga clic en la ficha CLI.

b. Introduzca el comando traceroute 10.1.0.2. ¿El comando se completó correctamente?

C. Compare el resultado del comando traceroute del router con el del comando tracert de la PC. ¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió?

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Probar la conectividad de extremo a extremo con el comando **tracert**	Paso 1	10	
	Paso 2b	10	
	Paso 2c	10	
	Paso 3a	10	
	Paso 3c	10	
	Paso 3d	10	
	Paso 3e	10	
	Paso 4b	10	
Total de la parte 1		**80**	
Parte 2: Comparar con el comando **traceroute** en un router	a	10	
	b	10	
Total de la parte 2		**20**	
Puntuación total		**100**	

.

3.4.34.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.34.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.34.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.7 35. Prueba de la latencia de red con los comandos ping y traceroute

3.4.35.1 Objetivo

Parte 1: Utilizar el comando ping para registrar la latencia de red

Parte 2: Utilizar el comando traceroute para registrar la latencia de red

3.4.35.2 Introducción

El objetivo de esta actividad de laboratorio es medir y evaluar la latencia de red en el tiempo y durante diferentes momentos del día para capturar una muestra representativa de la actividad típica de la red. Esto se logrará mediante el análisis del retardo del retorno desde una computadora remota con el comando ping. El tiempo de retraso del retorno, medido en milisegundos, se resume calculando la latencia promedio (media) y el intervalo (máximo y mínimo) del tiempo de retraso.

3.4.35.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

4.1 Normas y estándares.

4.2 Componentes y herramientas de Instalación.

3.4.35.4 Material Y Equipo Necesario

67. Equipo De Cómputo.
68. Conexión A Internet.
69. Packet Tracer

3.4.35.5 Metodología

Parte 1: Utilizar el comando ping para registrar la latencia de red

En la parte 1, examinará la latencia de red a varios sitios Web en distintas partes del mundo. Este proceso se puede utilizar en una red de producción empresarial para crear una línea de base de rendimiento.

Paso 1: Verificar la conectividad

Haga ping a los siguientes sitios Web de registros regionales de Internet (RIR) para verificar la conectividad:

```
C:\Users\User1> ping www.arin.net
C:\Users\User1> ping www.lacnic.net
C:\Users\User1> ping www.afrinic.net
C:\Users\User1> ping www.apnic.net
```

Paso 2: Recopilar los datos de red

Recopilará una cantidad de datos suficiente para calcular estadísticas sobre el resultado del comando ping mediante el envío de 25 solicitudes de eco a cada dirección del paso 1. Registre los resultados para cada sitio Web en archivos de texto.

a. En el símbolo del sistema, escriba ping para enumerar las opciones disponibles.

```
C:\Users\User1> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
<resultado omitido>
```

b. Si utiliza el comando ping con la opción de cuenta, podrá enviar 25 solicitudes de eco al destino, como se muestra a continuación. Además, creará un archivo de texto con el nombre arin.txt en el directorio actual. Este archivo de

texto contendrá los resultados de las solicitudes de eco.

c. Repita el comando ping para los otros sitios Web.

Paso 3: Verificar la recopilación de datos

Para ver los resultados en el archivo creado, introduzca el comando more en el símbolo del sistema.

```
C:\Users\User1> more arin.txt

Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
<resultado omitido>
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45

Ping statistics for 192.149.252.75:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Para verificar que los archivos se crearon, utilice el comando dir para enumerar los archivos en el directorio. También se puede utilizar el carácter comodín * para filtrar solo los archivos de texto.

```
C:\Users\User1> dir *.txt
Volume in drive C is OS
 Volume Serial Number is 0A97-D265

 Directory of C:\Users\User1

02/07/2013  12:59 PM             1,642 afrinic.txt
02/07/2013  01:00 PM             1,615 apnic.txt
02/07/2013  12:40 PM             1,641 arin.txt
02/07/2013  12:58 PM             1,589 lacnic.txt
               4 File(s)          6,487 bytes
               0 Dir(s)  34,391,453,696 bytes free
```

Registre sus resultados en la siguiente tabla:

	Mínimo	Máximo	Promedio
www.afrinic.net			
www.apnic.net			
www.arin.net			
www.lacnic.net			

Compare los resultados de retardo. ¿De qué manera afecta el retardo la ubicación geográfica?

Parte 2: Utilizar el comando traceroute para registrar la latencia de red

Según cuál sea el tamaño del ISP y la ubicación de los hosts de origen y destino, las rutas rastreadas pueden atravesar muchos saltos y una cantidad de ISP diferentes. Los comandos traceroute también pueden utilizarse para observar la latencia de red. En la parte 2, se utiliza el comando tracert para rastrear la ruta a los destinos utilizados en la parte 1.

El comando tracert utiliza paquetes ICMP de TTL superado y respuestas de eco ICMP para rastrear la ruta.

Paso 1: Utilizar el comando tracert y registrar el resultado en archivos de texto

Copie los siguientes comandos para crear los archivos de traceroute:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Paso 2: Utilizar el comando more para examinar la ruta rastreada

Utilice el comando more para acceder al contenido de estos archivos:

```
C:\Users\User1> more traceroute_arin.txt

Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    11 ms    12 ms    11 ms  10.39.0.1
  3    10 ms    15 ms    11 ms  172.21.0.116
  4    19 ms    10 ms    11 ms  70.169.73.90
  5    13 ms    10 ms    11 ms  chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]
  6    72 ms    71 ms    70 ms  mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
  7    72 ms    71 ms    72 ms  68.100.0.146
  8    74 ms    83 ms    73 ms  172.22.66.29
  9    75 ms    71 ms    73 ms  172.22.66.29
 10    74 ms    75 ms    73 ms  wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]
 11    71 ms    71 ms    71 ms  host-252-131.arin.net [192.149.252.131]
 12    73 ms    71 ms    71 ms  www.arin.net [192.149.252.75]

Trace complete.
```

En este ejemplo, demoró menos de 1 ms recibir una respuesta del gateway predeterminado (192.168.1.1) En el conteo de saltos 6, la ida y vuelta a 68.1.1.7 requirió un promedio de 71 ms. Para la ida y vuelta al destino final en www.arin.net, se requirió un promedio de 72 ms.

Entre las líneas 5 y 6, el retardo de red es mayor, según lo indica el aumento del tiempo de ida y vuelta de un promedio de 11 a 71 ms

b. Realice el mismo análisis con el resto de los resultados del comando tracert.

¿A qué conclusión puede llegar con respecto a la relación entre el tiempo de ida y vuelta y la ubicación geográfica?

Reflexión

1. Los resultados de tracert y ping pueden proporcionar información importante sobre la latencia de red. ¿Qué debe hacer si desea una representación precisa de la línea de base de la latencia de su red?

2. ¿Cómo puede utilizar la información de línea de base?

3.4.35.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.35.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.35.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/

3.4.36 Práctica 36. Administración de los archivos de configuración del router con software de emulación de terminal

3.4.36.1 Objetivo

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

Parte 3: Utilizar un archivo de configuración de respaldo para restaurar un router

3.4.36.2 Introducción

Se recomienda mantener archivos de configuración de respaldo de routers y switches en caso de que sea necesario restaurar una configuración anterior. El software de emulación de terminal puede utilizarse para realizar una copia de seguridad o para restaurar fácilmente un archivo de configuración de router o switch.

En esta práctica de laboratorio, utilizará Tera Term para realizar una copia de seguridad de un archivo de configuración en ejecución del router, eliminar el archivo de configuración de inicio del router, volver a cargar el router y, luego, restaurar la configuración del router faltante a partir del archivo de configuración de respaldo.

3.4.36.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

5.1 Memoria técnica

5.2 Análisis de necesidades y requerimientos.

3.4.36.4 Material Y Equipo Necesario

70. Equipo De Cómputo.

71. Conexión A Internet.

72. Packet Tracer

3.4.36.5 Metodología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router

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

Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.

Paso 2: Configurar los parámetros de red de la PC-A según la tabla de direccionamiento

Paso 3: Inicialice y vuelva a cargar el router y el switch.

Paso 4: Configurar el router.

a. Acceda al router mediante el puerto de consola e introduzca el modo de configuración global.
b. Establezca R1 como nombre del router.
c. Desactive la búsqueda del DNS.
d. Asigne class como la contraseña encriptada de EXEC privilegiado.
e. Asigne cisco como la contraseña de consola y habilite el inicio de sesión.
f. Asigne cisco como la contraseña de viy y habilite el inicio de sesión.
g. Encripte las contraseñas de texto no cifrado.
h. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
i. Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.
j. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 5: Configure el switch.

a. Acceda al switch mediante el puerto de consola e ingrese al modo de configuración global.
b. Establezca S1 como nombre del switch.

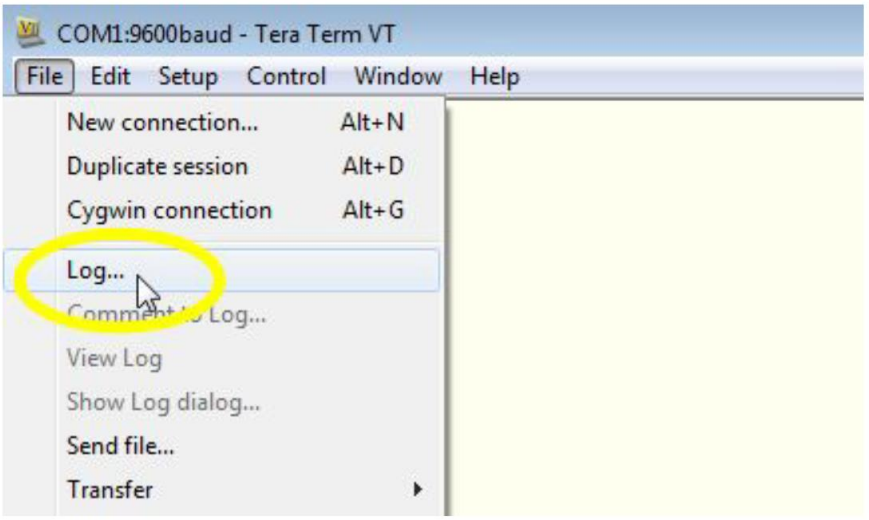
c. Desactive la búsqueda del DNS.
d. Asigne class como la contraseña encriptada de EXEC privilegiado.
e. Asigne cisco como la contraseña de consola y habilite el inicio de sesión.
f. Asigne cisco como la contraseña de vty y habilite el inicio de sesión.
g. Encripte las contraseñas de texto no cifrado.
h. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
i. Configure la interfaz de administración predeterminada SVI con la información de dirección la tabla de direccionamiento.
j. Configure el gateway predeleminado del swilca.
k. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

Paso 1: Establecer una sesión de consola de Tera Term con el router

Inicie el programa Tera Term y, en la ventana New Connection (Conexión nueva), seleccione el botón de opción Serial y el puerto de comunicaciones apropiado para su PC (es decir, COM1).

a. En Tera Term, presione Entrar para conectarse al router.
b. En el menú File (Archivo), seleccione Log... (Registrar... y guarde el archivo teraterm.log en el escritorio. Asegúrese de que las casilas de verificación Append (Anexar) y Plain text (Texto sin formato) estén activadas (marcadas).



c. El archivo de registro de Tera Term creará un registro de cada comando emitido y de cada resultado visualizado.

Paso 2: Mostrar la configuración en ejecución del router

a. Utilice la contraseña de consola para iniciar sesión en el router.
b. Ingrese al modo EXEC privilegiado.
c. Ingrese el comando show running-config.

d. Continúe presionando la barra espaciadora cuando se muestre --More-- (Más), hasta que vuelva a ver la petición de entrada R1% del router.
e. Haga clic en el ícono Tera Term: Log (Tera Term: registro) en la barra de tareas. Haga clic en Close (Cerrar) para finalizar la sesión de registro.

Parte 3: Utilizar un archivo de configuración de respaldo para restaurar un router

Paso 1: Borrar la configuración de inicio del router y volver a cargar

a. En el modo EXEC privilegiado, elimine la configuración de inicio

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

b. Recargue el router.

```
R1# reload
Proceed with reload? [confirm]
```

d. En la petición de entrada System Configuration Dialog (Cuadro de diálogo de configuración del sistema), escriba no. Aparecerá una petición de entrada de router que indica que hay un router sin configurar.
e. Ingrese al modo EXEC privilegiado e introduzca un comando show running-config para verificar que todas las configuraciones anteriores se hayan borrado.

Paso 2: Editar el archivo de configuración de respaldo guardado a fin de prepararlo para restablecer la configuración del router

Para restaurar la configuración del router desde un archivo de configuración en ejecución de respaldo guardado, debe editar el texto

a. Abra el archivo de texto teraterm.log.

b. Elimine cada aparición de --More-- en el archivo de texto.

c. Elimine las líneas iniciales del archivo de configuración de respaldo, de modo que la primera línea comience con el primer comando de configuración, como se muestra a continuación.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

d. Reemplace la contraseña secreta encriptada

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

e. Cambie a:

```
enable secret class
```

f. En las líneas para la interfaz GigabitEthemnet0/1, inserte una línea nueva para habilitar la interfaz.

```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

g. Cambie a:

Cambie a:

```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
```

h. Cambie la configuración del anuncio del mensaje del día (MOTD) para insertar caracteres delimitadores como si introdujera el comando en la línea de comandos.

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

Change to:

```
banner motd " Unauthorized Access is Prohibited! "
```

i. En las secciones line con 0 y viy 0 4, reemplace la contraseña encriptada.

```
line con 0
 password 7 104D000A0618
line vty 0 4
 password 7 104D000A0618
```

j. Cambie a:

Cambie a:

```
line con 0
 password cisco
line vty 0 4
 password cisco
```

k. Después de realizar todas las ediciones al archivo de configuración de respaldo, guarde los cambios con el nombre de archivo R1-config-backup.

Paso 3: Restaurar la configuración del router

Puede restaurar la configuración en ejecución editada directamente en la terminal de consola en el modo de configuración global del router; las configuraciones se introducen como si fueran comandos escritos de forma individual en la petición de entrada de comandos.

a. Ingrese al modo de configuración global desde la conexión de consola de Tera Term al router.
b. En el menú File (Archivo), seleccione Send file... (Enviar archivo).

c. Localice R1-config-backup y seleccione Open (Abrir).
d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copy running-config startup-config
```

e. Verifique la nueva configuración en ejecución

Paso 4: Realizar una copia de seguridad y restaurar el switch

Vuelva al comienzo de la parte 2 y siga los mismos pasos para realizar una copia de seguridad de la configuración del switch y restaurarla

Reflexión

¿Por qué cree que es importante utilizar un editor de texto en lugar de un procesador de textos para copiar y guardar las configuraciones de los comandos?

3.4.36.6 Sugerencias Didácticas

- Para esta actividad se sugiere que el alumno cuente con la versión 7.8 de Packet Tracer.

3.4.36.7 Reporte Del Alumno

El alumno debe de realizar la actividad detallando paso a paso la elaboración de esta, incluyendo capturas, mediante el formato de un reporte de prácticas dando detalle de los resultados obtenidos, así como su conclusión y aprendizajes obtenidos.

3.4.36.8 Bibliografías

- *Cisco Networking Academy: Learn Cybersecurity, Python & more*. (2023b, agosto 25). Networking Academy. https://www.netacad.com/