Universidad Continental

Redes

Guías de Laboratorio

Visión

Ser una de las 10 mejores universidades privadas del Perú al año 2020, reconocidos por nuestra excelencia académica y vocación de servicio, líderes en formación integral, con perspectiva global; promoviendo la competitividad del país.

Misión

Somos una universidad privada, innovadora y comprometida con el desarrollo del Perú, que se dedica a formar personas competentes, íntegras y emprendedoras, con visión internacional; para que se conviertan en ciudadanos responsables e impulsen el desarrollo de sus comunidades, impartiendo experiencias de aprendizaje vivificantes e inspiradoras; y generando una alta valoración mutua entre todos los grupos de interés.

Índice

Guía de práctica N° 1

Elementos de una red

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ……/……/…….	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo** (de la práctica)**:**
   Verá la forma en que se conecta a través de Internet a aquellos lugares, personas o empresas con los cuales interactúa a diario. Después de reflexionar y bosquejar la topología de su hogar o lugar de estudios, puede sacar conclusiones acerca de Internet que tal vez no haya considerado antes de esta actividad.

2. **Fundamento Teórico**

   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** (o **tracert**) 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 de internetworks. Cada router representa un punto en el que una red se conecta a otra y a través del cual se envió el paquete de datos. La cantidad de routers se conoce 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 qué 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 la información disponible en línea para mostrar la ruta gráficamente.

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

Si tiene problemas para descargar o instalar VisualRoute, solicite ayuda al instructor. Asegúrese de descargar la edición Lite.

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Download
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Download

3. Equipos, Materiales

- **1 Pc con Acceso a Internet sin restricciones.**
- Papel y lápices o bolígrafos (si los estudiantes crean una copia impresa)

4. Procedimientos:

Primero: Las redes constan de varios componentes diferentes.

Información básica/Situación

Dibuje y rotule un mapa de Internet tal como la interpreta en el presente. Incluya la ubicación de su hogar, lugar de estudios o universidad y del cableado, los equipos y los dispositivos correspondientes, entre otros. Es posible que desee incluir algunos de los siguientes elementos:

- Dispositivos o equipos
- Medios (cableado)
- Direcciones o nombres de enlaces
- Orígenes y destinos
- Proveedores de servicios de Internet

Al finalizar, conserve el trabajo en formato impreso, ya que se utilizará para referencia futura al final de este capítulo. Si se trata de un documento electrónico, guárdelo en una ubicación del servidor proporcionada por el instructor. Esté preparado para compartir y explicar su trabajo en clase.

Aquí verá un ejemplo que lo ayudará a comenzar: http://www.kk.org/internet-mapping.

responda a las siguientes Preguntas:

1. Después de revisar los dibujos de sus compañeros de clase, ¿había dispositivos informáticos que podría haber incluido en su diagrama? Si la respuesta es afirmativa, indique cuáles y por qué.

   _____

   _____

2. Después de revisar los dibujos de sus compañeros de clase, ¿qué similitudes y diferencias encontró en los diseños de algunos modelos? ¿Qué modificaciones le haría a su dibujo después de revisar los otros?

   _____

   _____

3. ¿De qué manera los íconos en el dibujo de una red podrían organizar el proceso mental y facilitar el aprendizaje? Justifique su respuesta.

   _____

   _____

   _____

PASO 2: Probar La Conectividad De Red Mediante El Comando Ping

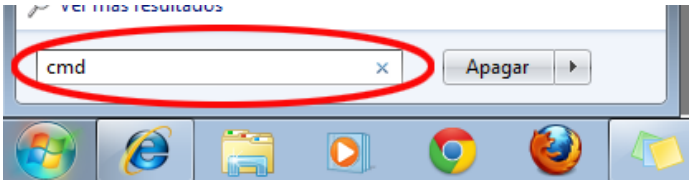
Con una conexión a Internet, usará tres utilidades de rastreo de rutas para examinar la ruta de Internet hacia las redes de destino. Esta actividad debe realizarse en una PC que tenga acceso a Internet y acceso a una línea de comandos. Primero, usará la utilidad tracert integrada en Windows. En segundo lugar, utilizará una herramienta traceroute basada en la Web (http://www.subnetonline.com/pages/network-tools/online-traceroute.php). Finalmente, utilizará el programa traceroute de VisualRoute.

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 línea de resultados, aparece el nombre de dominio completamente calificado (FQDN) 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.

e. 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
```

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.ª 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
```

Todos estos pings se ejecutaron desde una PC ubicada en los EE. UU. ¿Qué sucede con el tiempo promedio de ping en milisegundos cuando los datos viajan dentro del mismo continente (América del Norte) en comparación con datos que viajan desde América del Norte hacia distintos continentes?

_____

¿Qué se puede destacar de los pings que se enviaron al sitio Web europeo?

_____

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 posibilidad 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**

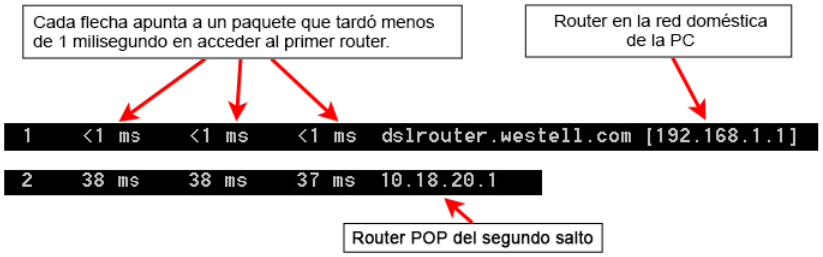
d. Interpretación de los resultados de **tracert**.

Las rutas rastreadas pueden atravesar muchos saltos y distintos proveedores de servicios de Internet (ISP), 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 x.x.x.x) 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 retorno 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 PC 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. 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 o es un ISP diferente? Utilice 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?

_____

_____

g. 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.
```

¿Qué sucede en el salto 7?

_____

_____

_____

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 http://www.subnetonline.com/pages/network-tools/online-tracepath.php para rastrear la ruta a los siguientes sitios Web:

www.cisco.com

www.afrinic.net

Capture y guarde el resultado en el bloc de notas.

¿En qué se diferencia el comando traceroute cuando se accede a www.cisco.com 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.

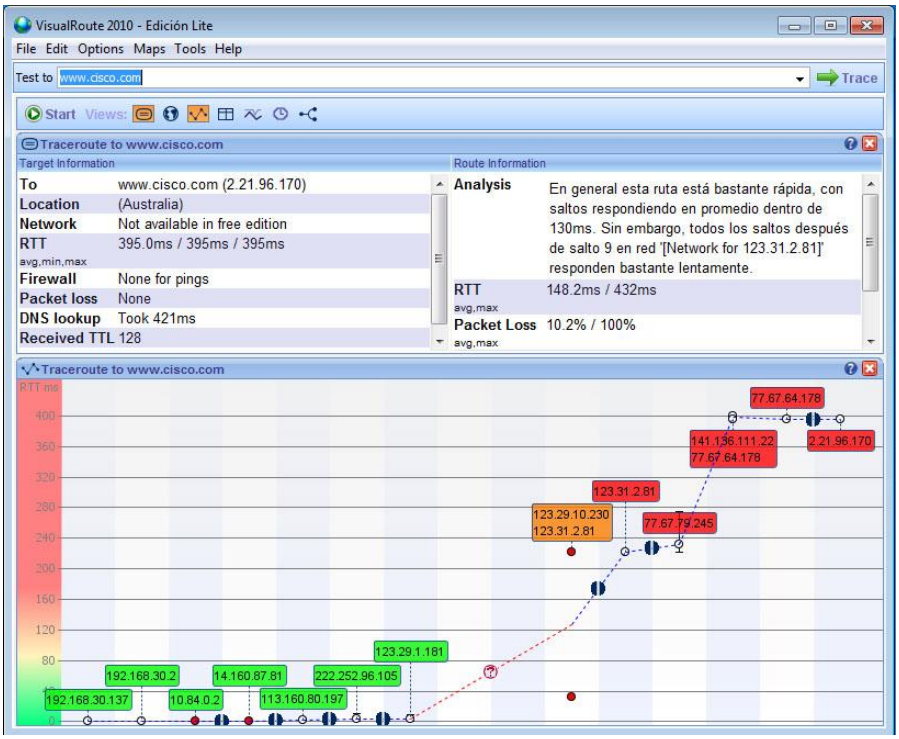
a. Si VisualRoute Lite Edition no está instalado, descárguelo del enlace siguiente:

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

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.



Parte 4: Comparar los resultados de traceroute

Compare los resultados de traceroute para www.cisco.com de las partes 2 y 3.

Paso 1: Indique la ruta a www.cisco.com que se obtiene al utilizar el comando tracert.

_____

_____

Paso 2: Indique la ruta a www.cisco.com que se obtiene al utilizar la herramienta basada en la Web que se encuentra en subnetonline.com.

_____

_____

Paso 3: Indique la ruta a www.cisco.com que se obtiene al utilizar VisualRoute Lite Edition.

_____

_____

¿Todas las utilidades de traceroute usaron las mismas rutas para llegar a www.cisco.com? ¿Por qué o por qué no?

_____

_____

5. Resultados

Ahora que se analizó traceroute mediante tres herramientas diferentes (tracert, interfaz Web y VisualRoute), ¿VisualRoute proporciona algún detalle que las otras dos herramientas no ofrezcan?

6. Conclusiones

6.1 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.

7. Sugerencias y /o recomendaciones

Averigüé acerca el mapa de Internet de Fibra óptica mundial.

8. Referencias bibliográficas consultadas y/o enlaces recomendados:

• Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 2

Establecimiento de una sesión de consola con Tera Term

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo** (de la práctica)**:**
   - Conectarse a un switch Cisco mediante un cable serial de consola.
   - Establecer una sesión de consola utilizando un emulador de terminal, como Tera Term.
   - Utilizar los comandos **show** para mostrar la configuración del dispositivo.
   - Configurar el reloj del switch

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cable de consola (DB-9 a RJ-45) para configurar el switch o el router a través del puerto de consola RJ-45
- Cable mini-USB para configurar el router a través del puerto de consola USB

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.

2. **Fundamento Teórico**

Información básica/Situación

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 cómo 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 esta práctica de laboratorio, solo mostrará los parámetros y configurará el reloj.

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

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

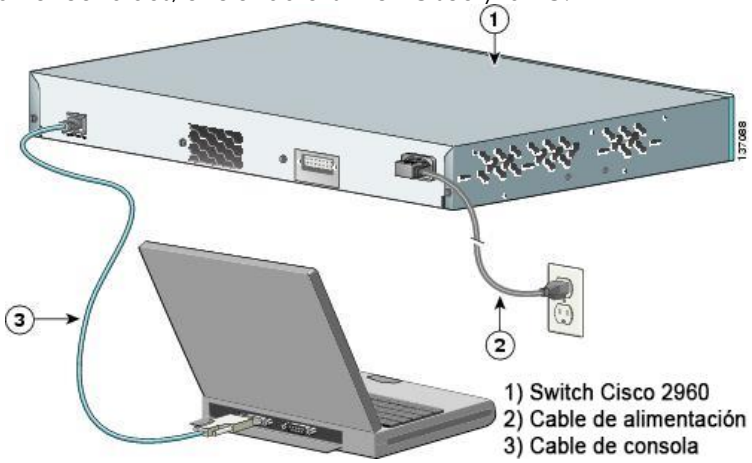
3. Equipos, Materiales y Reactivos

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cable de consola (DB-9 a RJ-45) para configurar el switch o el router a través del puerto de consola RJ-45
- Cable mini-USB para configurar el router a través del puerto de consola USB

4. Procedimientos:

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.



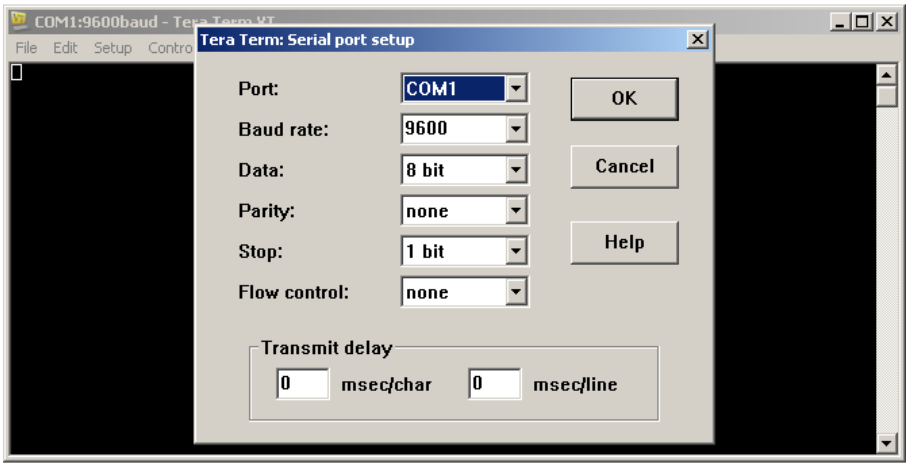
Paso 2: Configurar Tera Term para establecer una sesión de consola con el switch

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.

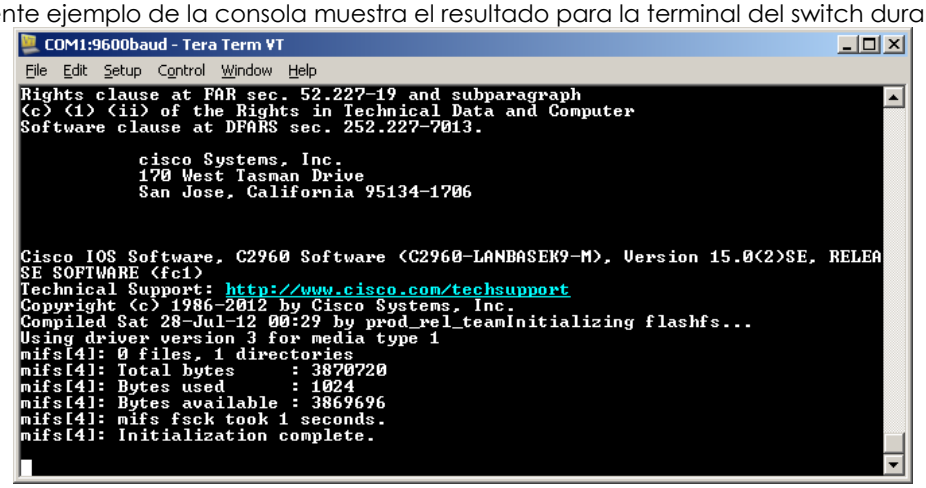
a. Inicie Tera Term haciendo clic en el botón **Inicio de Windows**, situado en la barra de tareas. Localice **Tera Term** en **Todos los programas**.
Nota: si no está instalado en el sistema, Tera Term se puede descargar del siguiente enlace seleccionando **Tera Term**:
http://logmett.com/index.php?/download/free-downloads.html

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

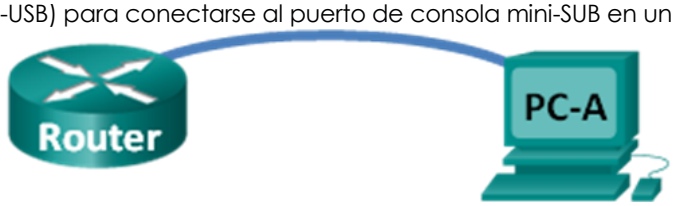
Switch# **clock set 15:08:00 Oct 26 2012**
Switch#
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43 UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by console.

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.

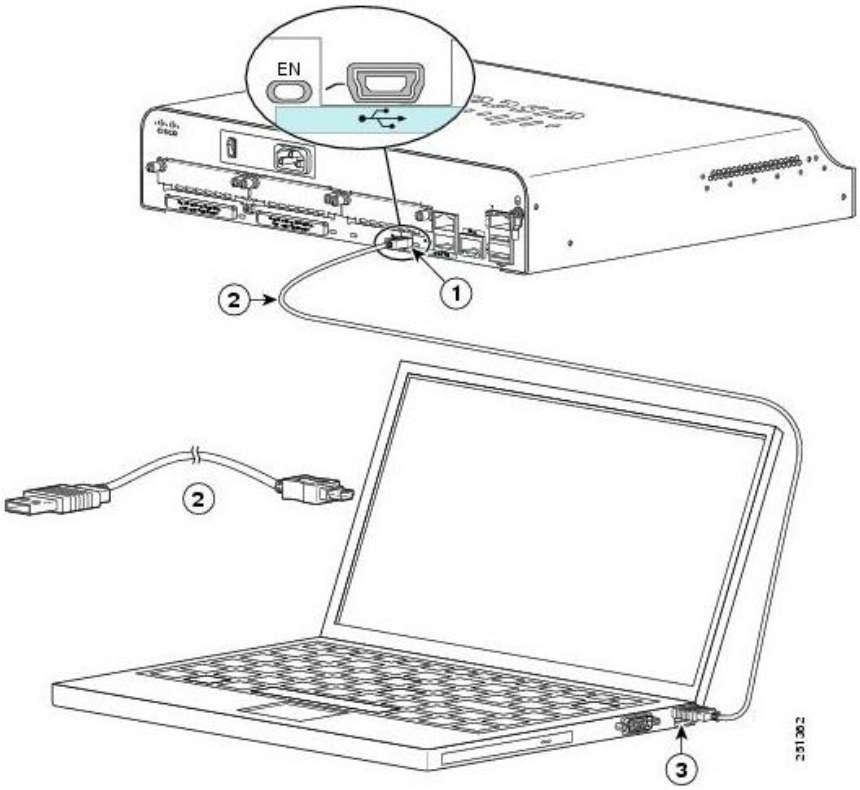
Nota: el cable de consola mini-USB es el mismo tipo de cable mini-USB que se utiliza con otros dispositivos electrónicos, como discos duros USB, impresoras USB o hubs USB. Estos cables mini-USB pueden adquirirse a través de Cisco Systems, Inc. o de otros proveedores externos. Asegúrese de utilizar un 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

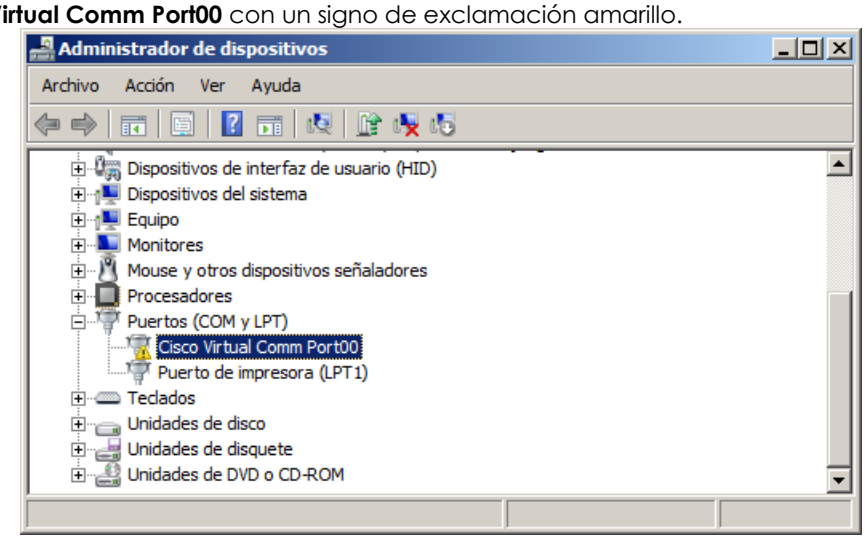
Paso 2: Verificar que la consola USB está lista

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.

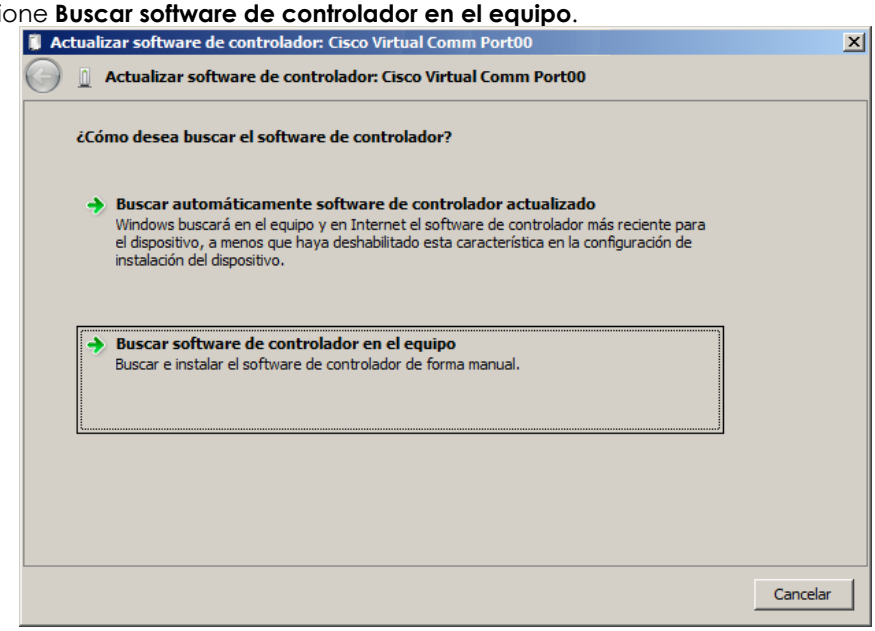
Paso 3: Habilitar el puerto COM para la PC con Windows 7 (optativo)

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

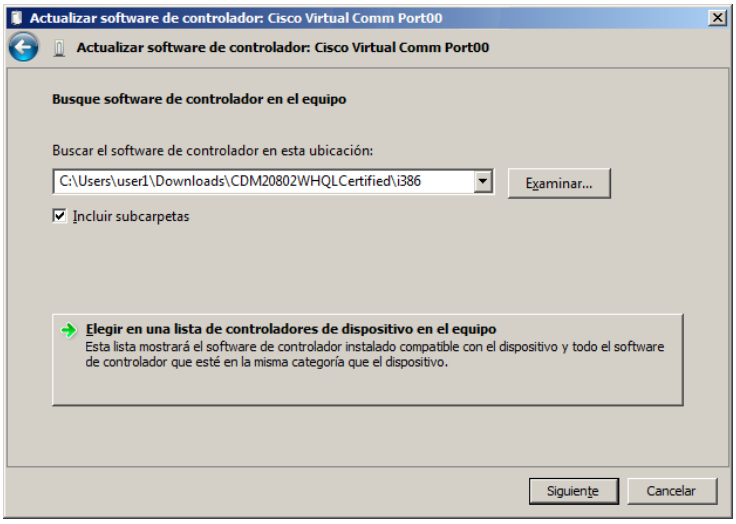
a. Haga clic en el ícono de **Inicio de Microsoft** para acceder al **Panel de control**.
b. Abra el **Administrador de dispositivos**.
c. Haga clic en el enlace de árbol **Puertos (COM y LPT)** para expandirlo. Aparecerá el ícono de **Cisco Virtual Comm Port00** con un signo de exclamación amarillo.



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**.

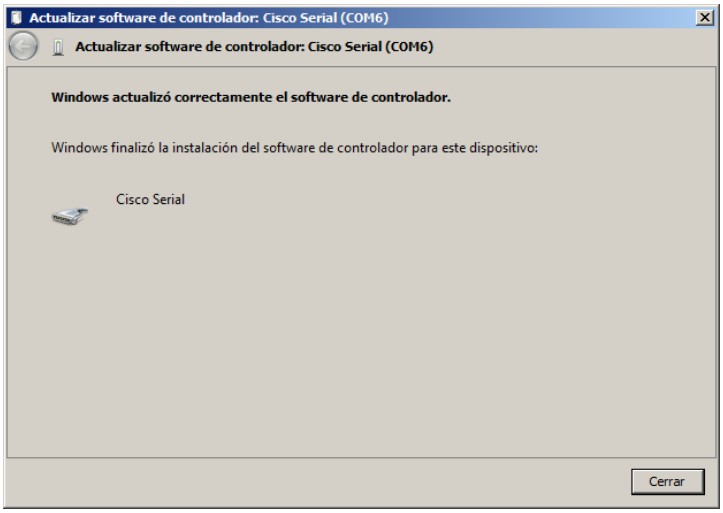


f. Seleccione **Elegir en una lista de controladores de dispositivo en el equipo** y haga clic en **Siguiente**.



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

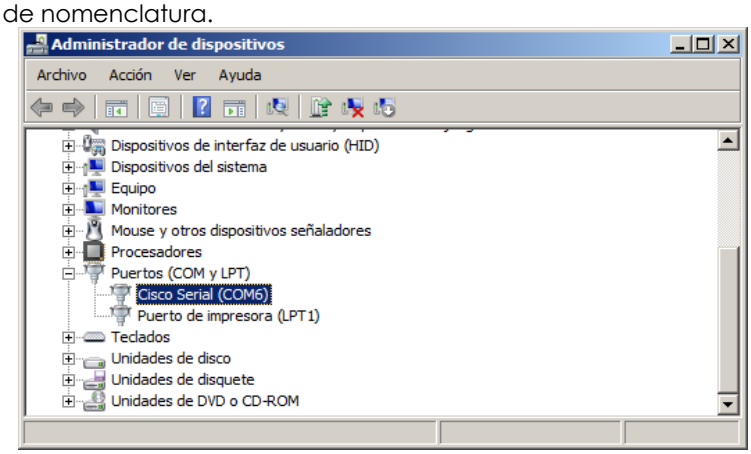
h. El controlador de dispositivo se instaló correctamente. Tome nota del número de puerto asignado en la parte superior de la ventana. En este ejemplo, se utiliza COM 6 para la comunicación con el router. Haga clic en **Cerrar**.



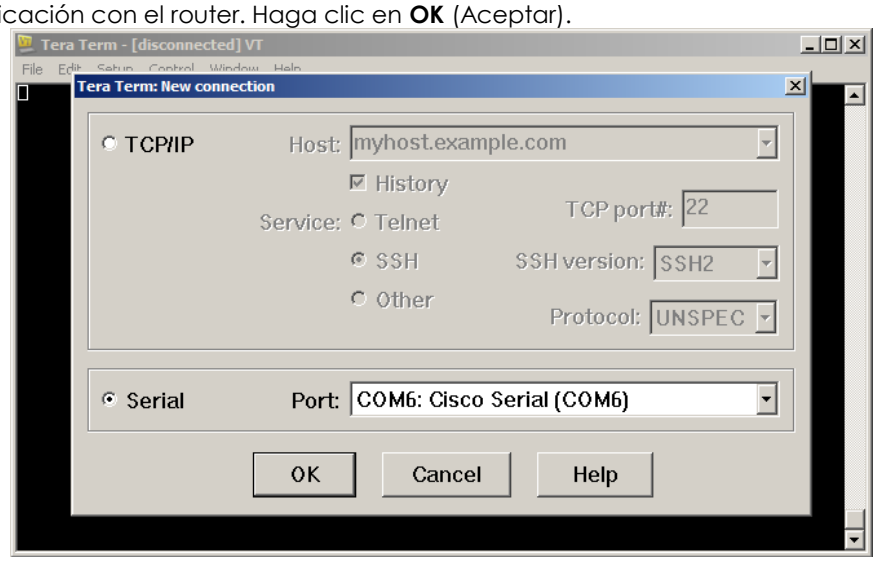
Paso 4: Determinar el número de puerto COM (optativo)

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).



5. Resultados

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

_____

_____

b. ¿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?

_____

_____

_____

_____

_____

_____

6. 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.				

7. Conclusiones

El método básico de conexión con los dispositivos de red es mediante una conexión de consola.

8. Sugerencias y /o recomendaciones

Averigüe como asegurar que una conexión de tipo serial pueda ser establecida con seguridad.

9. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 3

Creación de una red simple

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo** (de la práctica)**:**
   Al finalizar este laboratorio el estudiante podrá:
   - Configurar la topología de la red (Ethernet únicamente)
   - Configurar hosts en las PC
   - Configurar y verificar los parámetros básicos del switch
2. **Fundamento Teórico**
   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.
   Nota: los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio.
   Nota: asegúrese de que los switches se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice A para conocer el procedimiento de inicialización y recarga de un switch.

3. **Equipos, Materiales y Reactivos**
   - 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])
   - 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
   - Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
   - Cables Ethernet, como se muestra en la topología.
4. **Procedimientos:**

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.

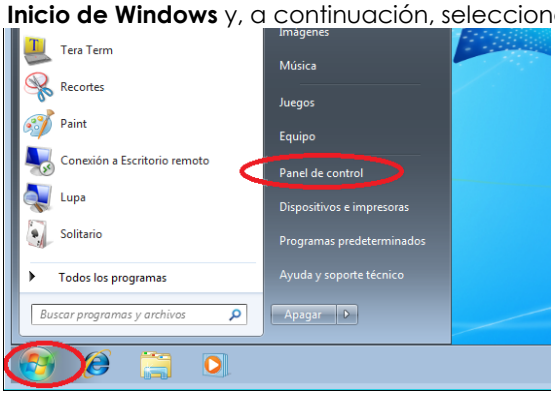
Paso 4: Inspeccionar visualmente las conexiones de la red

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.

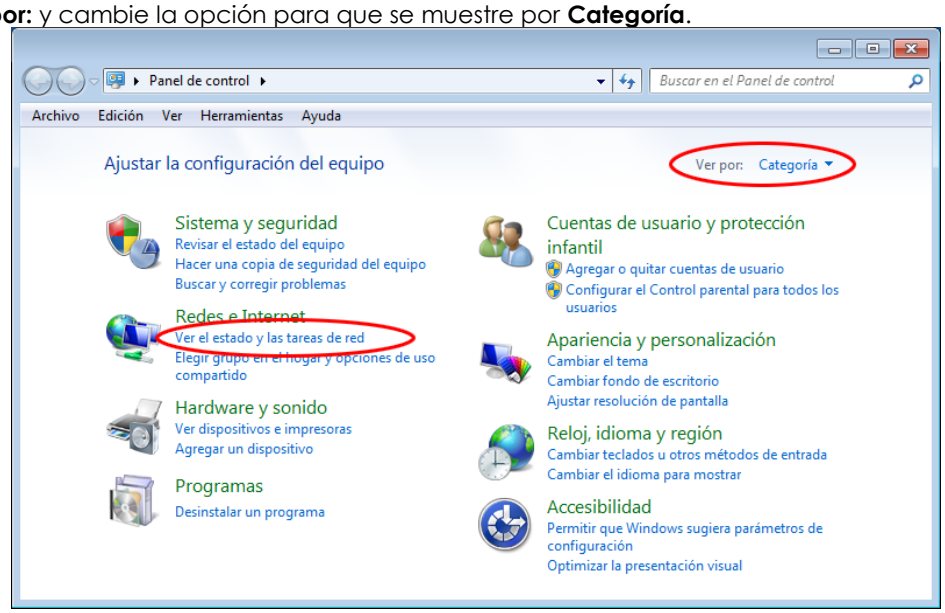
Parte 2: Configurar hosts en las PC

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

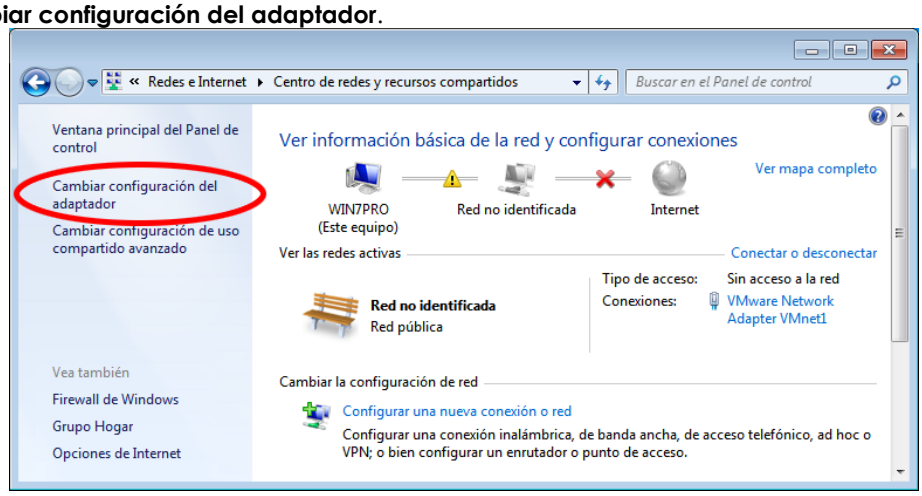
a. Haga clic en el ícono **Inicio de Windows** y, a continuación, seleccione **Panel de control**.



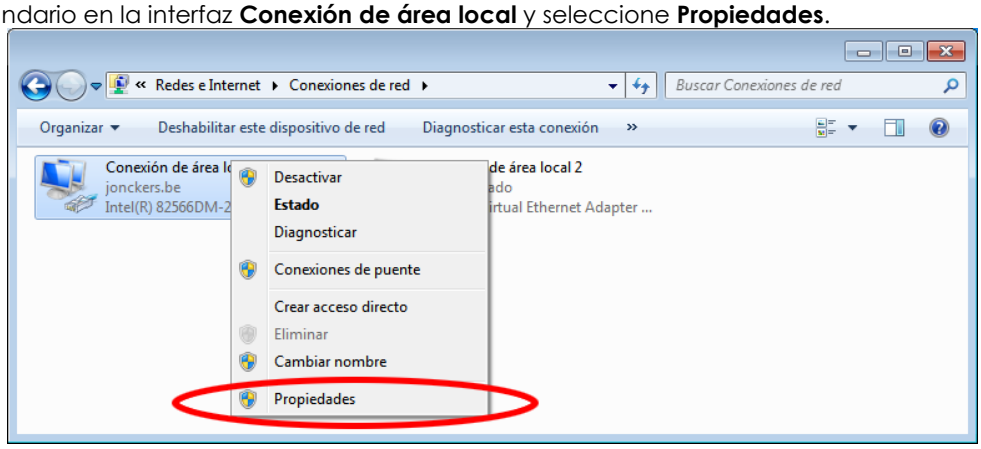
b. En la sección Redes e Internet, haga clic en el enlace **Ver el estado y las tareas de red**.
Nota: si en el panel de control se muestra una lista de íconos, haga clic en la opción desplegable que está junto a **Ver por:** y cambie la opción para que se muestre por **Categoría**.



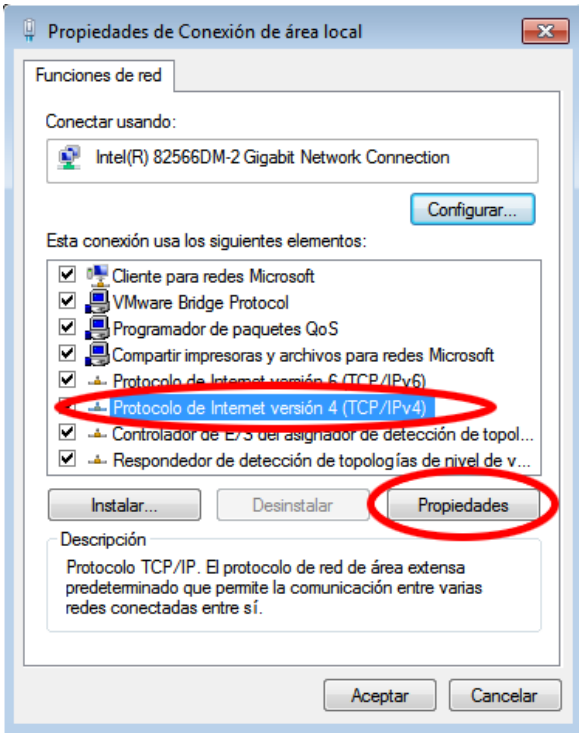
c. En el panel izquierdo de la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**.



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**.

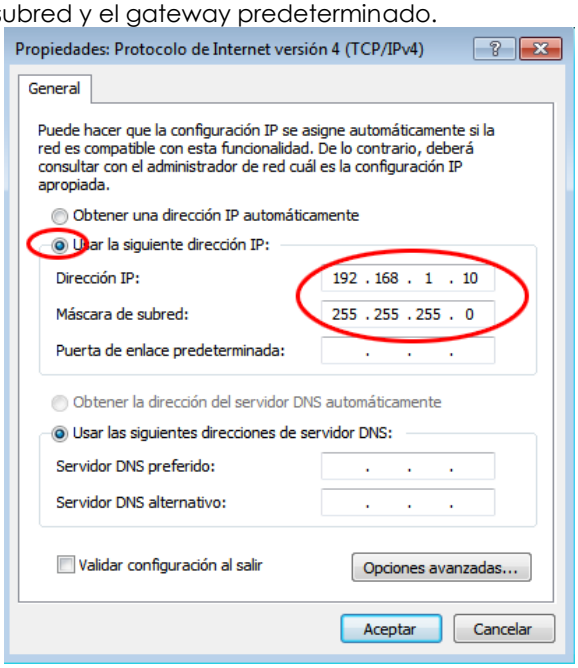


e. Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades**.



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.

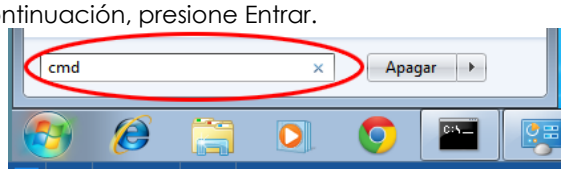
g. Después de introducir toda la información IP, haga clic en **Aceptar**. Haga clic en **Aceptar** en la ventana Propiedades de Conexión de área local para asignar la dirección IP al adaptador LAN.

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

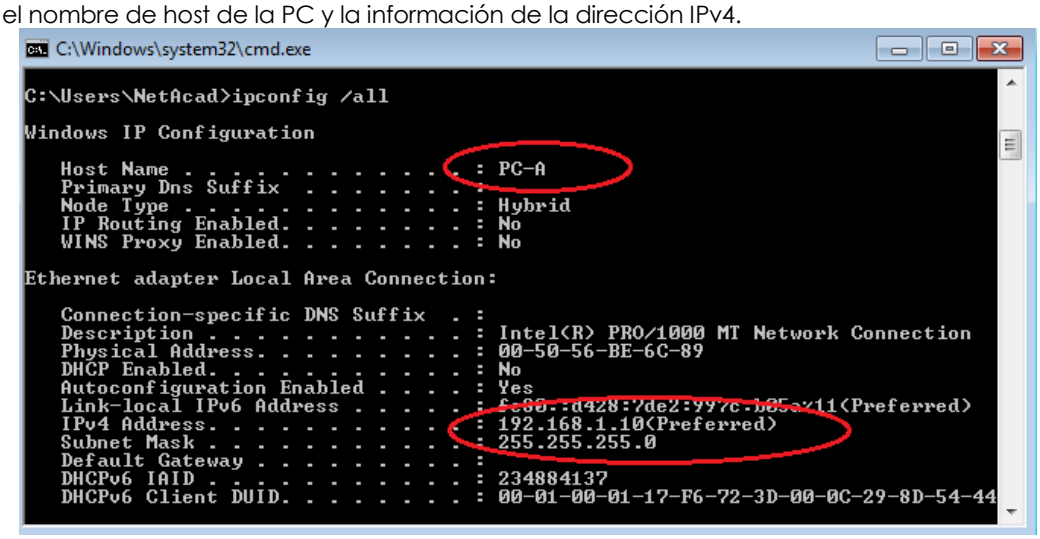
Paso 2: Verificar la configuración y la conectividad de la PC

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

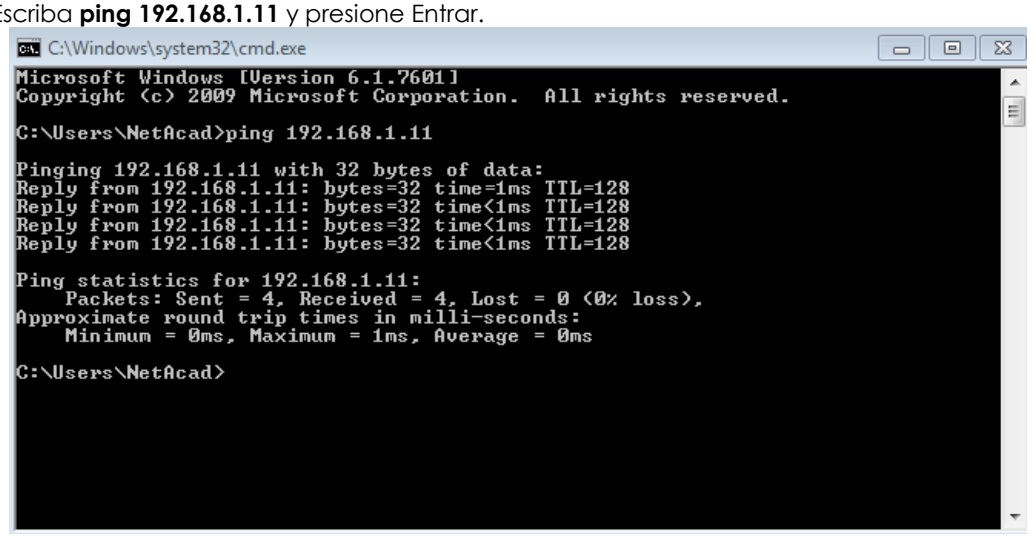
a. En la PC-A, haga clic en el ícono **Inicio de Windows**, escriba **cmd** en el cuadro de diálogo **Buscar programas y archivos** y, a continuación, presione Entrar.



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

	S1		S2	
Interfaz	**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>

5. Conclusiones

Los dispositivos de red son computadores por lo tanto se pueden manipular mediante comandos y archivos de configuración del Sistema Operativo IOS.

6. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a: Describir la estructura de comandos del software Cisco IOS.

7. Referencias bibliográficas consultadas y/o enlaces recomendados:

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 4

Configuración de una dirección de administración del switch

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo** (de la práctica)**:**
   Al finalizar este laboratorio el estudiante será capaz de:
   - Configurar un dispositivo de red básico
   - Verificar y probar la conectividad de red

2. **Fundamento Teórico**

   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.
   Nota: los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados producidos pueden variar de lo que se muestra en las prácticas de laboratorio.
   Nota: asegúrese de que el switch se haya borrado y no tenga una configuración de inicio. Si no está seguro, consulte con el instructor.

3. **Equipos, Materiales y Reactivos**
   - 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
   - 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
   - Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
   - Cables Ethernet, como se muestra en la topología.

4. **Procedimientos:**

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 **¡Error! No se encuentra el origen de la referencia.** 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
```

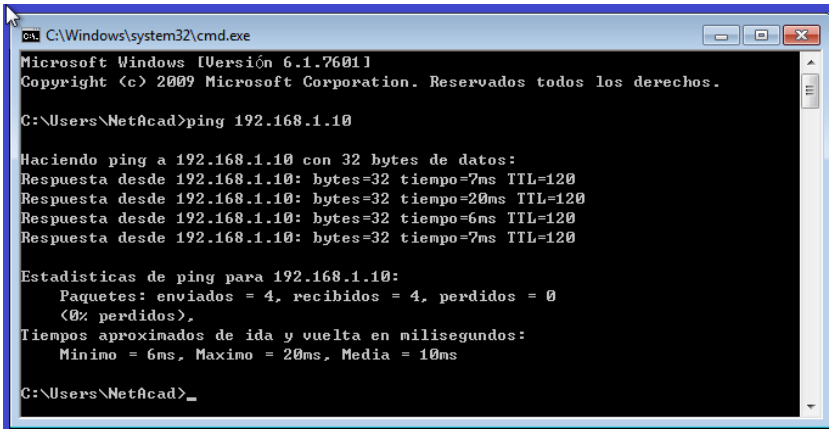
Paso 2: Probar la conectividad de extremo a extremo

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**

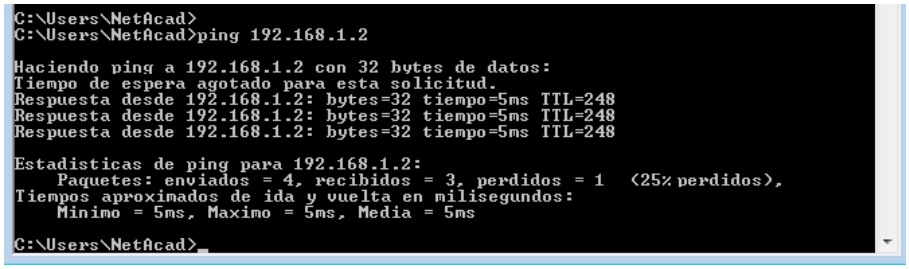
El resultado debe ser similar a la siguiente pantalla:



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.

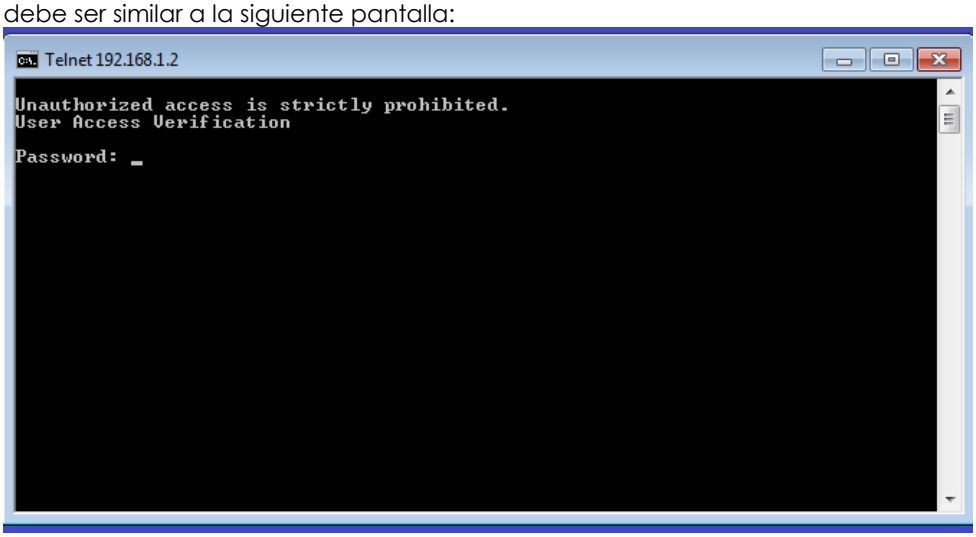
Nota: Windows 7 no admite Telnet en forma nativa. El administrador debe habilitar este protocolo. Para instalar el cliente Telnet, abra una ventana del símbolo del sistema y escriba **pkgmgr /iu:"TelnetClient"**.

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.

5. Resultados

¿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?

_____
_____

6. Conclusiones

Los Switches son dispositivos de red que operan en la capa II del modelo OSI, es decir emplean sobre todo direcciones MAC para establecer los circuitos de conmutación necesarios, por lo que no admiten que sus interfaces posean direcciones IP.
La excepción de direcciones IP, se da en el caso se requiera administrar un Switch remotamente, en ese caso se debe asignar una dirección IP al Switch.

7. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a: Configurar los parámetros iniciales en un dispositivo de red que utiliza el software Cisco IOS.

8. Referencias bibliográficas consultadas y/o enlaces recomendados

• Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 5

Uso de Wireshark para ver el tráfico de la red

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo (de la práctica):**

Al finalizar el laboratorio el estudiante podrá Capturar y analizar datos ICMP locales en Wireshark

2. **Fundamento Teórico**

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. **Equipos, Materiales y Reactivos**

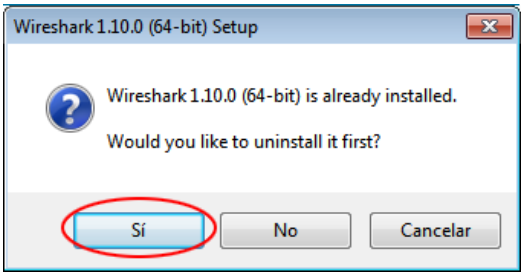
- 1 PC (Windows 7, Vista o XP, con acceso a Internet)
- Se utilizarán PC adicionales en una red de área local (LAN) para responder a las solicitudes de ping.

4. **Procedimientos:**

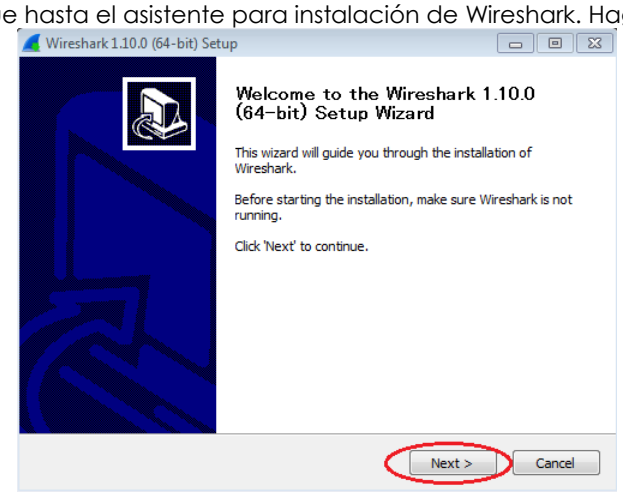
Paso 1: Instalar Wireshark

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.

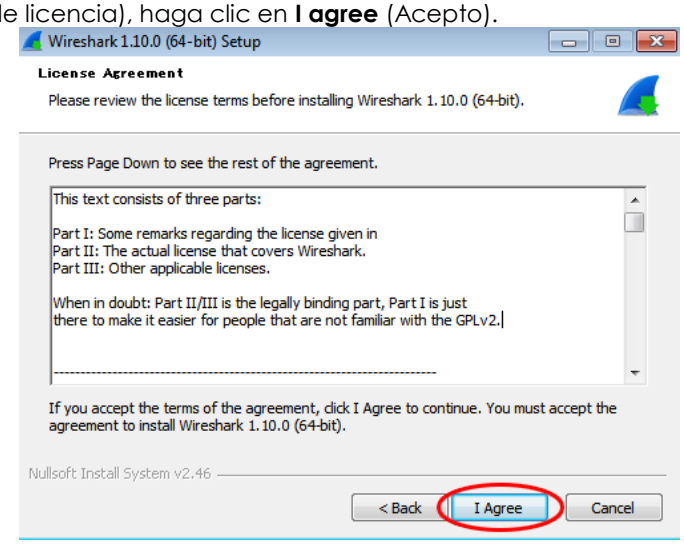
b. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí**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



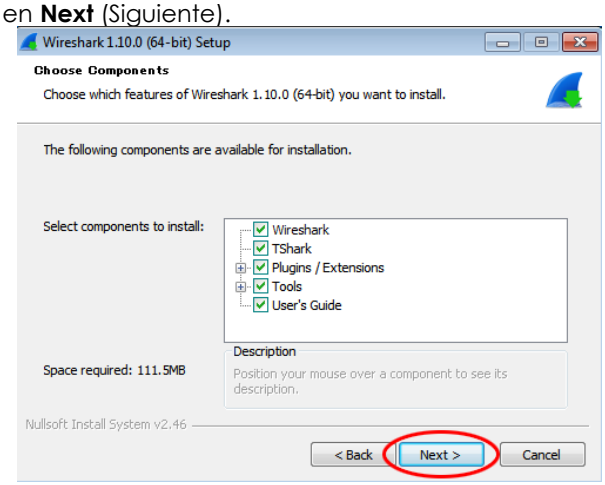
c. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Next** (Siguiente).



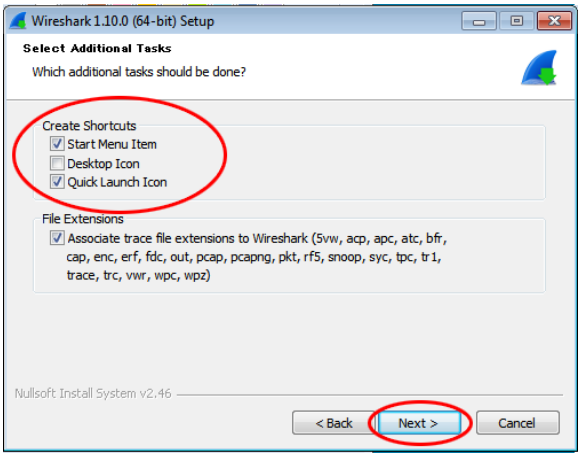
d. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement (Contrato de licencia), haga clic en **I agree** (Acepto).



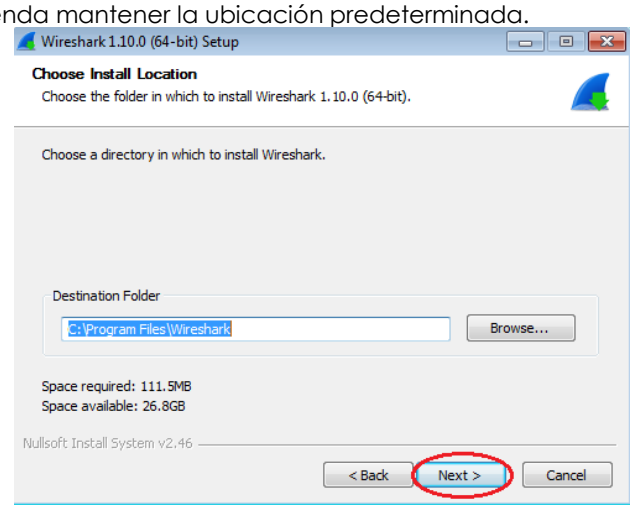
e. Guarde la configuración predeterminada en la ventana Choose Components (Elegir componentes) y haga clic en **Next** (Siguiente).



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

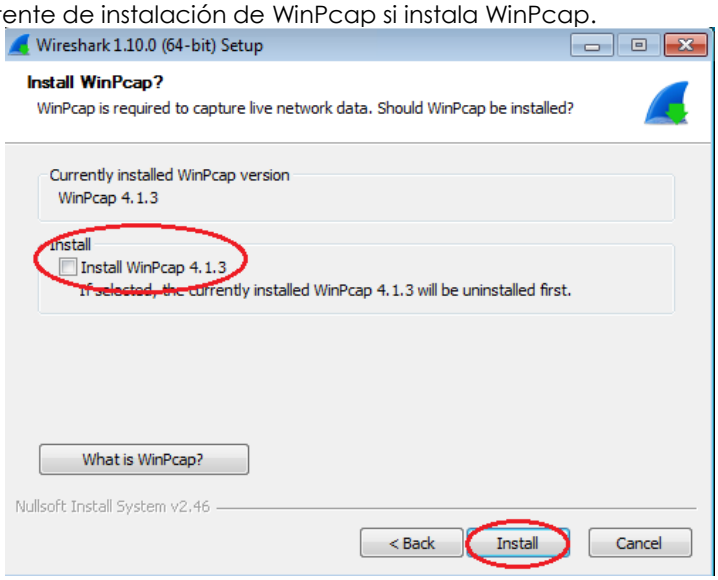


g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.

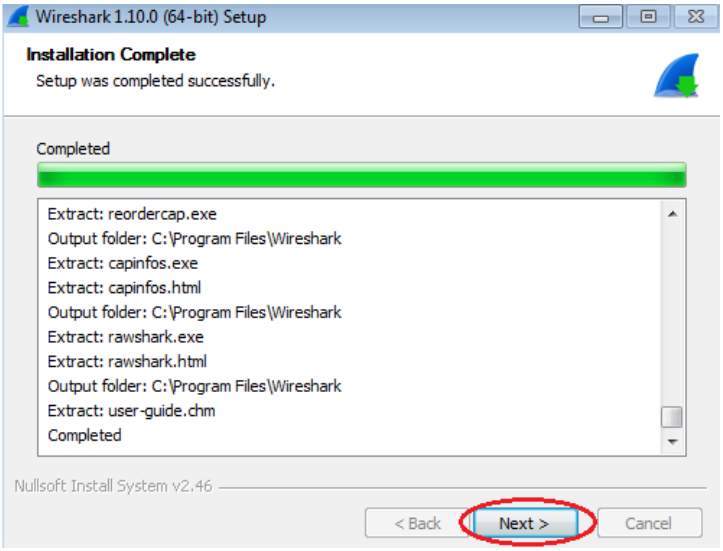


h. Para capturar datos de la red activa, WinPcap debe estar instalado en la PC. Si WinPcap ya está instalado en la PC, la casilla de verificación Install (Instalar) estará desactivada. Si la versión instalada de WinPcap es anterior a la versión que incluye Wireshark, se recomienda que permita que la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

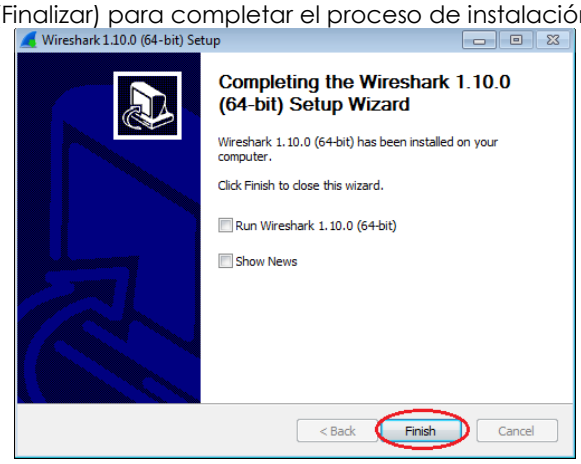
i. Finalice el asistente de instalación de WinPcap si instala WinPcap.



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

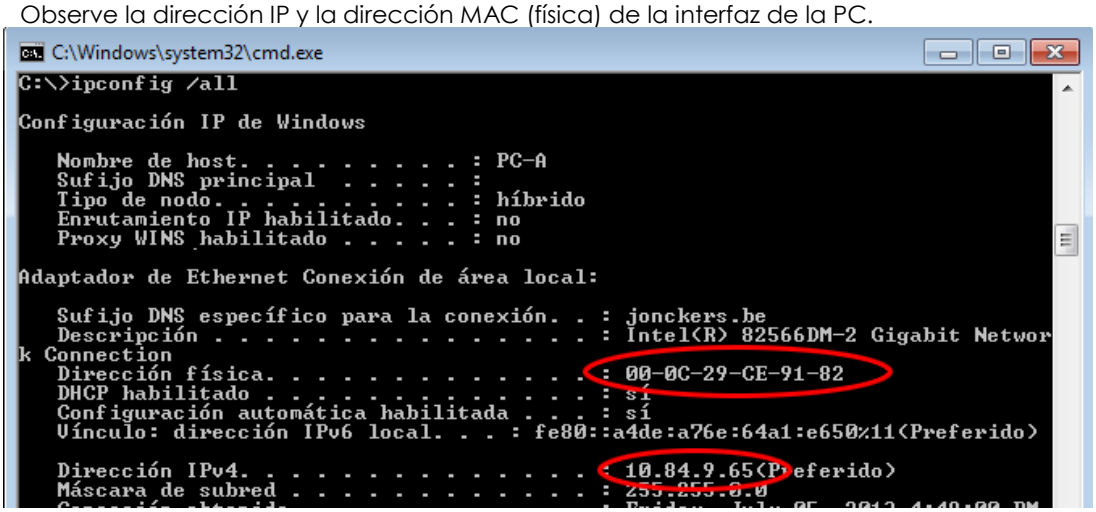
En la parte 2 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes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

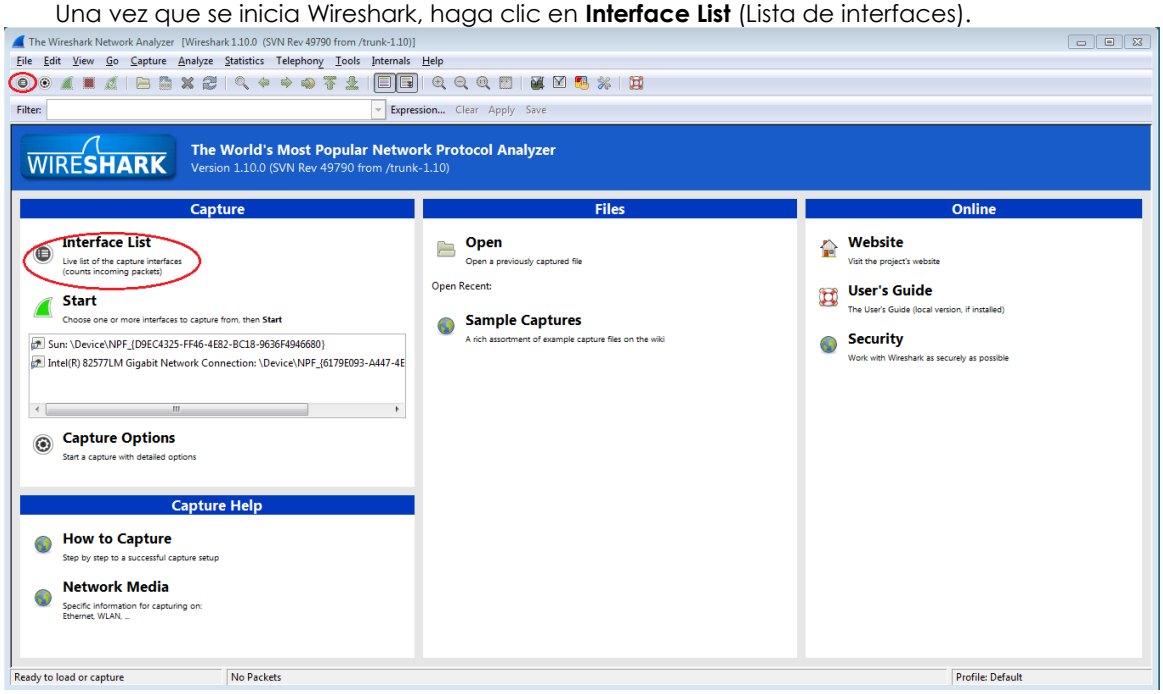


c. Solicite a un miembro del equipo la dirección IP de su PC y proporciónele la suya. En esta instancia, no proporcione su dirección MAC.

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**.

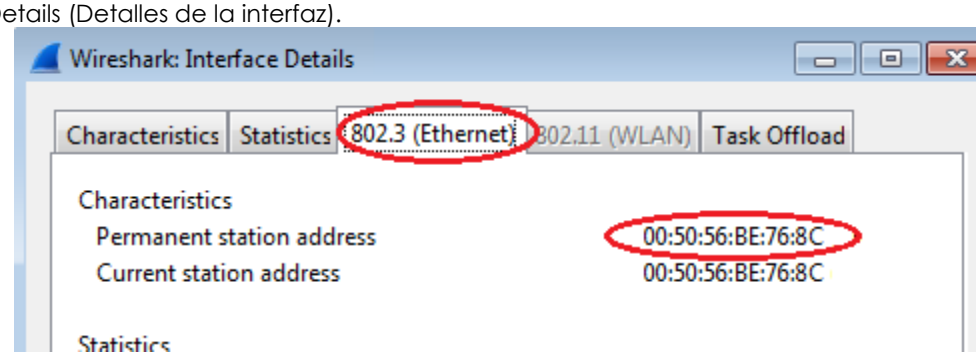
b. Una vez que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).



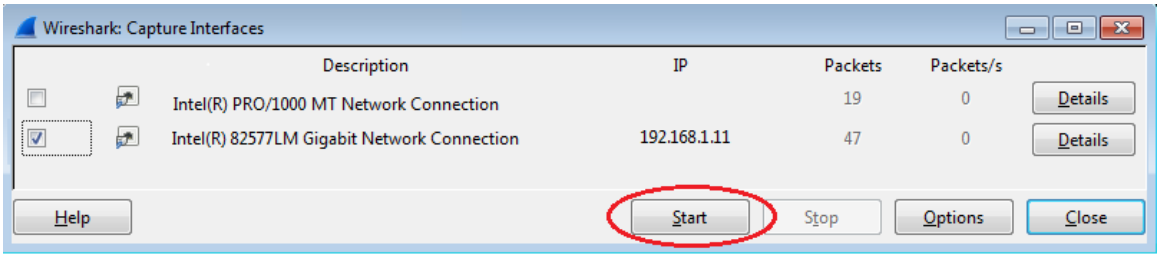
Nota: al hacer clic en el ícono de la primera interfaz de la fila de íconos, también se abre Interface List (Lista de interfaces).

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.

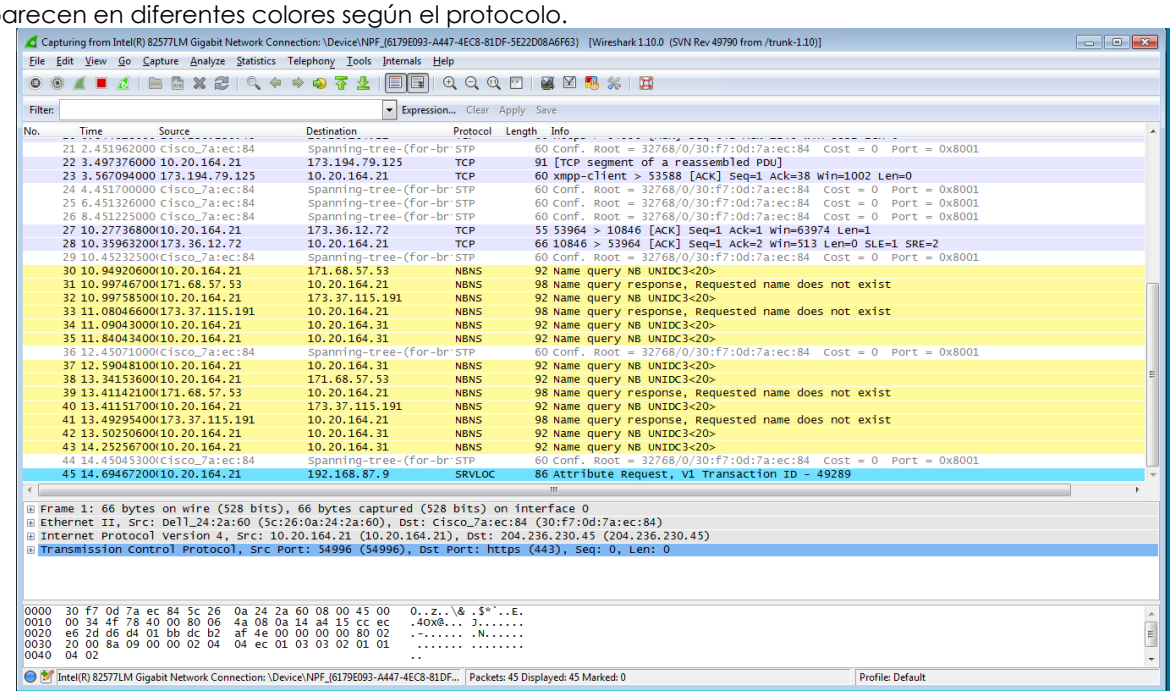
Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón **Details** (Detalles) y, a continuación, haga clic en la ficha **802.3 (Ethernet)**. Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre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



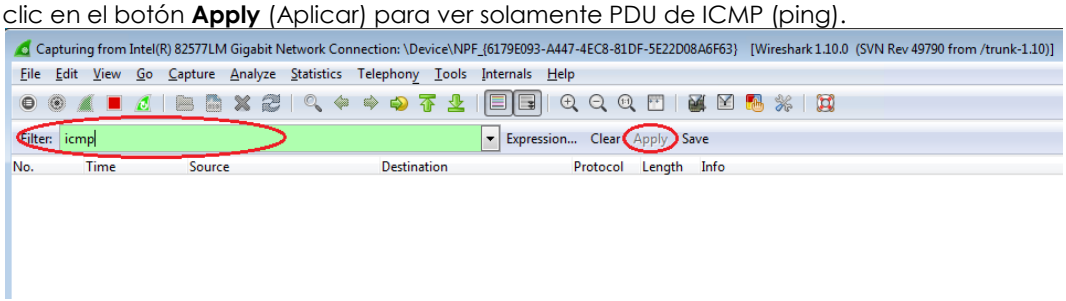
d. Después de activar la interfaz correcta, haga clic en **Start** (Comenzar) para comenzar la captura de datos.



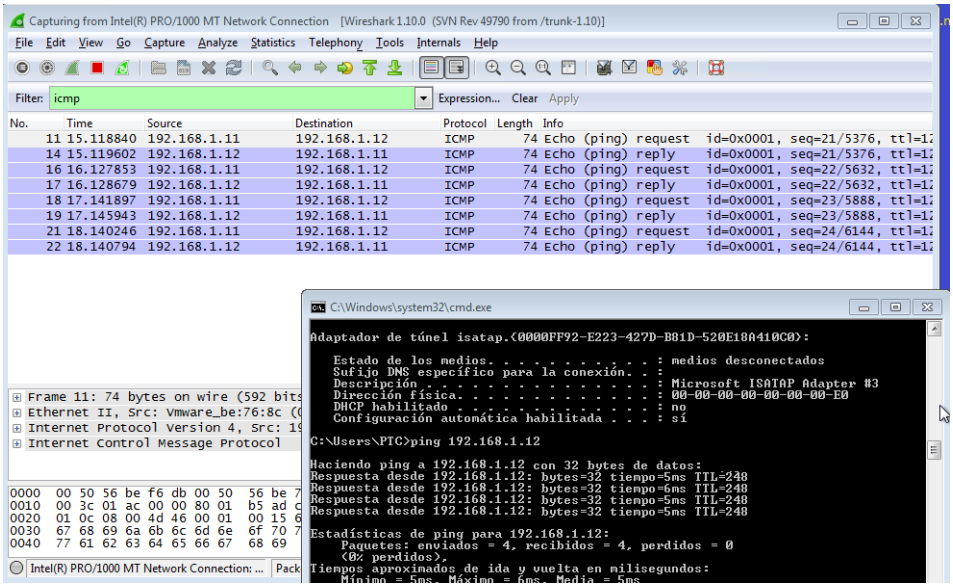
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.



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).

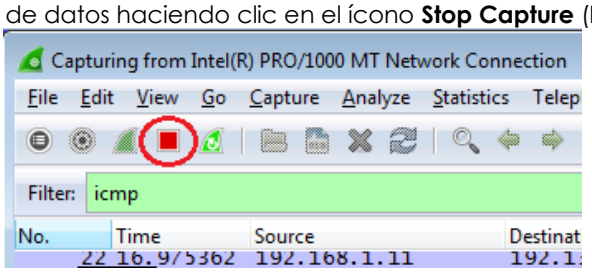


f. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior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



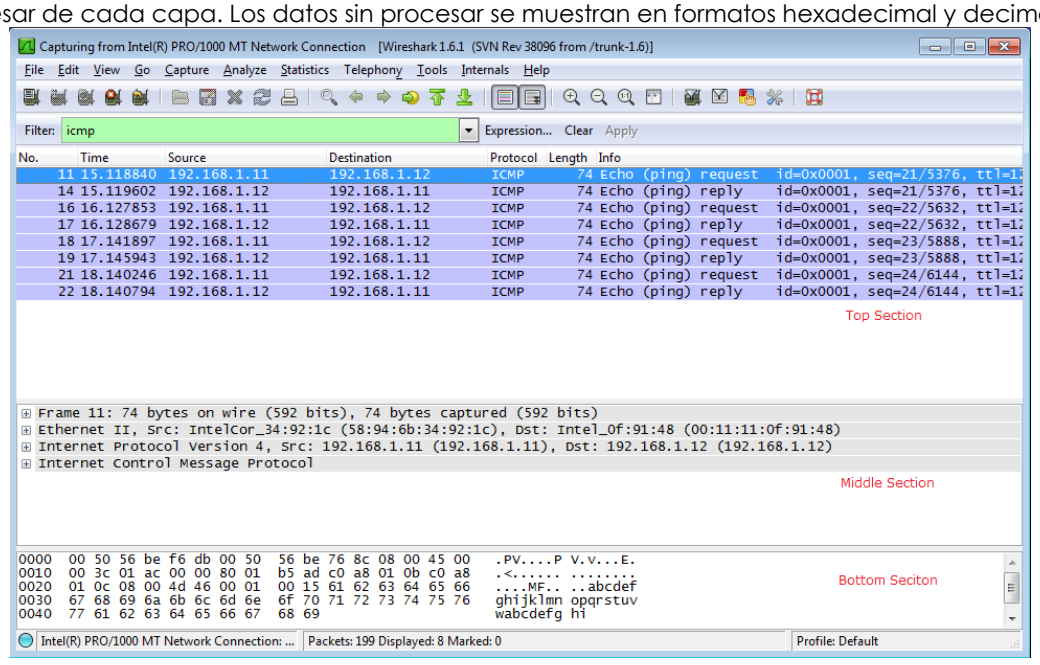
Nota: si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Apéndice A: Permitir el tráfico ICMP a través de un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall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

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

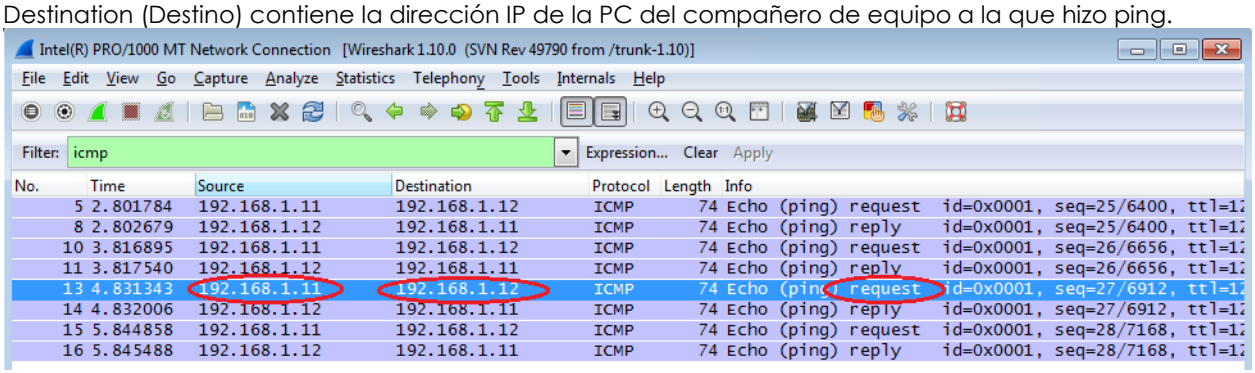


Paso 3: Examinar los datos capturados

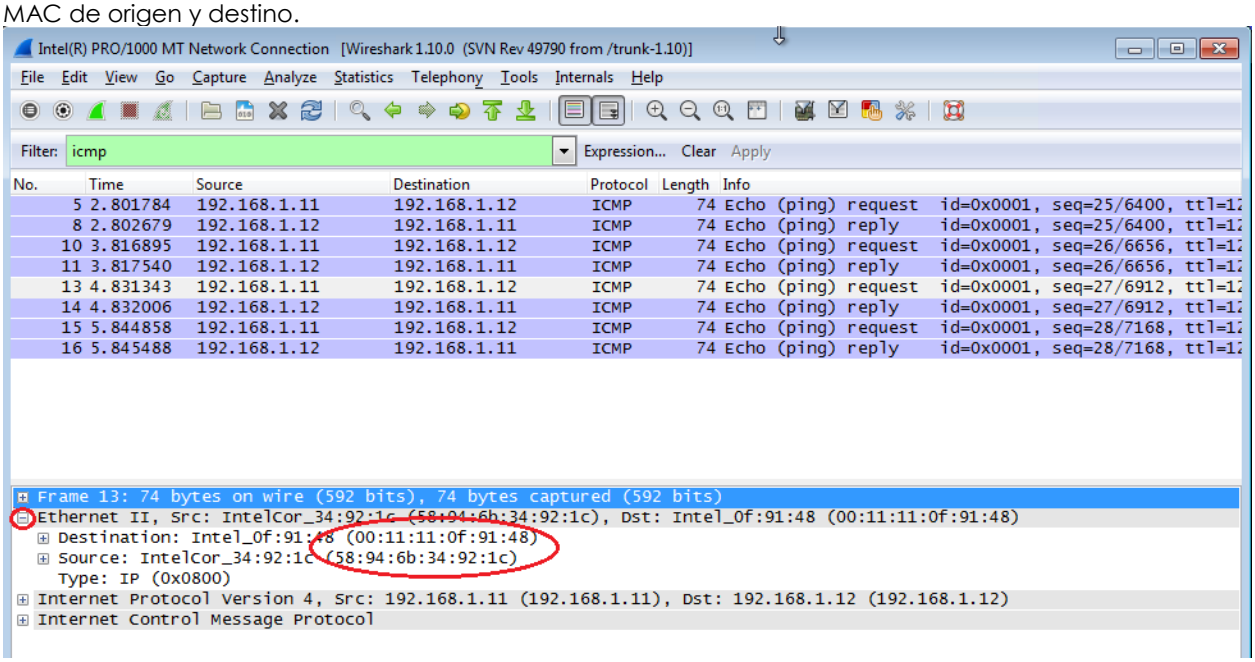
En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la 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?

_____

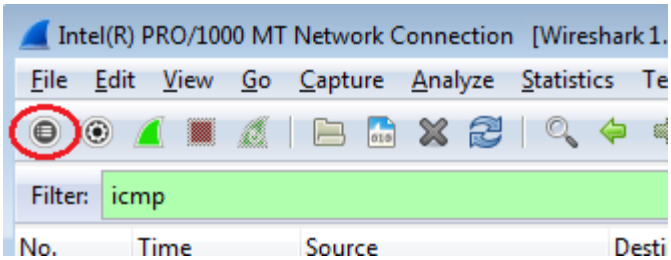
Nota: en el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPV4 (encabezado de IPv4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

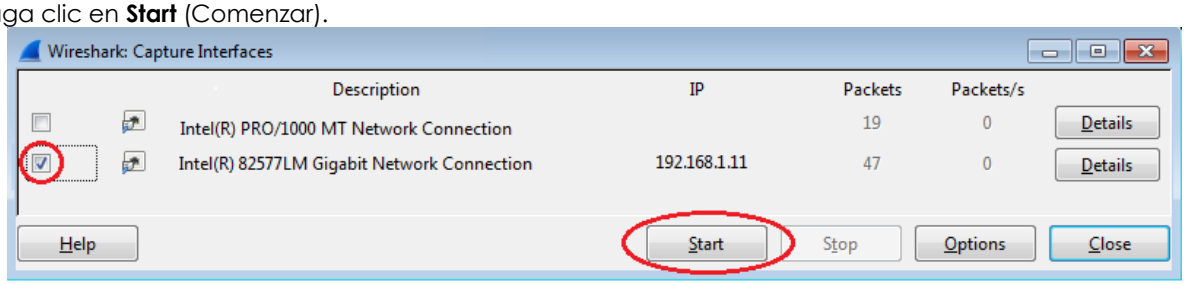
En la parte 3, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 2.

Paso 1: Comenzar a capturar datos en la interfaz

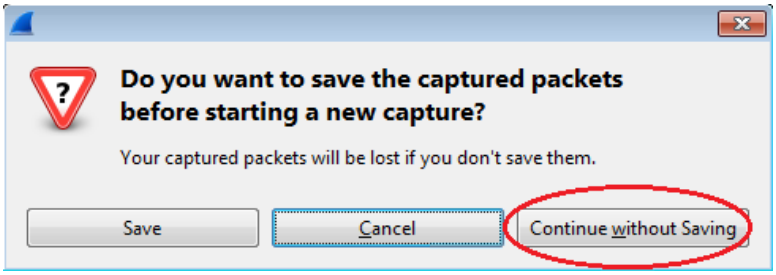
a. Haga clic en el ícono **Interface List** (Lista de interfaces) para volver a abrir la lista de interfaces de la PC.



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

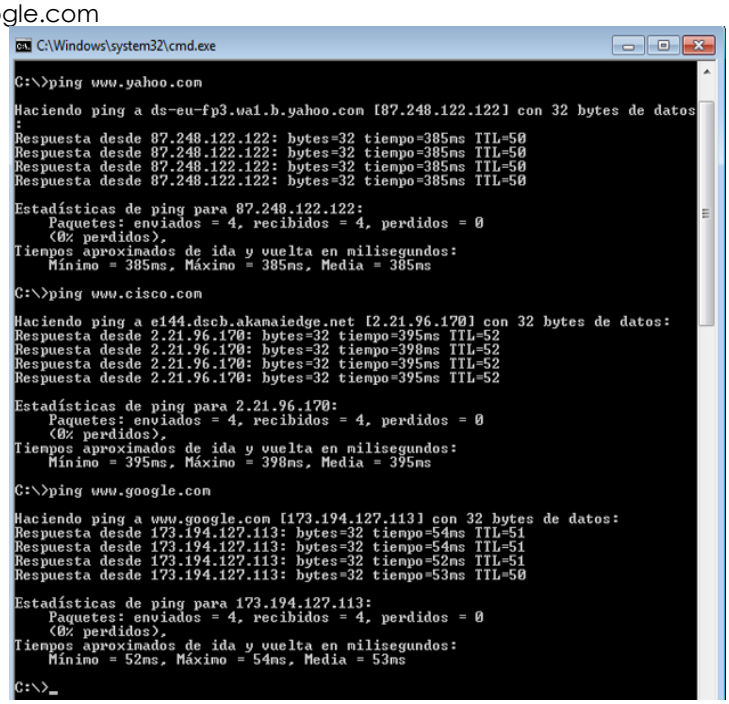


c. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



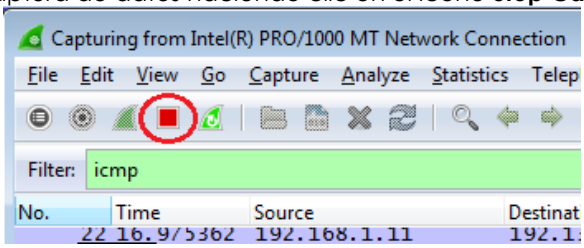
d. Con la captura activa, haga ping a los URL de los tres sitios Web siguientes:

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?

_____

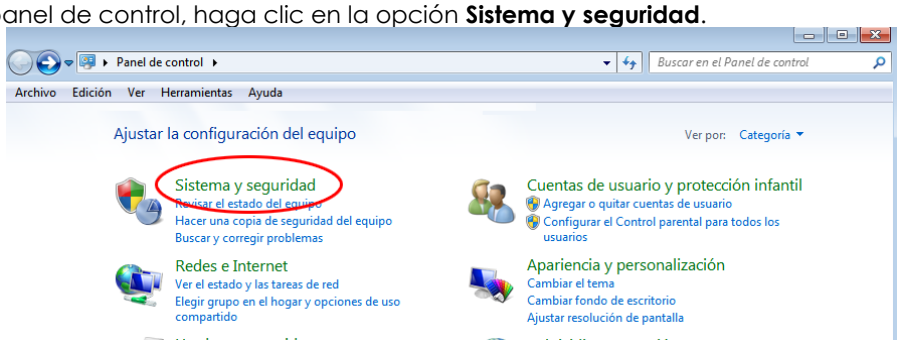
_____

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

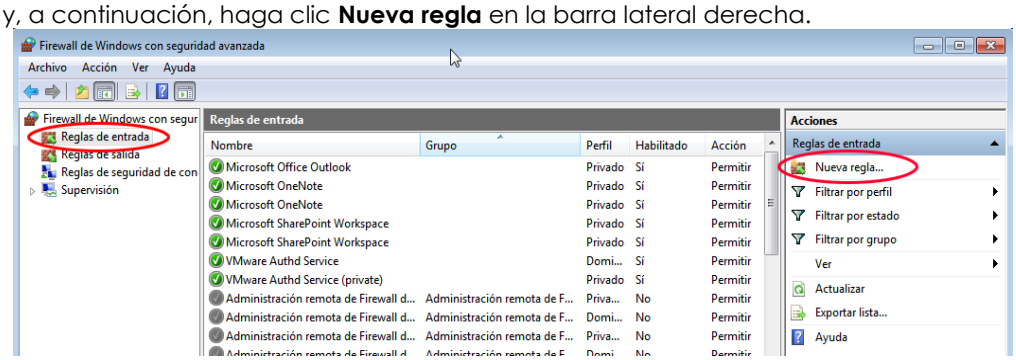
a. En el panel de control, haga clic en la opción **Sistema y seguridad**.



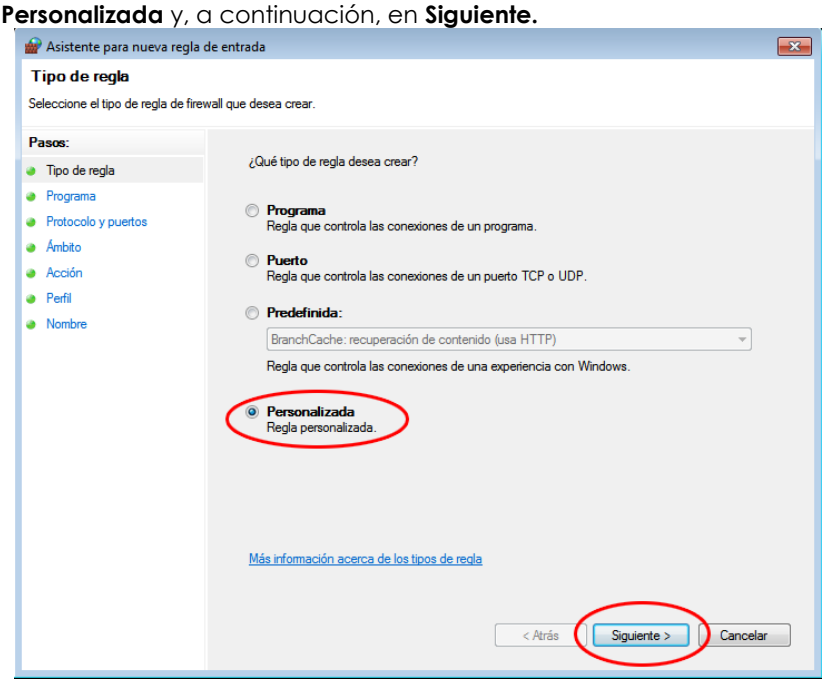
b. En la ventana Sistema y seguridad, haga clic en **Firewall de Windows**.

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

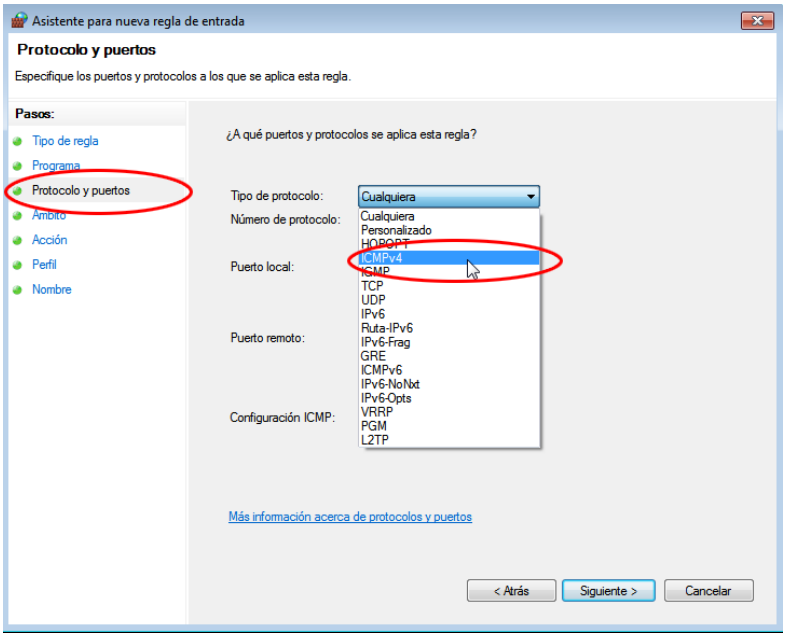
d. En la ventana Seguridad avanzada, seleccione la opción **Reglas de entrada** en la barra lateral izquierda y, a continuación, haga clic **Nueva regla** en la barra lateral derecha.



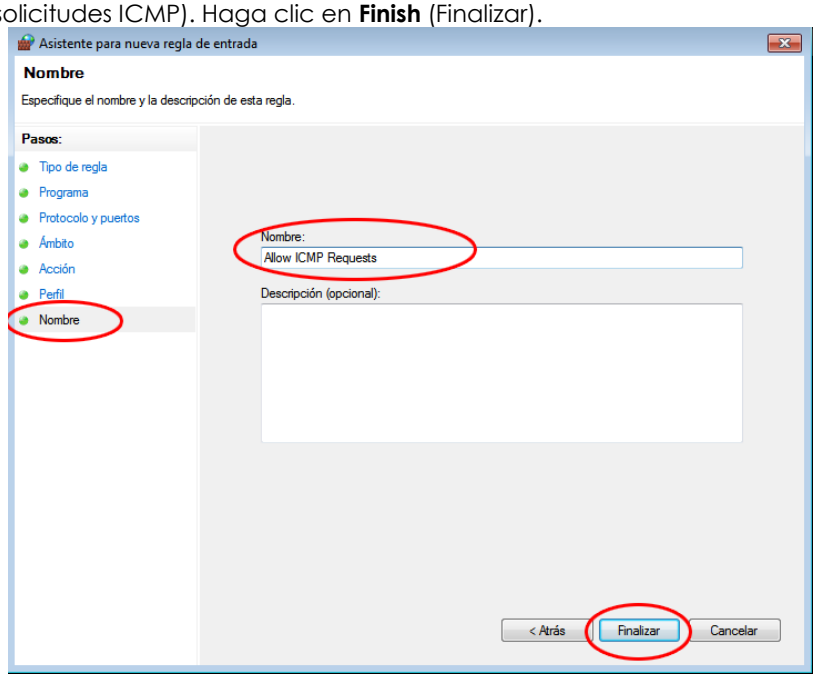
e. Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción **Personalizada** y, a continuación, en **Siguiente.**



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).

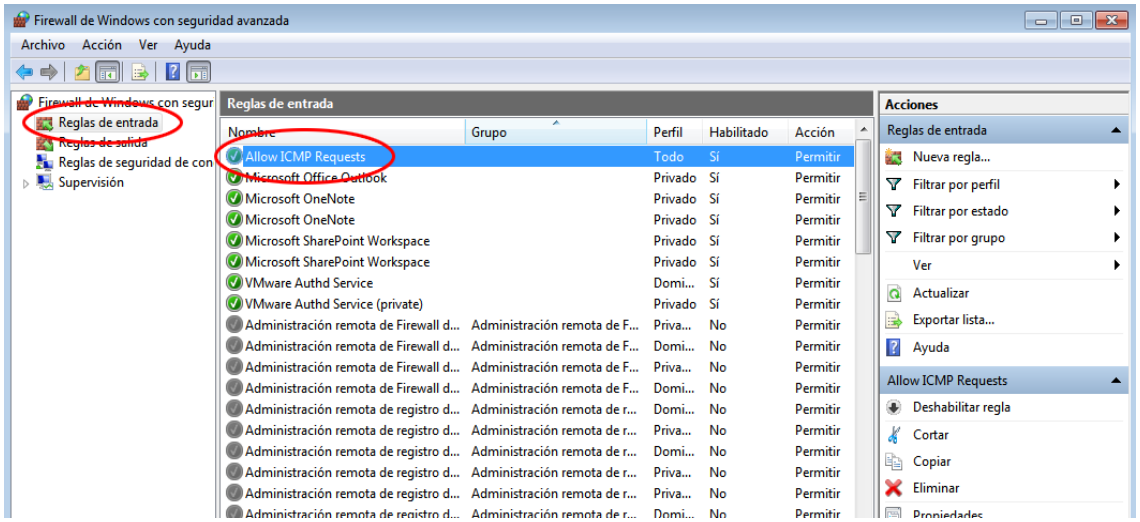


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

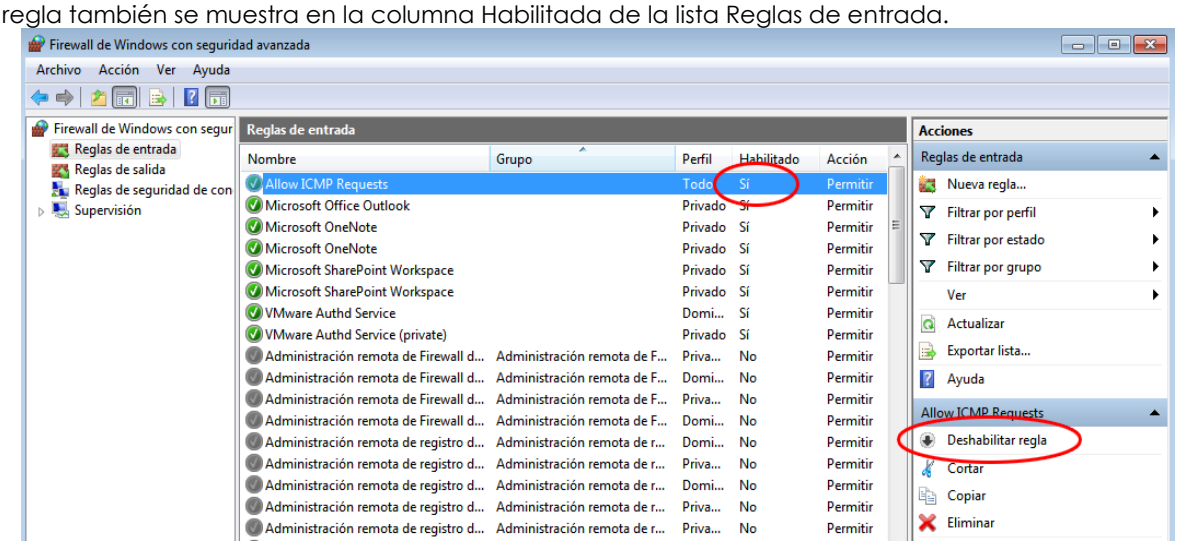
Paso 2: Deshabilitar o eliminar la nueva regla ICMP

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.

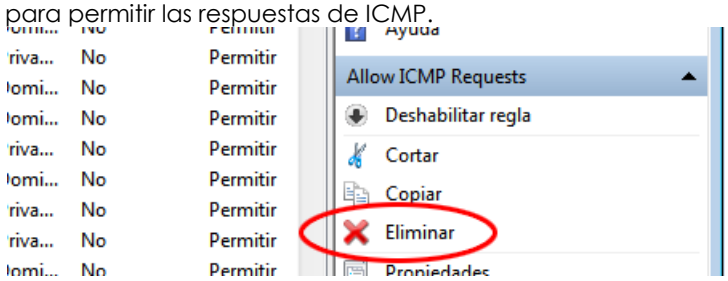
a. En el panel izquierdo de la ventana Seguridad avanzada, haga clic en **Reglas de entrada** y, a continuación, ubique la regla que creó en el paso 1.



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.



5. Conclusiones

El conocimiento de un software que pueda capturar paquetes de red es muy importante, así podemos entender la forma en que operan los protocolos de red y en como interactúan

6. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a: Explicar la función de los protocolos y de los organismos de estandarización para facilitar la interoperabilidad en las comunicaciones de red.

7. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 6

Armado de un cable cruzado Ethernet

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo (de la práctica):**
   - Analizar los estándares de cableado y los diagramas de pines de Ethernet
   - Armar un cable cruzado Etherne
   - Probar un cable cruzado Ethernet

2. **Fundamento Teórico**

   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.

   Nota: las capacidades de detección automática disponibles en muchos dispositivos, como el switch del router de servicios integrados (ISR) Cisco 1941, le permitirán ver los cables directos que conectan dispositivos similares.

3. **Equipos, Materiales y Reactivos**
   - Un tramo de cable, ya sea de categoría 5e o 5. El tramo de cable debe ser de 0,6 m a 0,9 m (de 2 ft a 3 ft).
   - 2 conectores RJ-45
   - Tenaza engarzadora RJ-45
   - Alicate
   - Pelacables
   - Comprobador de cables Ethernet (optativo)
   - 2 PC (Windows 7, Vista o XP)

4. **Procedimientos:**

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.

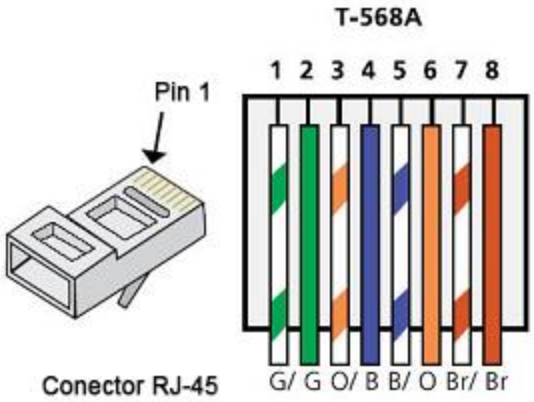
El switch Cisco 2960 tiene la función de detección automática activada de manera predeterminada; por lo tanto, la conexión de dos switches 2960 funciona con un cable cruzado o con un cable directo. Con algunos switches anteriores, este no es el caso, y se debe usar un cable cruzado.
Además, las interfaces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

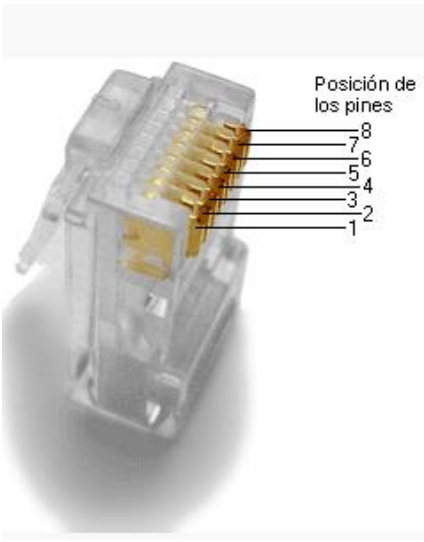
Paso 1: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-A.
En la tabla y los diagramas siguientes, se muestran el esquema de colores y el diagrama de pines, así como la función de los cuatro pares de hilos que se utilizan para el estándar 568-A.
Nota: en las instalaciones de LAN 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.



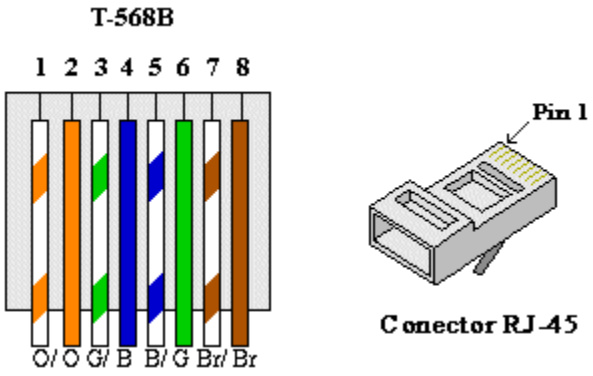


Paso 2: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-B.

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

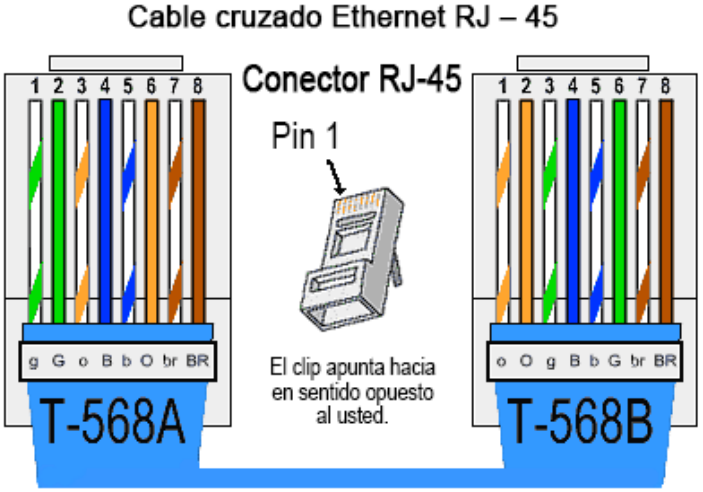
Ethernet 10/100/1000-BaseTX conforme al estándar 568-B

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

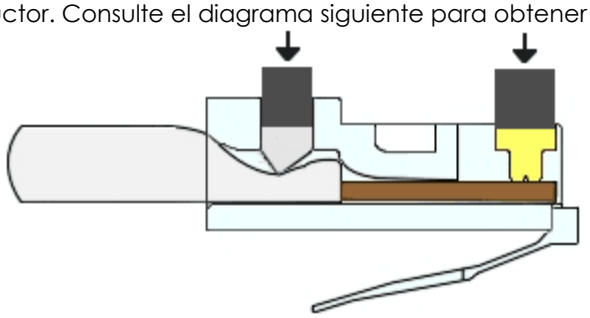
diagramas, si es necesario. Tome todas las precauciones posibles para mantener las torsiones del cable, a fin de proporcionar anulación de ruidos.

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.

5. Resultados

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

_____

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

_____

6. Conclusiones

Al armar cables de red(patch cords) es de suma importancia seguir los estándares de red estabklecidos por la ANSI EIA / TIA.

7. Sugerencias y /o recomendaciones:

Revisar en la plataforma de CISCO NetAcad el tema referente a : Visualización de información de NIC conectadas por cable e inalámbricas

8. Referencias bibliográficas consultadas y/o enlaces recomendados

• Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 7

Visualización de direcciones MAC de dispositivos de red

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Establecer la topología e inicializar los dispositivos
- Configurar dispositivos y verificar la conectividad
- Mostrar, describir y analizar las direcciones MAC de Ethernet

2. Fundamento Teórico

Cada dispositivo en una LAN Ethernet está identificado con una dirección MAC de la capa 2. Esta dirección se graba en la NIC. En esta práctica de laboratorio, se explorarán y analizarán los componentes que integran una dirección MAC, y cómo puede encontrar esta información en los diversos dispositivos de red, como un router, un switch y una PC.

Realizará el cableado de los equipos como se muestra en la topología. Luego, configurará el router y la PC según la tabla de direccionamiento. También probará la conectividad de red para verificar las configuraciones.

Una vez que los dispositivos estén configurados y que se haya verificado la conectividad de red, utilizará diferentes comandos para recuperar la información de los dispositivos y responder preguntas sobre los equipos de red.

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

3. Equipos, Materiales y Reactivos

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

4. Procedimientos:

Parte 1: Establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red, borrará cualquier configuración, si fuera necesario, y configurará los parámetros básicos, como direcciones IP de la interfaz en el router y la PC.

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

a. Conecte los dispositivos que se muestran en la topología y realice 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.

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 y el acceso a dispositivos. Para obtener información acerca de nombres y direcciones de dispositivos, consulte la topología y la tabla de direccionamiento.

Paso 1: Configurar la dirección IPv4 para la PC

a. Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A.

b. Haga ping a la dirección de gateway predeterminado del R1 desde el símbolo del sistema de la PC-A.

¿Tuvieron éxito los pings? ¿Por qué o por qué no?

_____

_____

Paso 2: Configurar el router.

a. Acceda al router mediante el puerto de consola e introduzca el modo de configuración global.

b. Asigne un nombre de host al router basado en la tabla de direccionamiento.

c. Desactive la búsqueda del DNS.

d. Configure y habilite la interfaz G0/1 en el router.

Paso 3: Verificar la conectividad de la red.

a. Haga ping a la dirección de gateway predeterminado del R1 desde la PC-A.

¿Tuvieron éxito los pings? _____

Parte 3: Mostrar, describir y analizar las direcciones MAC de Ethernet

Cada dispositivo en una LAN Ethernet tiene una dirección de control de acceso al medio (MAC) grabada en la tarjeta de interfaz de red (NIC). Las direcciones MAC de Ethernet tienen una longitud de 48 bits. Se muestran utilizando seis conjuntos de dígitos hexadecimales separados generalmente por guiones, dos puntos o puntos. En el siguiente ejemplo, se muestra la misma dirección MAC utilizando tres métodos de notación diferentes:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Nota: las direcciones MAC también se denominan "direcciones físicas", "direcciones de hardware" o "direcciones de hardware Ethernet".

En la parte 3, emitirá comandos para mostrar las direcciones MAC en una PC, un router y un switch, y analizará las propiedades de cada uno.

Paso 1: Analizar la dirección MAC para la NIC de la PC-A

Antes de analizar la dirección MAC en la PC-A, veamos un ejemplo de una NIC de PC distinta. Puede emitir el comando **ipconfig /all** para ver la dirección MAC de las NIC. A continuación, se muestra un resultado en pantalla de ejemplo. Cuando utilice el comando **ipconfig /all**, tenga en cuenta que las direcciones MAC se denominan "direcciones físicas". Si se lee la dirección MAC de izquierda a derecha, los primeros seis dígitos hexadecimales se refieren al proveedor (fabricante) de este dispositivo. Estos primeros seis dígitos hexadecimales (3 bytes) también se conocen como el "identificador único de organización" (OUI). La organización IEEE asigna este código de 3 bytes al proveedor. Para buscar al fabricante, puede utilizar una herramienta como www.macvendorlookup.com o ir al sitio Web de IEEE para buscar los códigos de proveedor OUI registrados. La dirección del sitio Web de IEEE para obtener información del OUI es

http://standards.ieee.org/develop/regauth/oui/public.html. Los últimos seis dígitos corresponden al número de serie de la NIC asignados por el fabricante.

a. Utilice el resultado del comando **ipconfig /all** para responder las siguientes preguntas.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : C8-0A-A9-FA-DE-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

¿Cuál es la porción del OUI de la dirección MAC para este dispositivo?

_____

¿Cuál es la porción del número de serie de la dirección MAC para este dispositivo?

_____

Utilice el ejemplo anterior para buscar el nombre del proveedor que fabricó esta NIC.

_____

b. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** e identifique la porción del OUI de la dirección MAC para la NIC de la PC-A.

_____

Identifique la porción del número de serie de la dirección MAC para la NIC de la PC-A.

_____

Identifique el nombre del proveedor que fabricó la NIC de la PC-A. _____

Paso 2: Analizar la dirección MAC para la interfaz G0/1 del R1

Puede utilizar una variedad de comandos para mostrar las direcciones MAC en el router.

a. Acceda al R1 mediante el puerto de consola y utilice el comando **show interfaces g0/1** para buscar la información de la dirección MAC. A continuación, se presenta un ejemplo. Utilice los resultados que genera el router para contestar las preguntas.

R1> **show interfaces g0/1**

```
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 30f7.0da3.1821)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 3000 bits/sec, 4 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     15183 packets input, 971564 bytes, 0 no buffer
     Received 13559 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 301 multicast, 0 pause input
```

```
1396 packets output, 126546 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
195 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es la dirección MAC para la interfaz G0/1 en el R1? _____

¿Cuál es el número de serie de la dirección MAC para G0/1? _____

¿Cuál es el OUI para G0/1? _____

Según este OUI, ¿cuál es el nombre del proveedor?_____

¿Qué significa BIA? _____

¿Por qué el resultado muestra la misma dirección MAC dos veces?

_____

b. Otra forma de mostrar las direcciones MAC en el router es por medio del comando **show arp**. Utilice el comando **show arp** para mostrar la información de la dirección MAC. Este comando asigna la dirección de capa 2 a su correspondiente dirección de capa 3. A continuación, se presenta un ejemplo. Utilice los resultados que genera el router para contestar las preguntas.

R1> **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	30f7.0da3.1821	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	0	c80a.a9fa.de0d	ARPA	GigabitEthernet0/1

¿Qué direcciones de capa 2 se muestran en el R1?

_____

¿Qué direcciones de capa 3 se muestran en el R1?

_____

¿Por qué piensa que no se muestra información para el switch con el comando **show arp**?

_____

Paso 3: Vea las direcciones MAC en el switch.

a. Acceda al switch mediante el puerto de consola y utilice el comando **show interfaces** para los puertos 5 y 6 para mostrar la información de la dirección MAC. A continuación, se presenta un ejemplo. Utilice los resultados que genera el switch para contestar las preguntas.

Switch> **show interfaces f0/5**

```
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.7285 (bia 0cd9.96e8.7285)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:45, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     3362 packets input, 302915 bytes, 0 no buffer
     Received 265 broadcasts (241 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 241 multicast, 0 pause input
     0 input packets with dribble condition detected
     38967 packets output, 2657748 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es la dirección MAC para la interfaz F0/5 en el switch? _____

Emita el mismo comando y anote la dirección MAC para F0/6. _____

¿Los OUI que se muestran en el switch son iguales a los que se mostraron en el router?

_____

El switch rastrea los dispositivos mediante sus direcciones MAC de capa 2. En la topología, el switch conoce la dirección MAC del R1 y la dirección MAC de la PC-A.

b. Emita el comando **show mac address-table** en el switch. A continuación, se presenta un ejemplo. Utilice los resultados que genera el switch para contestar las preguntas.

Switch> **show mac address-table**

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    30f7.0da3.1821    DYNAMIC     Fa0/5
   1    c80a.a9fa.de0d    DYNAMIC     Fa0/6
Total Mac Addresses for this criterion: 22
```

¿El switch mostró la dirección MAC de la PC-A? Si la respuesta fue afirmativa, ¿en qué puerto estaba?

_____

¿El switch mostró la dirección MAC del R1? Si la respuesta fue afirmativa, ¿en qué puerto estaba?

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.				

5. Resultados

a. ¿Puede tener broadcasts en el nivel de capa 2? Si la respuesta es afirmativa, ¿cuál sería la dirección MAC?

_____

_____

b. ¿Por qué necesitaría saber la dirección MAC de un dispositivo?

_____

_____

6. Conclusiones

A nivel de capa 2 (Enlace de datos) se emplean las direcciones MAC para lograr la comunicación entre los dispositivos.

Las direcciones MAC se emplean tanto para establecer comunicación de tipo Unicast, Multicast y BroadCast.

7. Sugerencias y /o recomendaciones:

Revisar en la plataforma de CISCO NetAcad el tema referente a : 5.0.1.2 Join My Social Circle

8. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 8

Uso de Wireshark para examinar tramas de Ethernet

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Examinar los campos de encabezado en una trama de Ethernet II
- Utilizar Wireshark para capturar y analizar tramas de Ethernet

2. Fundamento Teórico

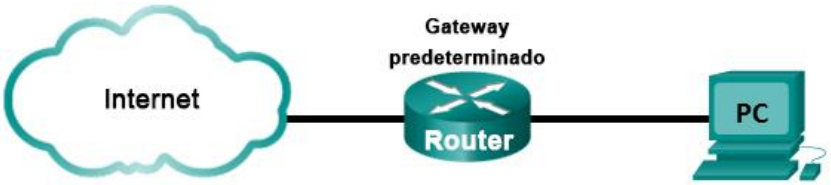
Cuando los protocolos de la capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas de interconexión de sistema abierto (OSI) y se encapsulan en la trama de la capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si los protocolos de capa superior son TCP e IP, y el acceso al medio es Ethernet, la encapsulación de la trama de la capa 2 será Ethernet II. Esto es típico de un entorno LAN.

Cuando se aprende sobre los conceptos de la capa 2, es útil analizar la información del encabezado de la trama. En la primera parte de esta práctica de laboratorio, revisará los campos incluidos en una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar los campos de encabezado de la trama de Ethernet II para el tráfico local y remoto.

3. Equipos, Materiales y Reactivos

- 1 PC (Windows 7, Vista o XP con acceso a Internet y Wireshark instalado)

4. Procedimientos:



Parte 1: Examinar los campos de encabezado en una trama de Ethernet II

En la parte 1, examinará los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de estos campos.

Paso 1: Revisar las descripciones y las longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

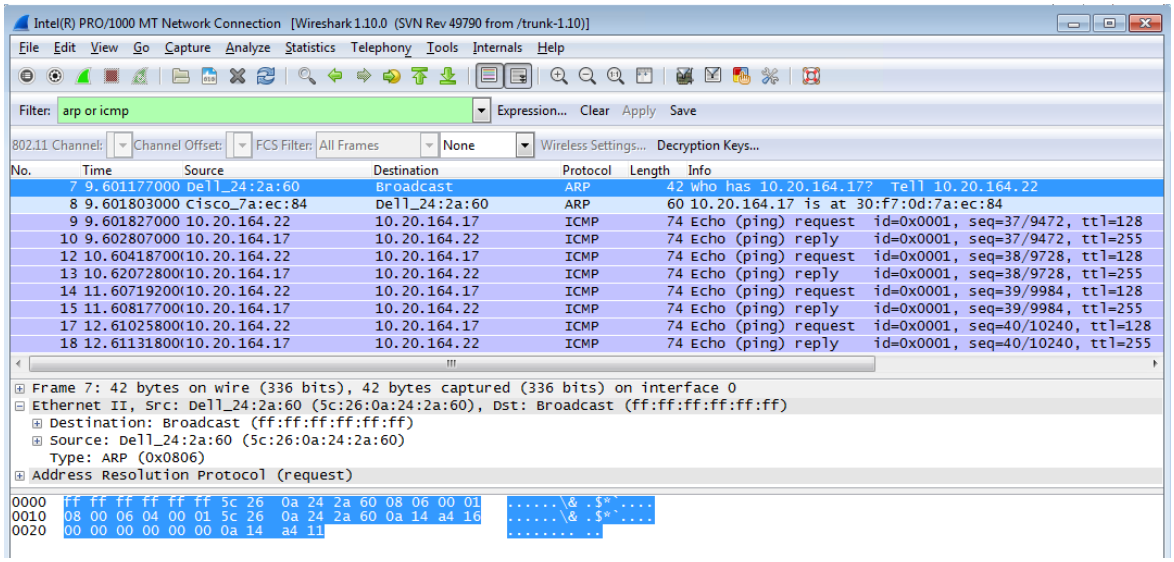
Paso 2: Examinar la configuración de red de la PC

La dirección IP del host de esta PC es 10.20.164.22 y la dirección IP del gateway predeterminado es 10.20.164.17.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : cisco.com
   Vínculo: dirección IPv6 local. . . . . : fe80::b875:731b:3c7b:c0b1
   Dirección IPv4. . . . . . . . . . . . . : 10.20.164.22
   Máscara de subred . . . . . . . . . . . : 255.255.255.240
   Puerta de enlace predeterminada . . . . . : 10.20.164.17
```

Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

En la siguiente captura de Wireshark, se muestran los paquetes que generó un ping que se emitió desde un host de la PC hasta su gateway predeterminado. Se aplicó un filtro a Wireshark para ver los protocolos ARP e ICMP únicamente. La sesión comienza con una consulta de ARP para la dirección MAC del router del gateway, seguida de cuatro solicitudes y respuestas de ping.



Paso 4: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP

En la tabla siguiente, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada como 12 dígitos hexadecimales, 0-9, A-F. Un formato común es 12:34:56:78:9A:BC. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC); los seis últimos números hexadecimales corresponden al número de serie de la NIC. La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast.
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)	
Tipo de trama	0x0806	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior que admite Ethernet II. Dos tipos comunes de trama son: Valor Descripción 0x0800 Protocolo IPv4 0x0806 Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 y 1,500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica.

¿Qué es importante acerca del contenido del campo de la dirección de destino?

_____

_____

¿Por qué la PC envía un broadcast de ARP antes de enviar la primera solicitud de ping?

_____

_____

_____

¿Cuál es la dirección MAC del origen en la primera trama? _____

¿Cuál es la ID de proveedor (OUI) de la NIC de origen? _____

¿Qué parte de la dirección MAC es la OUI?

_____

¿Cuál es el número de serie de la NIC de origen? _____

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

En la parte 2, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego examinará la información incluida en los campos de encabezado de la trama.

Paso 1: Determinar la dirección IP del gateway predeterminado en la PC

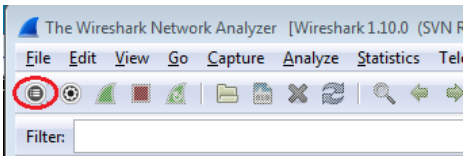
Abra una ventana del símbolo del sistema y emita el comando **ipconfig**.

¿Cuál es la dirección IP del gateway predeterminado de la PC? _____

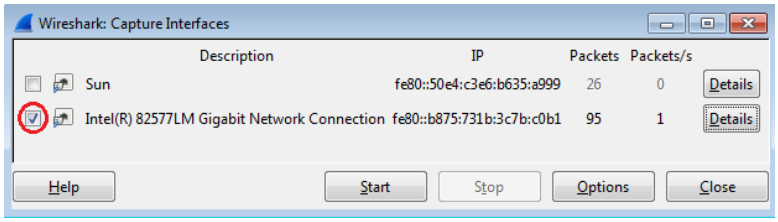
Paso 2: Iniciar la captura de tráfico en la NIC de la PC

a. Abra Wireshark.

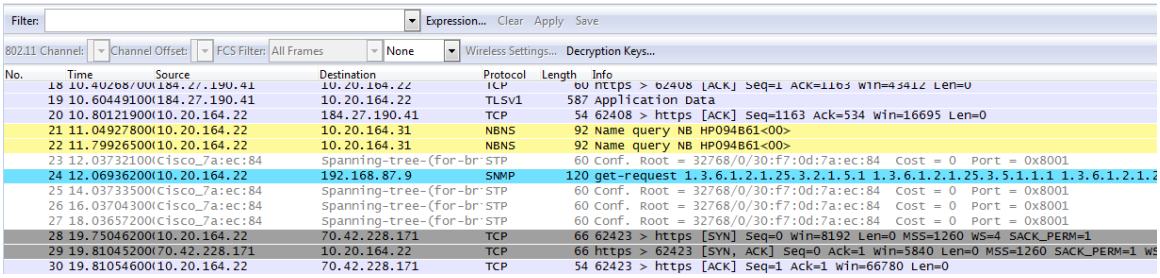
b. En la barra de herramientas de Wireshark Network Analyzer, haga clic en el ícono **Interface List** (Lista de interfaces).



c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), seleccione la interfaz para iniciar la captura de tráfico haciendo clic en la casilla de verificación apropiada, y luego haga clic en **Start** (Comenzar). Si no está seguro de qué interfaz activar, haga clic en **Details** (Detalles) para obtener más información sobre cada interfaz enumerada.



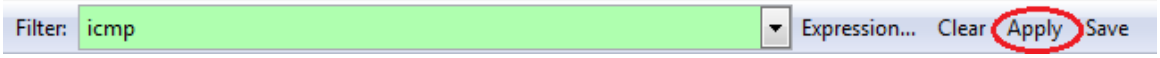
d. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).



Paso 3: Filtrar Wireshark para mostrar solamente el tráfico de ICMP

Puede utilizar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra lo que se muestra en la pantalla. Por ahora, solo se debe ver el tráfico de ICMP.

En el cuadro **Filter** (Filtrar) de Wireshark, escriba **icmp**. Si escribió el filtro correctamente, el cuadro se volverá verde. Si el cuadro está de color verde, haga clic en **Apply** (Aplicar) para aplicar el filtro.

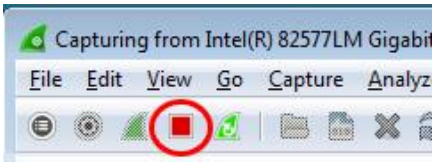


Paso 4: En la ventana del símbolo del sistema, haga ping al gateway predeterminado de la PC

En esta ventana, utilice la dirección IP que registró en el paso 1 para hacer ping al gateway predeterminado.

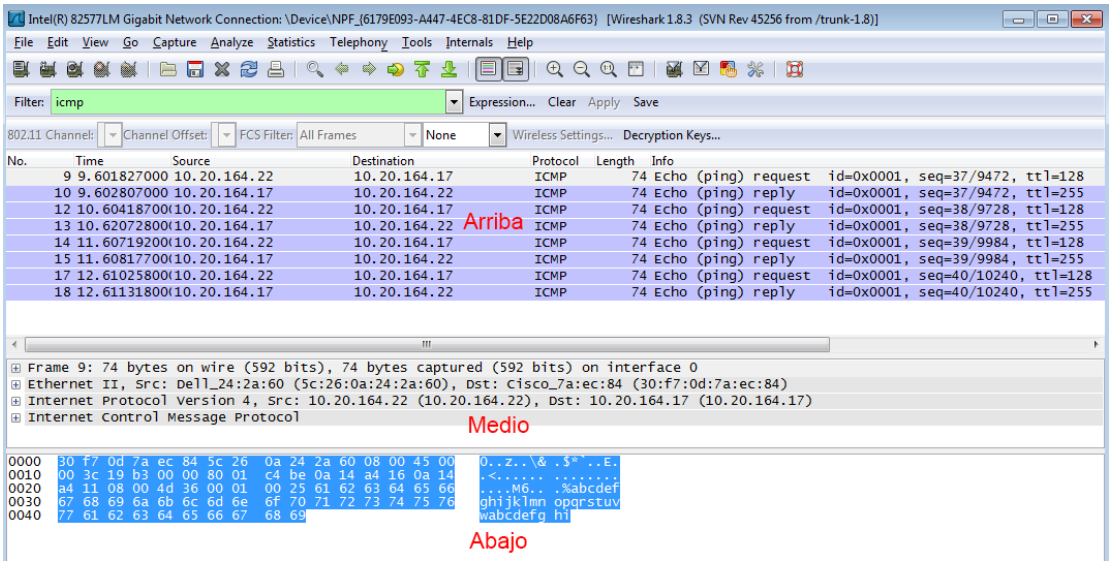
Paso 5: Detener la captura de tráfico en la NIC

Haga clic en el ícono **Stop Capture** (Detener captura) para detener la captura de tráfico.



Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark

La ventana principal de Wireshark está dividida en tres secciones: el panel de la lista de paquetes (Arriba), el panel de detalles del paquete (Medio) y el panel de bytes del paquete (Abajo). Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark mostrará la información ICMP en el panel de la lista de paquetes de Wireshark, como se muestra en el ejemplo siguiente.



a. En el panel de la lista de paquetes (sección superior), haga clic en la primera trama que se indica. Debería ver **Echo (ping) request** (Solicitud de eco [ping]) debajo del encabezado **Info** (Información). Esta acción debería resaltar la línea en color azul.

b. Examine la primera línea del panel de detalles del paquete (sección media). En esta línea, se muestra la longitud de la trama; 74 bytes en este ejemplo.

c. En la segunda línea del panel de detalles del paquete, se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y destino.

¿Cuál es la dirección MAC de la NIC de la PC? _____

¿Cuál es la dirección MAC del gateway predeterminado? _____

d. Puede hacer clic en el signo más (+) que se encuentra al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo más cambia al signo menos (-).

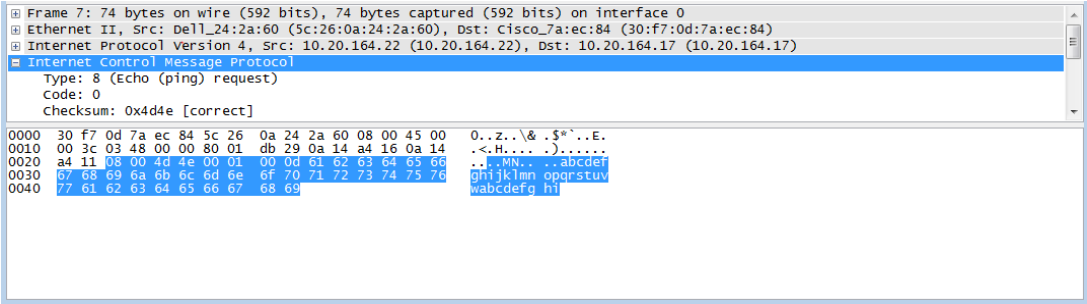
¿Qué tipo de trama se muestra? _____

e. Las dos últimas líneas que se muestran en la sección media proporcionan información sobre el campo de datos de la trama. Observe que los datos contienen la información de la dirección IPv4 de origen y destino.

¿Cuál es la dirección IP de origen? _____

¿Cuál es la dirección IP de destino? _____

f. Puede hacer clic en cualquier línea de la sección media para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel de bytes del paquete (sección inferior). Haga clic en la línea **Internet Control Message Protocol** (Protocolo de mensajes de control de Internet) en la sección media y examine qué está resaltado en el panel de bytes del paquete.



¿Qué indican los dos últimos octetos resaltados? _____

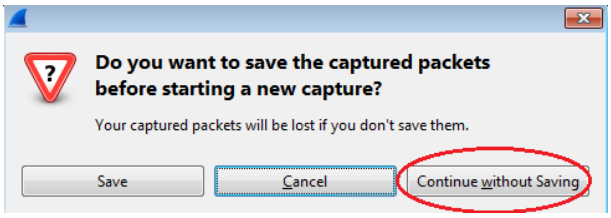
g. Haga clic en la trama siguiente de la sección superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y destino se invirtieron, porque esta trama se envió desde el router del gateway predeterminado como una respuesta al primer ping.

¿Qué dirección de dispositivo y dirección MAC se muestran como la dirección de destino?

_____

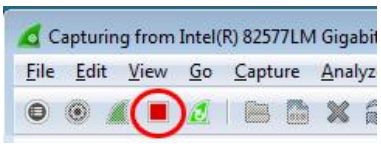
Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono **Start Capture** (Iniciar captura) para iniciar una nueva captura de Wireshark. Aparece una ventana emergente en la que se le pregunta si desea guardar los paquetes capturados anteriormente en un archivo antes de iniciar una nueva captura. Haga clic en **Continue without Saving** (Continuar sin guardar).



Paso 8: En la ventana del símbolo del sistema, hacer ping a www.cisco.com

Paso 9: Detener la captura de paquetes



Paso 10: Examinar los datos nuevos en el panel de la lista de paquetes de Wireshark

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y destino?

Origen: _____

Destino: _____

¿Cuáles son las direcciones IP de origen y destino incluidas en el campo de datos de la trama?

Origen: _____

Destino: _____

Compare estas direcciones con las direcciones que recibió en el paso 7. La única dirección que cambió es la dirección IP de destino. ¿Por qué la dirección IP de destino cambió y la dirección MAC de destino siguió siendo la misma?

_____

_____

_____

_____

5. Resultados

Wireshark no muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

_____

_____

6. Conclusiones

Wireshark permite capturar y analizar tramas de Ethernet, pero es sumamente deseable entender la pila de protocolos TCP/IP para obtener información útil.

7. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a: Visualización de direcciones MAC de dispositivos de red.

8. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 9

Observación del protocolo ARP mediante la CLI de Windows, la CLI del IOS y Wireshark

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo (de la práctica):**

Al finalizar el laboratorio el estudiante podrá:

- Utilizar el comando ARP de Windows
- Utilizar el comando show ARP del IOS
- Utilizar Wireshark para examinar los intercambios ARP

2. **Fundamento Teórico**

TCP/IP utiliza el protocolo de resolución de direcciones (ARP) para asignar una dirección IP de capa 3 a una dirección MAC de capa 2. Cuando se coloca una trama en la red, debe tener una dirección MAC de destino. Para descubrir dinámicamente la dirección MAC del dispositivo de destino, se transmite una solicitud de ARP en la LAN. El dispositivo que contiene la dirección IP de destino responde, y la dirección MAC se registra en la caché ARP. Cada dispositivo en la LAN mantiene su propio caché ARP, o un área pequeña en RAM que contiene los resultados ARP. Un cronómetro de caché de ARP elimina las entradas ARP que no se han usado por un determinado período de tiempo.

ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN. Por el contrario, los tiempos de espera ilimitados podrían provocar errores con dispositivos que dejan la red o cambiar la dirección de la Capa 3.

Un administrador de red debe estar al tanto del ARP, pero es posible que no interactúe con el protocolo regularmente. ARP es un protocolo que permite que los dispositivos de red se comuniquen con el protocolo TCP/IP. Sin ARP no hay un método eficiente para construir el datagrama de la dirección de destino de la Capa 2. También, ARP es un riesgo de seguridad potencial. La suplantación de identidad de ARP, o envenenamiento de ARP, es una técnica usada por un atacante para inyectar una dirección MAC incorrecta asociada a una red. Un atacante falsifica la dirección MAC de un dispositivo y las tramas son enviadas a un destino equivocado. Configurar manualmente asociaciones ARP estáticas es una manera de impedir la suplantación de identidad de ARP. Por último, se puede configurar una lista de direcciones MAC autorizadas en los dispositivos Cisco para restringir el acceso a la red solo a los dispositivos aprobados.

En esta práctica de laboratorio, utilizará los comandos ARP tanto en los routers Windows como Cisco para visualizar la tabla ARP. También borrará la caché ARP y agregará entradas ARP estáticas.

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

3. **Equipos, Materiales y Reactivos**

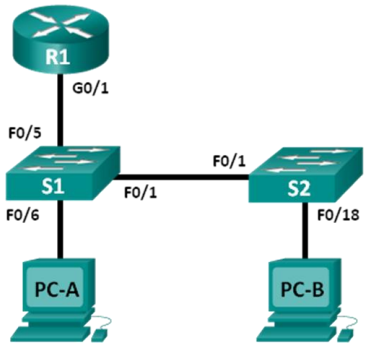
- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])

- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal instalado, por ejemplo, Tera Term y Wireshark)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

4. Procedimientos:

Parte 1: Armar y configurar la red

Paso 1: Tender el cableado de red de acuerdo con la topología



Paso 2: Configurar las direcciones IP de los dispositivos de acuerdo con la tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Paso 3: Verificar la conectividad de red haciendo ping a todos los dispositivos de la PC-B

Parte 2: Usar el comando ARP de Windows

El comando **arp** permite al usuario ver y modificar la caché ARP en Windows. A este comando se accede desde el símbolo del sistema de Windows.

Paso 1: Visualizar la caché ARP

a. Abra una ventana de comandos en la PC-A y escriba **arp**.

C:\Users\User1> **arp**

```
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
```

```
  eth_addr       Specifies a physical address.
  if_addr        If present, this specifies the Internet address of the
                 interface whose address translation table should be modified.
                 If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

b. Observe el resultado.

¿Qué comando se usaría para mostrar todas las entradas en la caché ARP? _____

¿Qué comando se usaría para eliminar todas las entradas de la caché ARP (purgar la caché ARP)?

_____

¿Qué comando se usaría para eliminar la entrada de la caché ARP para 192.168.1.11?

_____

c. Escriba **arp –a** para visualizar la tabla ARP.

C:\Users\User1> **arp –a**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Nota: la tabla ARP está vacía si utiliza Windows XP (como se muestra a continuación).

C:\Documents and Settings\User1> **arp -a**

No ARP Entries Found.

d. Haga ping de la PC-A a la PC-B para agregar dinámicamente entradas de la caché ARP.

C:\Documents and Settings\User1> **ping 192.168.1.2**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

¿Cuál es la dirección física para el host con dirección IP 192.168.1.2? _____

Paso 2: Ajustar las entradas en la caché ARP manualmente

Para eliminar las entradas en la caché ARP, emita el comando **arp –d {inet-addr | *}**. Las direcciones se pueden eliminar de manera individual al especificar la dirección IP, o bien todas juntas con el wildcard *. Verifique que la caché ARP contenga las entradas siguientes: el gateway predeterminado R1 G0/1 (192.168.1.1), la PC-B (192.168.1.2) y los dos switches (192.168.1.11 y 192.168.1.12).

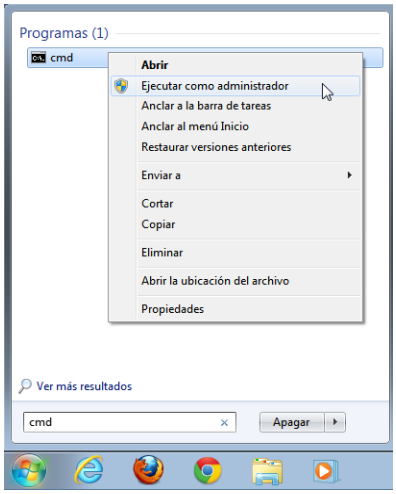
a. En la PC-A, haga ping a todas las direcciones de la tabla de direcciones.

b. Verifique que todas las direcciones se hayan agregado a la caché ARP. Si la dirección no está en la caché ARP, haga ping a la dirección de destino y verifique que se haya agregado a la caché ARP.

C:\Users\User1> **arp –a**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

c. Como administrador, acceda al símbolo del sistema. Haga clic en el ícono **Inicio** y, en el cuadro *Buscar programas y archivo*, escriba **cmd**. Cuando aparezca el ícono **cmd**, haga clic con el botón secundario en él y seleccione **Ejecutar como administrador**. Haga clic en **Sí** para permitir que este programa realice los cambios.



d. En la ventana del símbolo del sistema Administrador, escriba **arp –d ***. Este comando elimina todas las entradas de la caché ARP. Verifique que todas las entradas de la caché ARP se hayan eliminado; para eso, escriba **arp-a** en el símbolo del sistema.

C:\windows\system32> **arp –d ***
C:\windows\system32> **arp –a**

```
No ARP Entries Found.
```

e. Espere unos minutos. El protocolo de descubrimiento de vecinos comienza a llenar la caché ARP nuevamente.

C:\Users\User1> **arp –a**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

f. En la PC-A, haga ping a la PC-B (192.168.1.2) y a los switches (192.168.1.11 y 192.168.1.12) para agregar las entradas ARP. Verifique que las entradas ARP se hayan agregado a la caché.

C:\Users\User1> **arp –a**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

g. Registre la dirección física del switch S2. _____

h. Elimine una entrada de caché ARP específica escribiendo **arp –d *inet-addr***. En el símbolo del sistema, escriba **arp –d 192.168.1.12** para eliminar la entrada ARP para el S2.

C:\windows\system32> **arp –d 192.168.1.12**

i. Escriba **arp –a** para verificar que la entrada ARP para el S2 se eliminó de la caché ARP.

C:\Users\User1> **arp –a**

```
Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

j. Puede agregar una entrada de caché ARP específica escribiendo **arp –s *inet_addr_mac_addr***. En este ejemplo, se utilizará la dirección IP y la dirección MAC para el S2. Use la dirección MAC registrada en el paso g.

C:\windows\system32> **arp –s 192.168.1.12 0c-d9-96-d2-40-40**

k. Verifique que la entrada ARP para el S2 se haya agregado a la caché.

l.

Parte 3: Utilizar el comando show arp del IOS

Cisco IOS también puede mostrar la caché ARP en los routers y switches mediante el comando **show arp** o **show ip arp**.

Paso 1: Mostrar las entradas ARP del router R1

R1# **show arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0   0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

Observe que no hay ningún valor de Age (-) para la primera entrada, la interfaz del router G0/1 (el gateway predeterminado de LAN). Age es la cantidad de minutos (min) que la entrada estuvo en la caché ARP y se incrementa para las otras entradas. El protocolo de descubrimiento de vecinos llena las entradas ARP de las direcciones IP y MAC de la PC-A y la PC-B.

Paso 2: Agregar entradas ARP del router R1

Puede agregar entradas ARP a la tabla ARP del router haciendo ping a otros dispositivos.

a. Haga ping al switch S1.

R1# **ping 192.168.1.11**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. Verifique que una entrada ARP para el switch S1 se haya agregado a la tabla ARP del R1.

R1# **show ip arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            6   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            6   0050.56be.768c  ARPA   GigabitEthernet0/1
Internet  192.168.1.11           0   0cd9.96e8.8a40  ARPA   GigabitEthernet0/1
R1#
```

Paso 3: Mostrar las entradas ARP del switch S1

S1# **show ip arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             46   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2              8   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3              8   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
S1#
```

Paso 4: Agregar entradas ARP en el switch S1

Al hacer ping a otros dispositivos, también se puede agregar entradas ARP a la tabla ARP del switch.

a. En el switch S1, haga ping al switch S2.

S1# **ping 192.168.1.12**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

b. Verifique que la entrada ARP para el switch S2 se haya agregado a la tabla ARP del S1.

S1# **show ip arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             5   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2            11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3            11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11            -   0cd9.96e8.8a40  ARPA   Vlan1
Internet  192.168.1.12            2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

Parte 4: Utilizar Wireshark para examinar los intercambios ARP

En la parte 4, examinará los intercambios ARP mediante Wireshark para capturar y evaluar el intercambio ARP. También examinará la latencia de red que causan los intercambios ARP entre los dispositivos.

Paso 1: Configurar Wireshark para las capturas de paquetes

a. Inicie Wireshark.

b. Elija la interfaz de red que desea usar para capturar los intercambios ARP.

Paso 2: Capturar y evaluar las comunicaciones del ARP

a. Inicie la captura de paquetes en Wireshark. Utilice el filtro para mostrar solamente los paquetes ARP.

b. Purgue la caché ARP; para eso, escriba el comando **arp –d *** en el símbolo del sistema.

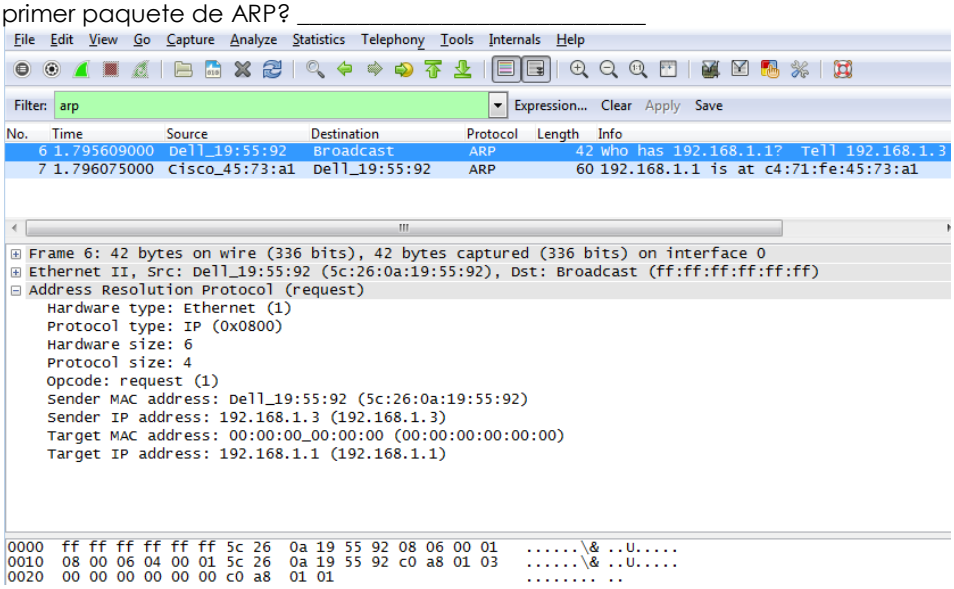
c. Verifique que la caché ARP se haya borrado.

d. Envíe un ping al gateway predeterminado mediante el comando **ping 192.168.1.1**.

e. Después de hacer ping al gateway predeterminado, detenga la captura de Wireshark.

f. Examine las capturas de Wireshark para los intercambios ARP en el panel de detalles del paquete.

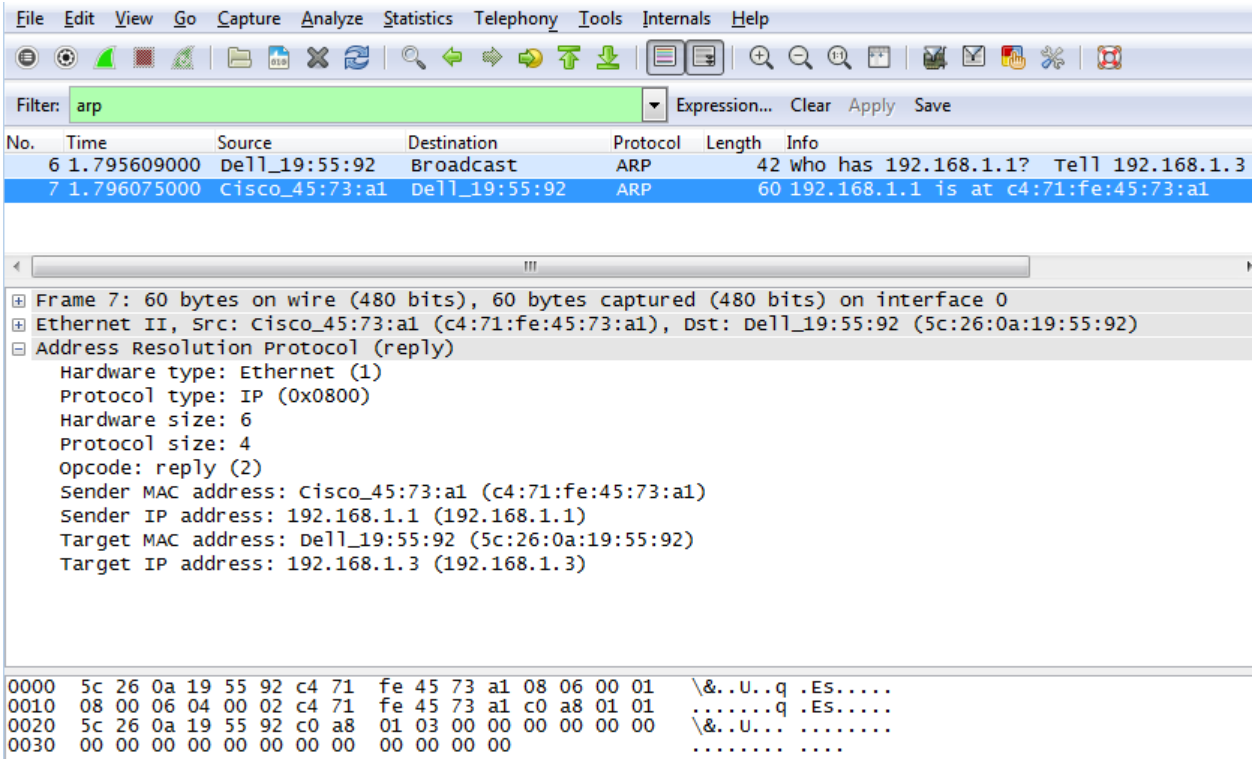
¿Cuál fue el primer paquete de ARP? _____



Complete la siguiente tabla con información sobre el primer paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

¿Cuál fue el segundo paquete de ARP? _____



Complete la siguiente tabla con información sobre el segundo paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

Paso 3: Examinar la latencia de red que causa el ARP

a. Borre las entradas ARP de la PC-A.

b. Inicie una captura de Wireshark.

c. Haga ping al switch S2 (192.168.1.12). El ping debe ser correcto después de la primera solicitud de eco.

Nota: si todos los pings son correctos, el S1 debe volver a cargarse para observar la latencia de red con el ARP.

C:\Users\User1> **ping 192.168.1.12**

```
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255


Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

d. Una vez finalizado el ping, detenga la captura de Wireshark. Utilice el filtro de Wireshark para mostrar solamente los resultados de ARP e ICMP. En Wireshark, escriba **arp o icmp** en el área de entrada **Filter:** (Filtro:).

e. Examine la captura de Wireshark. En este ejemplo, la trama 10 es la primera solicitud de ICMP que se envía de la PC-A al S1. Dado que no hay una entrada ARP para el S1, se envió una solicitud de ARP a la dirección IP de administración del S1 en la que se solicita la dirección MAC. Durante los intercambios ARP, la solicitud de eco no recibió una respuesta antes de agotarse el tiempo de espera de la solicitud. (Tramas 8 a 12)

Después de que la entrada ARP para el S1 se agregó a la caché ARP, los últimos tres intercambios ICMP fueron correctos, como se muestra en las tramas 26, 27 y 30-33.

Como se muestra en la captura de Wireshark, ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN.

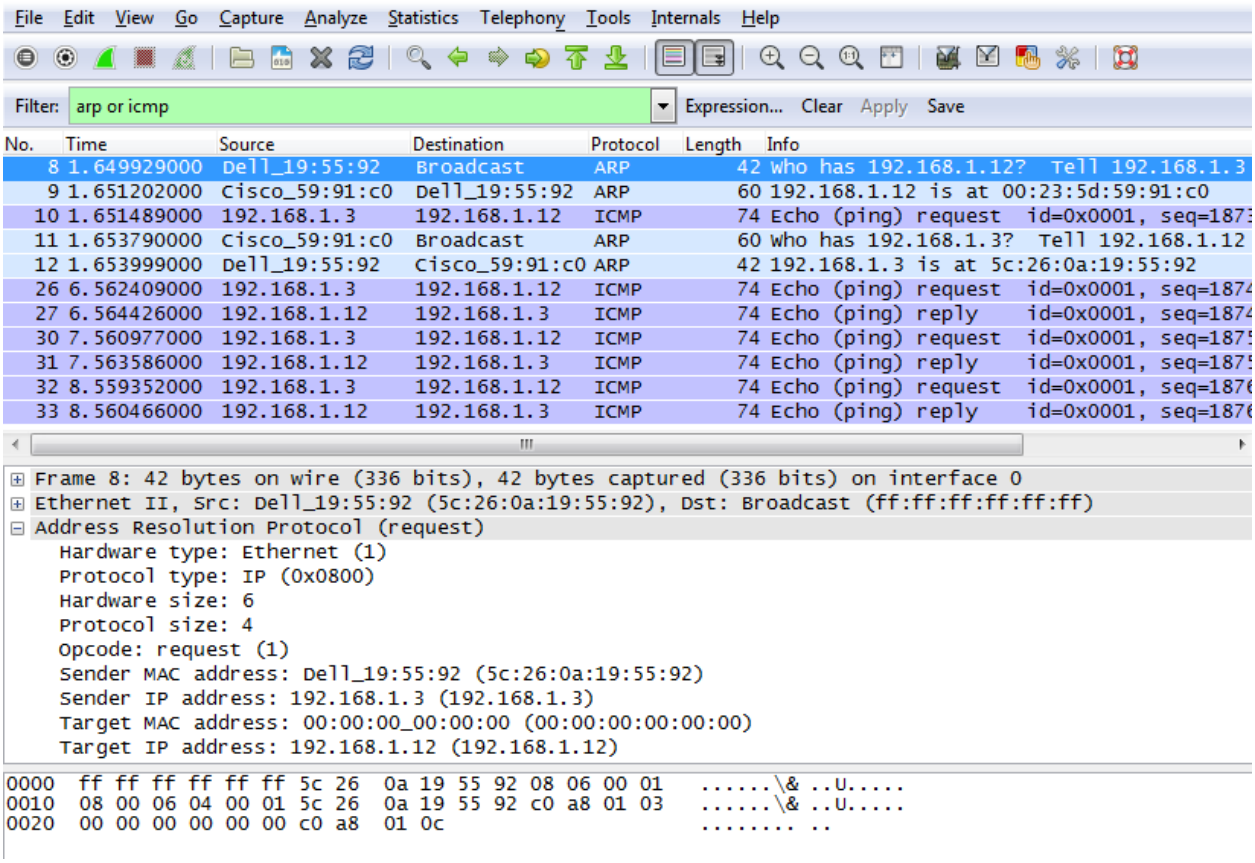


Tabla de resumen de interfaces del router

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.

5. Resultados

a. ¿Cómo y cuándo se quitan las entradas ARP estáticas?

_____

b. ¿Por qué desea agregar entradas ARP estáticas en la caché?

_____

c. Si las solicitudes ARP pueden causar latencia de red, ¿por qué no es conveniente tener tiempos de espera ilimitados para las entradas ARP?

_____

6. Conclusiones

El protocolo ARP es empleado por los Hosts para determinar las direcciones IP de los dispositivos

considerando la dirección MAC que se proporcione.

7. **Sugerencias y /o recomendaciones**
   Revisar en la plataforma de CISCO NetAcad el tema referente a: Uso de la CLI del IOS con las tablas de direcciones MAC del switch.

8. **Referencias bibliográficas consultadas y/o enlaces recomendados**
   - Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 10

Armado de una red de switch y router

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Establecer la topología e inicializar los dispositivos
- Configurar dispositivos y verificar la conectividad
- Mostrar información del dispositivo

2. Fundamento Teórico

Esta es una práctica de laboratorio exhaustiva para repasar los comandos del IOS que se abarcaron anteriormente. En esta práctica 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.

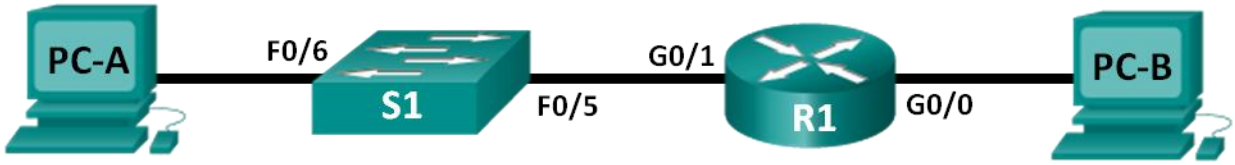
En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos reales necesarios para configurar el router. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento intentando configurar los dispositivos sin consultar el apéndice.

3. Equipos, Materiales y Reactivos

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

4. Procedimientos:

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: Emplee la siguiente tabla de direccionamiento:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	No aplicable
	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	No aplicable	No aplicable	No aplicable
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Paso 3: 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. Consulte**¡Error! No se encuentra el origen de la referencia.** y**¡Error! No se encuentra el origen de la referencia.** 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
```

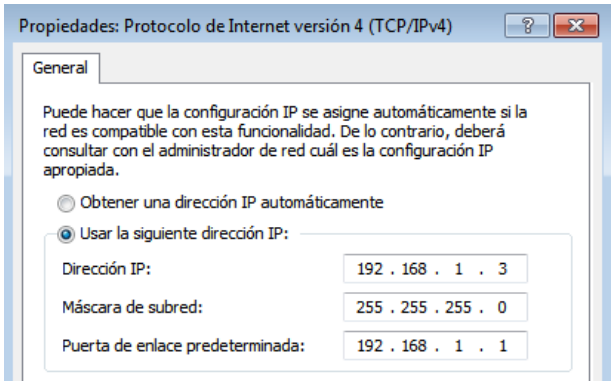
```
GigabitEthernet0/2     unassigned      YES unset  down                  down
Switch#
```

Tabla de resumen de interfaces del router

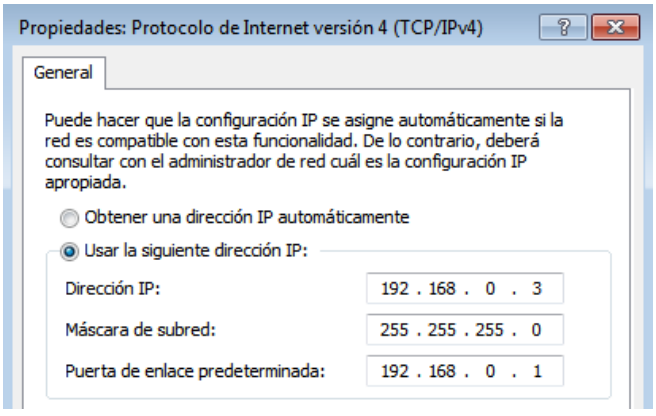
Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet #2**	**Interfaz serial #1**	**Interfaz serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (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.				

Paso 8: Configure las interfaces de la PC.

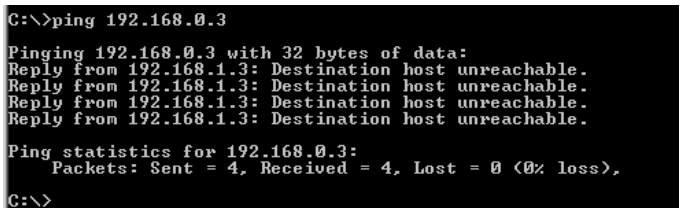
a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.



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.



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**

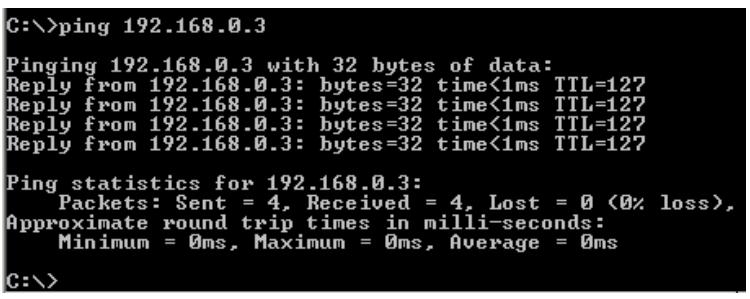
R1#

*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.



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>

5. Resultados

a. Si la interfaz G0/1 se mostrara administrativamente inactiva, ¿qué comando de configuración de interfaz usaría para activar la interfaz?

_____

b. ¿Qué ocurriría si hubiera configurado incorrectamente la interfaz G0/1 en el router con una dirección IP 192.168.1.2?

_____

_____

_____

_____

6. Conclusiones

Tanto los Switches como los routers requieren ser configurados para obtener el mejor rendimiento posible de acuerdo a la topología de red que se requiera.

7. Sugerencias y /o recomendaciones
Revisar en la plataforma de CISCO NetAcad el tema referente a : Exploración de las características físicas del router

8. Referencias bibliográficas consultadas y/o enlaces recomendados:
Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 11

Uso de Wireshark para examinar una captura de UDP y DNS

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Registrar la información de configuración IP de una PC
- Utilizar Wireshark para capturar consultas y respuestas DNS
- Analizar los paquetes DNS o UDP capturados

2. Fundamento Teórico

Si alguna vez usó Internet, usó el Sistema de nombres de dominios (DNS). El DNS es una red distribuida de servidores que traduce nombres de dominio fáciles de usar, como www.google.com, en una dirección IP. Cuando escribe el URL de un sitio Web en el explorador, la PC realiza una consulta DNS a la dirección IP del servidor DNS. La consulta del servidor DNS de la PC y la respuesta del servidor DNS utilizan el protocolo de datagramas de usuario (UDP) como el protocolo de la capa de transporte. UDP opera sin conexión y no requiere una configuración de sesión como TCP. Las consultas y respuestas DNS son muy pequeñas y no requieren la sobrecarga de TCP.

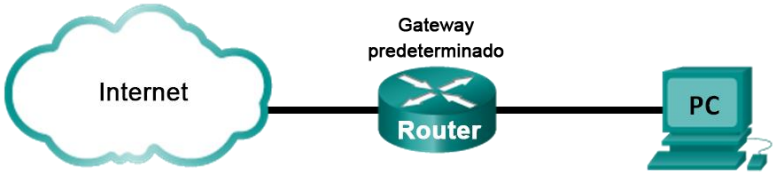
En esta práctica de laboratorio, se comunicará con un servidor DNS enviando una consulta DNS mediante el protocolo de transporte UDP. Utilizará Wireshark para examinar los intercambios de consultas y respuestas DNS con el servidor de nombres.

3. Equipos, Materiales y Reactivos

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

4. Procedimientos:

Topologia:



Parte 1: Registrar la información de configuración IP de la PC

En la parte 1, utilizará el comando **ipconfig /all** en la PC local para buscar y registrar las direcciones MAC e IP de la tarjeta de interfaz de red (NIC) de la PC, la dirección IP del gateway predeterminado especificado y la dirección IP del servidor DNS especificada para la PC. Registre esta información en la

tabla proporcionada. La información se utilizará en las partes siguientes de esta práctica de laboratorio con análisis de paquetes.

Dirección IP	
Dirección MAC	
Dirección IP de la puerta de enlace predeterminada	
Dirección IP del servidor DNS	

Part 119557697: Utilizar Wireshark para capturar consultas y respuestas DNS

En la parte 2, configurará Wireshark para capturar paquetes de consultas y respuestas DNS para demostrar el uso del protocolo de transporte UDP mientras se comunica con un servidor DNS.

a. Haga clic en el botón **Inicio** de Windows y navegue hasta el programa Wireshark.

Nota: si Wireshark aún no está instalado, se puede descargar de http://www.wireshark.org/download.html.

b. Seleccione una interfaz para que Wireshark capture paquetes. Utilice **Interface List** (Lista de interfaces) para elegir la interfaz asociada a las direcciones IP y de control de acceso al medio (MAC) registradas de la PC en la parte 1.

c. Después de seleccionar la interfaz deseada, haga clic en **Start** (Comenzar) para capturar los paquetes.

d. Abra un explorador Web y escriba **www.google.com**. Presione Entrar para continuar.

e. Haga clic en **Stop** (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.

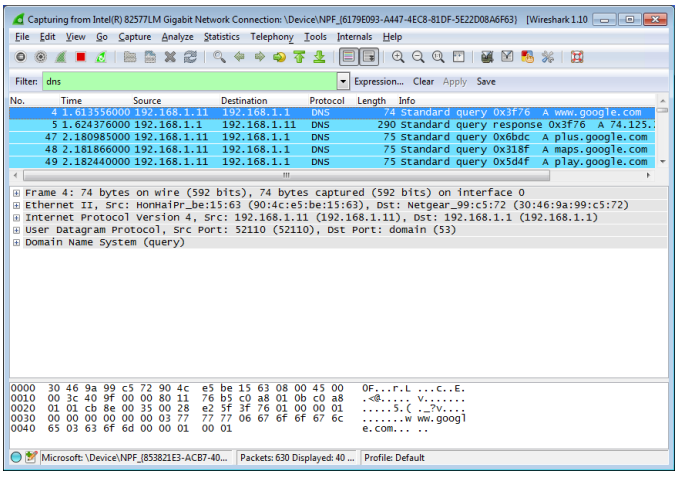
Parte 2: Analizar los paquetes DNS o UDP capturados

En la parte 3, examinará los paquetes UDP que se generaron al comunicarse con un servidor DNS para las direcciones IP para www.google.com.

Step 2: Filtrar paquetes DNS

a. En la ventana principal de Wireshark, escriba **dns** en el área de entrada de la barra de herramientas **Filter** (Filtrar). Haga clic en **Apply** (Aplicar) o presione Entrar.

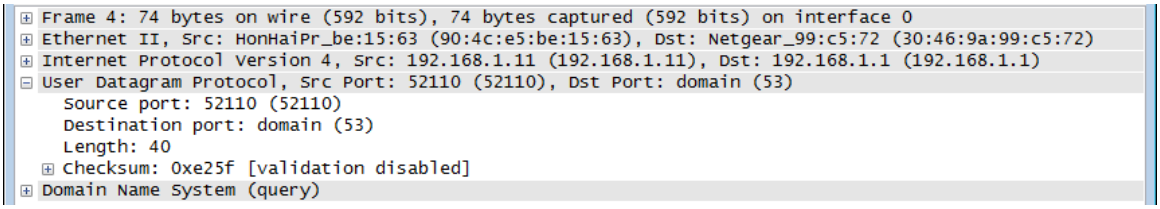
Nota: si no ve resultados después de aplicar el filtro DNS, cierre el explorador Web y, en la ventana del símbolo del sistema, escriba **ipconfig /flushdns** para eliminar todos los resultados anteriores del DNS. Reinicie la captura de Wireshark y repita las instrucciones de la parte 2b a la parte 2e. Si el problema no se resuelve, en la ventana del símbolo del sistema, puede escribir **nslookup www.google.com** como alternativa para el explorador Web.



b. En el panel de la lista de paquetes (sección superior) de la ventana principal, ubique el paquete que incluye "standard query" (consulta estándar) y "A www.google.com". Vea la trama 4, por ejemplo.

Step 3: Examinar el segmento UDP mediante una consulta DNS

Examine UDP mediante una consulta DNS para www.google.com según lo capturado por Wireshark. En este ejemplo, está seleccionada la trama 4 de la captura de Wireshark en la lista de paquetes para su análisis. Los protocolos en esta consulta se muestran en el panel de detalles del paquete (sección media) de la ventana principal. Las entradas del protocolo están resaltadas en gris.



a. En el panel de detalles del paquete, la trama 4 tenía 74 bytes de datos en el cable, tal como se muestra en la primera línea. Esta es la cantidad de bytes para enviar una consulta DNS a un servidor de nombres que solicita direcciones IP de www.google.com.

b. En la línea Ethernet II, se muestran las direcciones MAC de origen y destino. La dirección MAC de origen proviene de la PC local, ya que esta originó la consulta DNS. La dirección MAC de destino proviene del gateway predeterminado, dado que esta es la última parada antes de que la consulta abandone la red local.

¿La dirección MAC de origen es la misma que la que se registró en la parte 1 para la PC local?

_____

c. En la línea Internet Protocol Version 4 (Protocolo de Internet versión 4), la captura de Wireshark de paquetes IP indica que la dirección IP de origen de esta consulta DNS es 192.168.1.11 y la dirección IP de destino es 192.168.1.1. En este ejemplo, la dirección de destino es el gateway predeterminado. El router es el gateway predeterminado en esta red.

¿Puede emparejar las direcciones IP y MAC para los dispositivos de origen y destino?

Dispositivo	Dirección IP	Dirección MAC
PC local		
Gateway predeterminado		

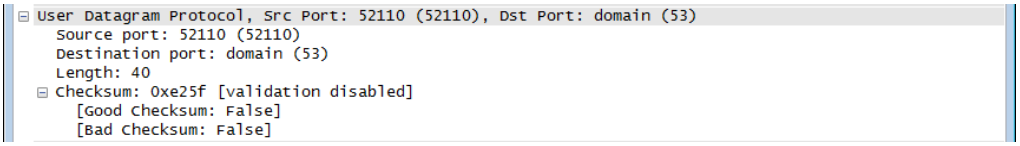
El paquete y el encabezado IP encapsulan el segmento UDP. El segmento UDP contiene la consulta DNS como los datos.

d. Un encabezado UDP solo tiene cuatro campos: source port (puerto de origen), destination port (puerto de destino), length (longitud) y checksum. Cada campo en el encabezado UDP es de solo 16 bits, como se ilustra a continuación.

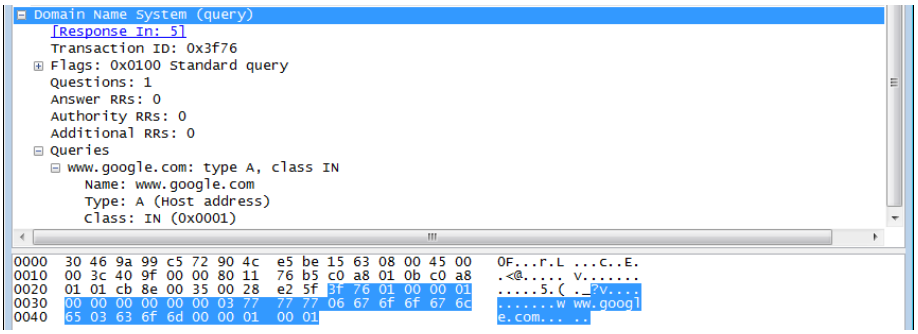
SEGMENTO UDP

0	16	31
PUERTO DE ORIGEN UDP	PUERTO DE DESTINO UDP	
LONGITUD DE MENSAJE UDP	CHECKSUM DE UDP	
DATOS		
DATOS...		

Amplíe el protocolo de datagramas de usuario en el panel de detalles del paquete haciendo clic en el signo más (+). Observe que hay solo cuatro campos. El número de puerto de origen en este ejemplo es 52110. La PC local generó el puerto de origen aleatoriamente utilizando los números de puerto que no están reservados. El puerto de destino es 53. El puerto 53 es un puerto conocido reservado para ser utilizado con DNS. En el puerto 53, los servidores DNS escuchan las consultas DNS de los clientes.



En este ejemplo, la longitud de este segmento UDP es de 40 bytes. De los 40 bytes, 8 bytes se utilizan como encabezado. Los otros 32 bytes los utilizan los datos de la consulta DNS. Estos 32 bytes están resaltados en la ilustración siguiente en el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.



El valor de checksum se usa para determinar la integridad del paquete después de haber atravesado Internet.

El encabezado UDP tiene una sobrecarga baja, porque UDP no tiene campos asociados con el protocolo de enlace de tres vías en TCP. Cualquier problema de confiabilidad de transferencia de datos que ocurra debe solucionarse en la capa de aplicación.

Registre los resultados de Wireshark en la tabla siguiente:

Tamaño de trama	
Dirección MAC de origen	
Dirección MAC de destino	
Dirección IP de origen	
Dirección IP de destino	
Puerto de origen	
Puerto de destino	

¿La dirección IP de origen es la misma que la dirección IP de la PC local registrada en la parte 1?

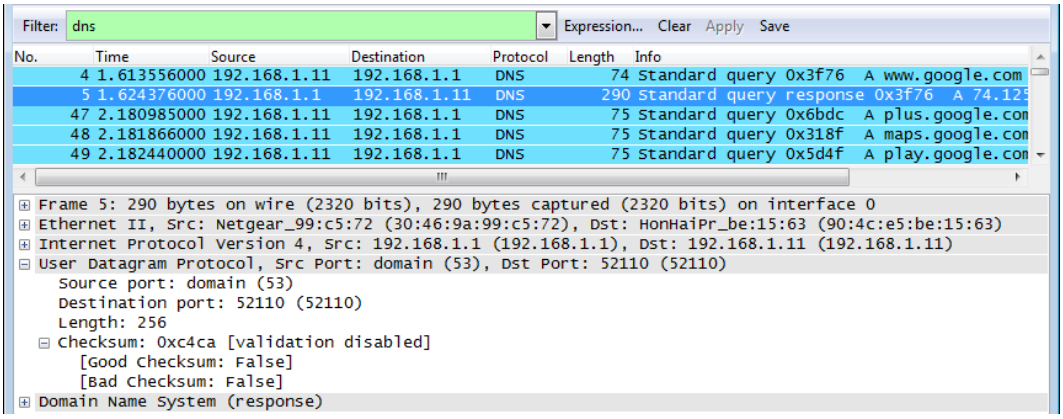
_____

¿La dirección IP de destino es la misma que el gateway predeterminado que se registró en la parte 1? _____

Step 4: Examinar el UDP usando la respuesta DNS

En este paso, examinará el paquete de respuesta DNS y verificará que este también utilice UDP.

a. En este ejemplo, la trama 5 es el paquete de respuesta DNS correspondiente. Observe que la cantidad de bytes en el cable es 290 bytes. Es un paquete más grande con respecto al paquete de consulta DNS.



b. En la trama Ethernet II para la respuesta DNS, ¿de qué dispositivo proviene la dirección MAC de origen y de qué dispositivo proviene la dirección MAC de destino?

c. Observe las direcciones IP de origen y destino en el paquete IP. ¿Cuál es la dirección IP de destino? ¿Cuál es la dirección IP de origen?

Dirección IP de destino: _____Dirección IP de origen: _____

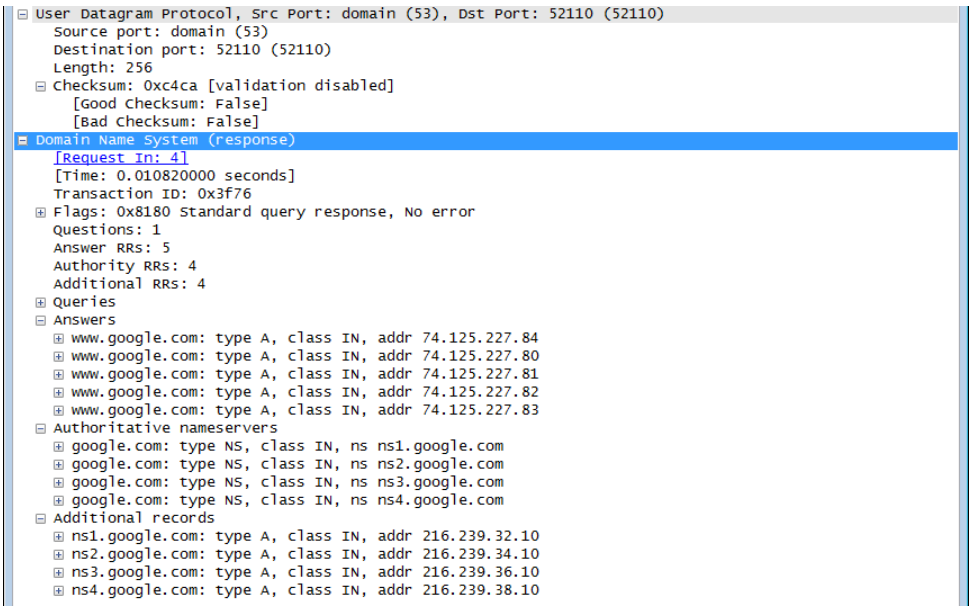
¿Qué ocurrió con los roles de origen y destino para el host local y el gateway predeterminado?

_____

d. En el segmento UDP, el rol de los números de puerto también se invirtió. El número de puerto de destino es 52110. El número de puerto 52110 es el mismo puerto que el que generó la PC local cuando se envió la consulta DNS al servidor DNS. La PC local escucha una respuesta DNS en este puerto.

El número de puerto de origen es 53. El servidor DNS escucha una consulta DNS en el puerto 53 y luego envía una respuesta DNS con un número de puerto de origen 53 de vuelta a quien originó la consulta DNS.

Cuando la respuesta DNS esté expandida, observe las direcciones IP resueltas para www.google.com en la sección **Answers** (Respuestas).



5. Resultados

¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para DNS?

_____

_____

_____

_____

6. Conclusiones

Al establecer una comunicación con un servidor de Internet, lo primero que sucede es se consultará a un servidor DNS enviando una consulta DNS mediante el protocolo de transporte UDP.
Esta consulta puede ser fácilmente interceptada y por ende también modificada.

7. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a: Uso de Wireshark para examinar capturas de FTP y TFTP.

8. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 12

Identificación de direcciones IPv4

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ……/……/…….	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. **Propósito /Objetivo (de la práctica):**

Al finalizar el laboratorio el estudiante podrá:

Identificar direcciones IPv4

Clasificar direcciones IPv4

2. **Fundamento Teórico**

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 (IPv4). Identificará los diversos tipos de direcciones IPv4 y los componentes que ayudan a formar la dirección, como la porción de red, la porción de host y la máscara de subred. Entre los tipos de direcciones que se abarcan, se incluyen las siguientes: pública, privada, unicast y multicast.

3. **Equipos, Materiales y Reactivos**

- 1 PC con acceso al Internet
-

4. **Procedimientos:**

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		

5. Resultados

¿Por qué debemos seguir estudiando y aprendiendo sobre el direccionamiento IPv4 si el espacio de direcciones IPv4 disponible está agotado?

_____

_____

6. Conclusiones

Toda dirección de red IP esta conformada por dos componentes dirección de red y dirección de Host, la dirección de red se delimita mediante la máscara de red.

7. Sugerencias y /o recomendaciones

8. Referencias bibliográficas consultadas y/o enlaces recomendados

Guía de práctica N° 13

División de red en subredes

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Determinar la cantidad de subredes.
- Diseñar un esquema de direccionamiento adecuado.
- Asignar direcciones y pares de mascaras de subred a las interfaces del dispositivo.
- Examinar el uso del espacio de direcciones de red disponible y el crecimiento potencial futuro.

2. Fundamento Teórico

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 proporcionará 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.

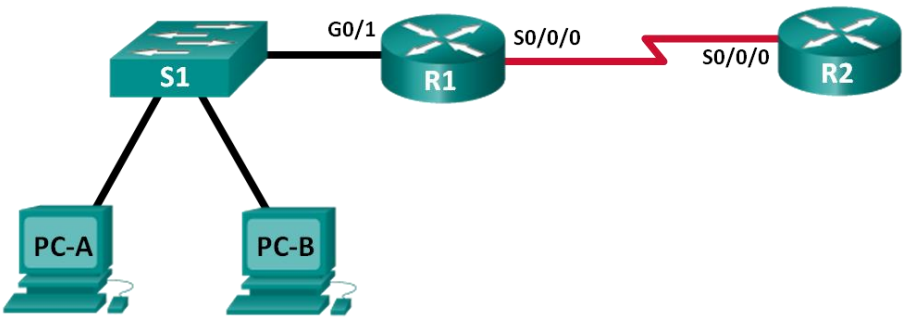
3. Equipos, Materiales y Reactivos

- 1 Pc son packet tracer instalado.

4. Procedimientos:

Paso 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.



a. Determine la cantidad de subredes en la topología de la red A.

i. ¿Cuántas subredes hay? _____

ii. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____

iii. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? _____

iv. ¿Cuál es la máscara de subred nueva en formato decimal punteado? _____

v. ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

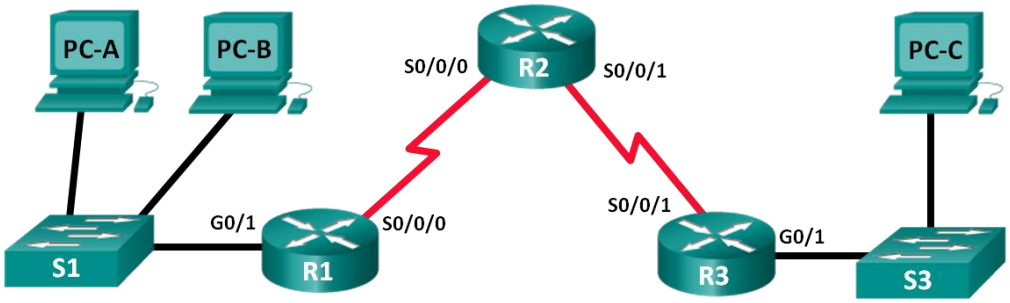
b. Registre la información de subred.

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				

5. 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.



a. Determine la cantidad de subredes en la topología de la red B.

i. ¿Cuántas subredes hay? _____

ii. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____

iii. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? _____

iv. ¿Cuál es la máscara de subred nueva en formato decimal punteado? _____

v. ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

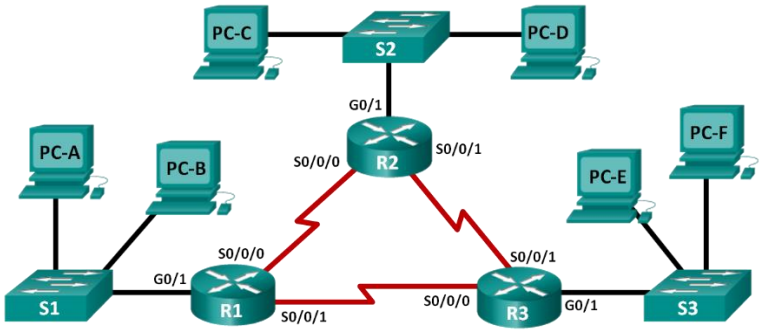
b. Registre la información de subred.

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				

6. 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.



a. Determine la cantidad de subredes en la topología de la red C.

i. ¿Cuántas subredes hay? _____

ii. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____

iii. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? _____

iv. ¿Cuál es la máscara de subred nueva en formato decimal punteado? _____

v. ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

b. 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				

c. Asignar direcciones a los dispositivos de red en las subredes

i. Complete la siguiente tabla con las direcciones IP y las máscaras de subred para las interfaces del router:

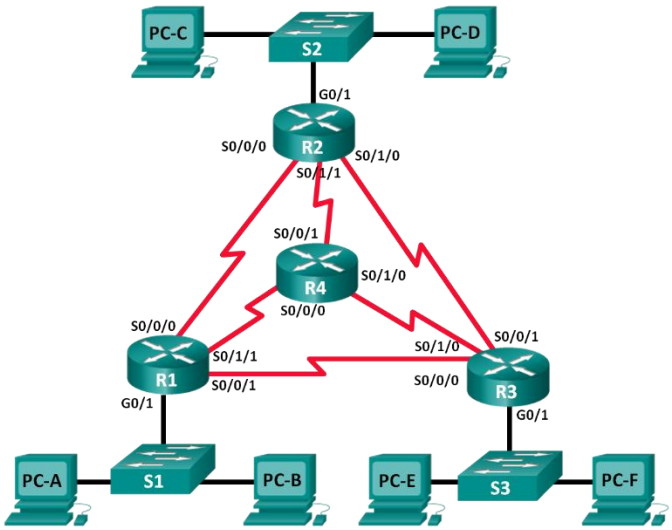
Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R2	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		
R3	GigabitEthernet 0/1		
	Serial 0/0/0		
	Serial 0/0/1		

ii. 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			

7. 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.



a. Determine la cantidad de subredes en la topología de la red D.

i. ¿Cuántas subredes hay? _____

ii. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____

iii. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? _____

iv. ¿Cuál es la máscara de subred nueva en formato decimal punteado? _____

v. ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

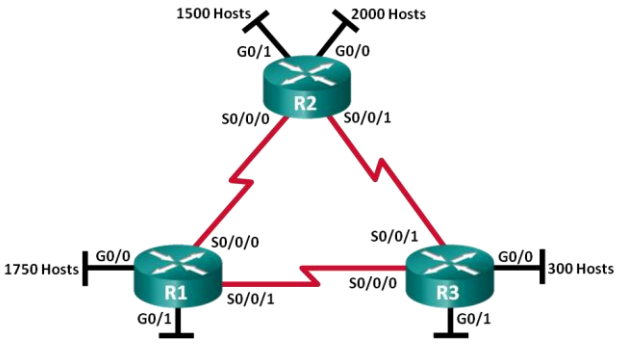
b. Registre la información de subred.

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				

8. 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.



a. Determine la cantidad de subredes en la topología de la red E.

i. ¿Cuántas subredes hay? _____

ii. ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____

iii. ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? _____

iv. ¿Cuál es la máscara de subred nueva en formato decimal punteado? _____

v. ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

b. 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				

c. Asignar direcciones a los dispositivos de red en las subredes

i. 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		

9. Resultados

a. ¿Qué información es necesaria cuando debe determinar un esquema de direccionamiento adecuado para una red?

_____

_____

b. Una vez asignadas las subredes, ¿se utilizarán todas las direcciones de host en cada subred?

_____

_____

10. Conclusiones

Para efectuar la subdivisión de redes se puede tomar un bit de la porción de host, cada bit prestado supone una división en dos de la red original.

11. Sugerencias y /o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a : 9.0.1.2 Call Me!

Referencias bibliográficas consultadas y/o enlaces recomendados:

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 14

Implementación de un esquema de direccionamiento IPv4 en subredes

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

- Diseñar un esquema de división en subredes
- Configurar los dispositivos
- Probar la red y resolver los problemas encontrados

2. Fundamento Teórico

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.

3. Equipos, Materiales y Reactivos

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

4. Procedimientos:

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?

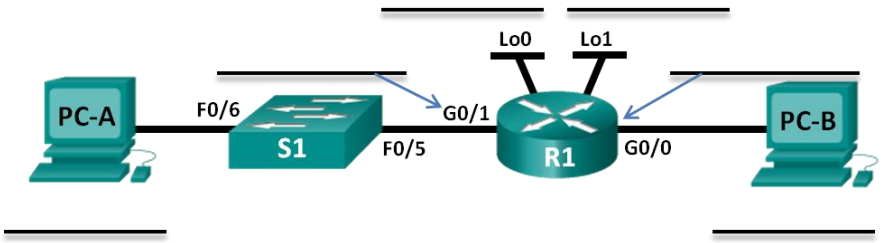
_____

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.

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?_____
_____

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.				

Detalles de configuración para los pasos de la parte 2

Paso 5: 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>
```

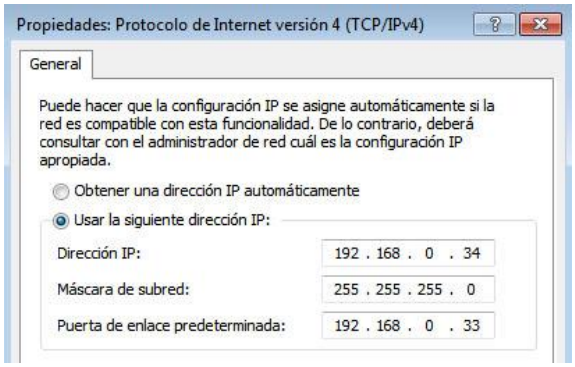
R1(config-if)# **end**

f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

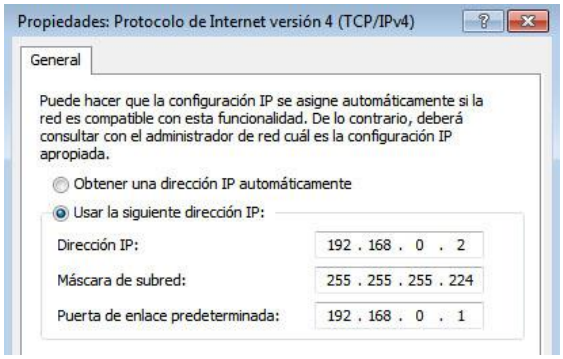
R1# **copy running-config startup-config**

Paso 6: 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.



5. Resultados

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?

_____
_____

¿Por qué piensa que la dirección IP del gateway o del router es generalmente la primera dirección IP utilizable en la red?

_____
_____

6. Conclusiones

Antes de afrontar una situación de configuración de direcciones de red es importante crear el respectivo diseño, así se podrán evaluar previamente cada uno de los requisitos e implementar el diseño sin mayores problemas de direccionamiento.

7. Sugerencias y/o recomendaciones

Revisar en la plataforma de CISCO NetAcad el tema referente a : 9.1.4.10 Investigación de calculadoras de subredes

8. Referencias bibliográficas consultadas y/o enlaces recomendados

- Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.

Guía de práctica N° 15

Diseño e implementación de un esquema de direccionamiento VLSM

Sección :	Docente: Pedro Yuri Marquez Solis
Fecha : ...../...../.....	Duración: 70 min

Instrucciones: Seguir atentamente las instrucciones que indique el docente

1. Propósito /Objetivo (de la práctica):

Al finalizar el laboratorio el estudiante podrá:

Examinar los requisitos de la red
Diseñar el esquema de direcciones VLSM
Cablear y configurar la red IPv4

2. Fundamento Teórico

La máscara de subred de longitud variable (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. Equipos, Materiales y Reactivos

- 3 routers (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o comparable)
- 1 PC (con programa de emulación de terminal, como Tera Term, para configurar los routers)
- Cable de consola para configurar los dispositivos Cisco IOS a través de los puertos de consola
- Cables Ethernet (optativos) y seriales, según se muestra en la topología

4. Procedimientos:

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.

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.

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.				

5. Resultados

¿Puede pensar en un atajo para calcular las direcciones de red de las subredes /30 consecutivas?

_____

_____

_____

6. **Conclusiones**

7. **Sugerencias y /o recomendaciones:**
   Revisar en la plataforma de CISCO NetAcad el tema referente a : 9.2.1.4 Diseño e implementación de un Esquema de direccionamiento de VLSM

8. **Referencias bibliográficas consultadas y/o enlaces recomendados**
   - Cisco NetWorking Academy. Switching y routing CCNA: Introducción a redes.