Cisco | Networking Academy®
Mind Wide Open™

Switching y routing CCNA: Introducción a redes

Manual de Packet Tracer para el instructor

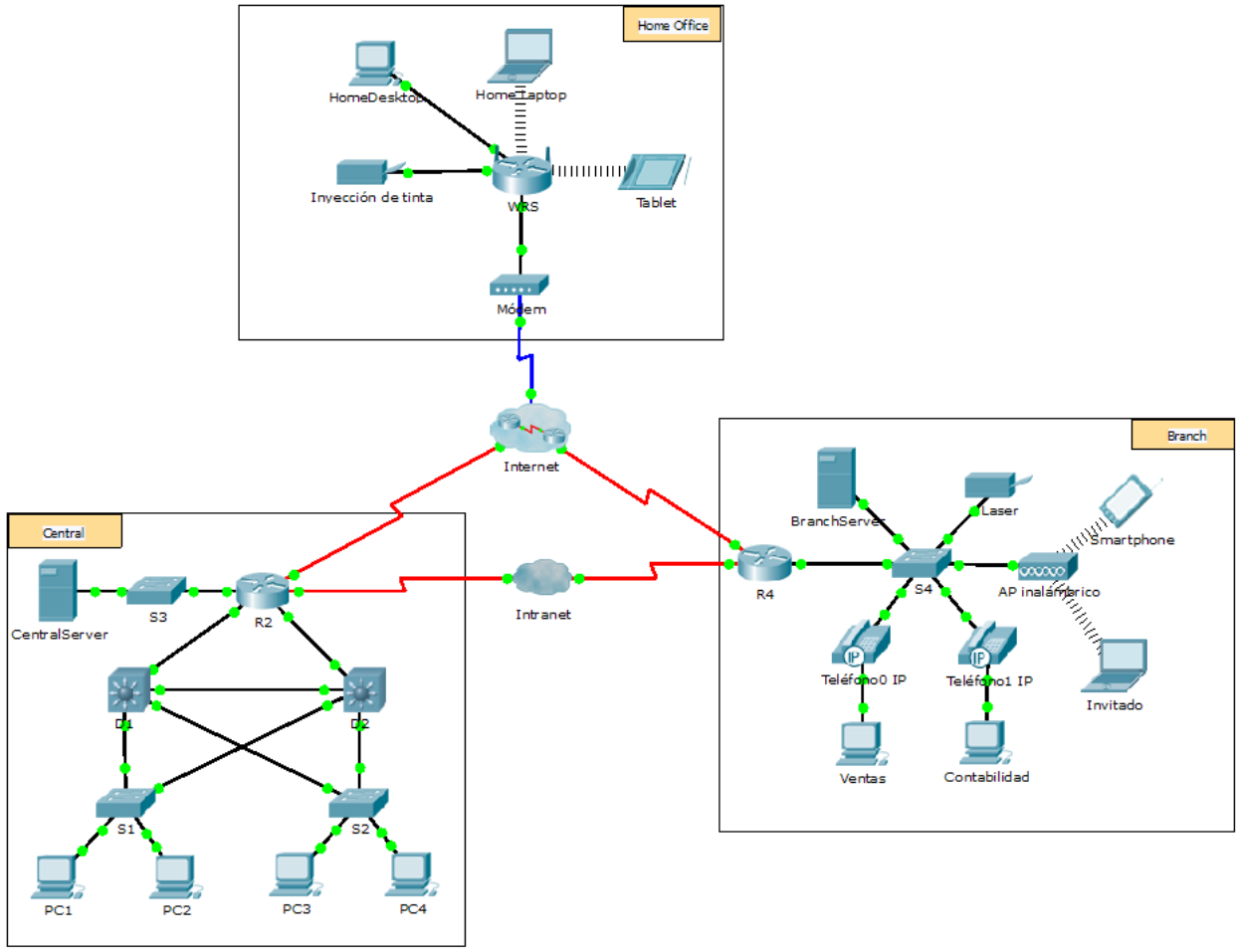
Packet Tracer: Representación de la red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Todos los clientes tienen total conectividad a los servidores. Por cuestiones de diversidad de tramas, el entorno no es completamente realista. Por ejemplo:

- Se utilizan la sobrecarga de PAT y NAT en la red de sucursal, pero la red central 10.X.X.X se comparte de forma pública.
- Hay un servidor DNS separado en la red 172 debido a que las PC no son capaces de utilizar la dirección pública del servidor de archivos. A diferencia de BIND, el servidor DNS simulado es básico y no reenvía las solicitudes que no conoce a un servidor raíz, por lo que se duplican los registros A.
- EIGRP se ejecuta en la nube, a diferencia de BGP.
- El switch de sucursal proporciona DHCP, simplemente porque puede hacerlo, lo que hace que ese lado de la simulación sea diferente al del lado de la red central.
- La nube incluye dos servidores: uno utiliza el IP correcto de netacad.com, y el otro utiliza el IP correcto del DNS de Google.
- Las contraseñas del router son “cisco” y “class”, pero existen un “banner motd” y un “banner login” que brindan fácilmente las contraseñas a los curiosos.
- Los switches S1 y S2 tienen el protocolo de árbol de expansión PVST habilitado. Cada uno tiene un puerto de bloqueo diferente, por lo que todas las conexiones están verdes.

Topología



Objetivos

Parte 1: Descripción general del programa Packet Tracer

Parte 2: Exploración de LAN, WAN e Internet

Información básica

Packet Tracer es un programa de software flexible y divertido para llevar a casa que lo ayudará con sus estudios de Cisco Certified Network Associate (CCNA). Packet Tracer le permite experimentar con comportamientos de red, armar modelos de red y preguntarse "¿qué pasaría si...?". En esta actividad, explorará una red relativamente compleja que pone de relieve algunas de las características de Packet Tracer. Al hacerlo, aprenderá cómo acceder a la función de Ayuda y a los tutoriales. También aprenderá cómo alternar entre diversos modos y espacios de trabajo. Finalmente, explorará la forma en que Packet Tracer sirve como herramienta de creación de modelos para representaciones de red.

Nota: no es importante que comprenda todo lo que vea y haga en esta actividad. Explore la red por su cuenta con libertad. Si desea hacerlo de forma más sistemática, siga estos pasos. Responda las preguntas lo mejor que pueda.

Parte 1: Descripción general del programa Packet Tracer

El tamaño de la red es mayor que la mayoría de las redes con las que trabajará en este curso (si bien verá esta topología a menudo en sus estudios de Networking Academy). Es posible que deba ajustar el tamaño de la ventana de Packet Tracer para ver la red completa. De ser necesario, puede utilizar las herramientas Acercar y Alejar para ajustar el tamaño de la ventana de Packet Tracer.

Paso 1: Acceder a las páginas de ayuda, a videos de tutoriales y a los recursos en línea de Packet Tracer

a. Acceda a las páginas de ayuda de Packet Tracer de dos maneras:

   1) Haga clic en el ícono de signo de interrogación que está en la esquina superior derecha de la barra de herramientas del menú.

   2) Haga clic en el menú **Help** (Ayuda) y, a continuación, seleccione **Contents** (Contenido).

b. Acceda a los videos de tutoriales de Packet Tracer haciendo clic en **Help** > **Tutorials** (Tutoriales). Estos videos son una demostración visual de la información que se encuentra en las páginas de **ayuda** y diversos aspectos del programa de software Packet Tracer. Antes de continuar con esta actividad, debe familiarizarse con la interfaz y el modo de simulación de Packet Tracer.

   1) Vea el video **Interface Overview** (Descripción general de la interfaz) en la sección **Getting Started** (Introducción) de Tutorials.

   2) Vea el video **Simulation Environment** (Entorno de simulación) en la sección **Realtime and Simulation Modes** (Modos de tiempo real y de simulación) de **Tutorials**.

c. Busque el tutorial “Configuring Devices Using the Desktop Tab” (Configuración de dispositivos mediante la ficha Desktop [Escritorio]). Mire la primera parte para responder la siguiente pregunta: ¿Qué información se puede configurar en la ventana IP Configuration (Configuración IP)? Puede elegir DHCP o Static (Estático) y configurar la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS.

Paso 2: Alternar entre los modos de tiempo real y de simulación

a. Busque la palabra **Realtime** (Tiempo real) en la esquina inferior derecha de la interfaz de Packet Tracer. En el modo de tiempo real, la red siempre funciona como una red real, ya sea que trabaje en la red o no. La configuración se realiza en tiempo real, y la red responde prácticamente en tiempo real.

b. Haga clic en la ficha que está justo detrás de la ficha **Realtime** para cambiar al modo **Simulation** (Simulación). En el modo de simulación, puede ver la red en funcionamiento a menor velocidad, lo que le permite observar las rutas por las que viajan los datos e inspeccionar los paquetes de datos en detalle.

c. En el panel de simulación, haga clic en **Auto Capture / Play** (Captura/reproducción automática). Ahora debería ver los paquetes de datos, que se representan con sobres de diversos colores, que viajan entre los dispositivos.

d. Haga clic en **Auto Capture / Play** nuevamente para pausar la simulación.

e. Haga clic en **Capture / Forward** (Capturar/avanzar) para avanzar en la simulación. Haga clic en este botón algunas veces más para ver el efecto.

f. En la topología de la red a la izquierda, haga clic en cualquiera de los sobres en un dispositivo intermediario e investigue qué hay dentro. En el curso de sus estudios de CCNA, aprenderá el significado la mayor parte del contenido de estos sobres. Por el momento, intente responder las siguientes preguntas:

   - En la **ficha OSI Model** (Modelo OSI), ¿cuántas **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida) tienen información? Las respuestas varían según la capa del dispositivo.

- En las fichas **Inbound PDU Details** (Detalles de la PDU de entrada) y **Outbound PDU Details** (Detalles de la PDU de salida), ¿cuáles son los encabezados de las secciones principales? Las respuestas varían, pero algunas respuestas probables son Ethernet 802.3, LLC, STP BPDU, etcétera.
- Alterne entre las fichas **Inbound PDU Details** y **Outbound PDU Details**. ¿Observa cambios en la información? Si es así, ¿qué es lo que cambia? Las respuestas varían, pero las direcciones de origen o destino de la capa de enlace de datos cambian. También pueden cambiar otros datos, según el paquete que haya abierto el estudiante.

g. Haga clic en el botón de alternancia arriba de **Simulation** en la esquina inferior derecha para volver al modo **Realtime**.

Paso 3: Alternar entre las vistas Logical y Physical

a. Busque la palabra **Logical** (Lógico) en la esquina superior izquierda de la interfaz de Packet Tracer. Actualmente se encuentra en el área de trabajo **Logical**, donde pasará la mayor parte del tiempo de creación, configuración, investigación y resolución de problemas de redes.

Nota: si bien puede agregar un mapa geográfico como imagen de fondo para el área de trabajo **Logical**, generalmente no tiene ninguna relación con la ubicación física real de los dispositivos.

b. Haga clic en la ficha que está debajo **Logical** para pasar al área de trabajo **Physical** (Físico). El propósito del área de trabajo **Physical** es darle una dimensión física a la topología lógica de la red. Le da una idea de la escala y la ubicación (cómo se vería la red en un entorno real).

c. Durante sus estudios en CCNA, utilizará esta área de trabajo de manera ocasional. Por el momento, solo debe saber que ese espacio está allí, disponible para que lo utilice. Para obtener más información sobre el área de trabajo Physical, consulte los archivos de ayuda y los videos de tutoriales.

d. Haga clic en el botón de alternancia ubicado debajo de **Physical** en la esquina superior derecha para volver al área de trabajo **Logical**.

Parte 2: Exploración de LAN, WAN e Internet

El modelo de red en esta actividad incluye muchas de las tecnologías que llegará a dominar en sus estudios en CCNA y representa una versión simplificada de la forma en que podría verse una red de pequeña o mediana empresa. Explore la red por su cuenta con libertad. Cuando esté listo, siga estos pasos y responda las preguntas.

Paso 1: Identificar los componentes comunes de una red según se los representa en Packet Tracer

a. La barra de herramientas de íconos tiene diferentes categorías de componentes de red. Debería ver las categorías que corresponden a los dispositivos intermediarios, los dispositivos finales y los medios. La categoría **Connections** (Conexiones, cuyo ícono es un rayo) representa los medios de red que admite Packet Tracer. También hay una categoría llamada **End Devices** (Dispositivos finales) y dos categorías específicas de Packet Tracer: **Custom Made Devices** (Dispositivos personalizados) y **Multiuser Connection** (Conexión multiusuario).

b. Enumere las categorías de los dispositivos intermediarios. Routers, switches, hubs, dispositivos inalámbricos y emulación de WAN.

c. Sin ingresar en la nube de Internet o de intranet, ¿cuántos íconos de la topología representan dispositivos terminales (solo una conexión conduce a ellos)? 13

d. Sin contar las dos nubes, ¿cuántos íconos de la topología representan dispositivos intermediarios (varias conexiones conducen a ellos)? 11

e. ¿Cuántos de esos dispositivos intermediarios son routers? Nota: el dispositivo Linksys es un router. 5

f. ¿Cuántos dispositivos finales **no** son computadoras de escritorio? 8

g. ¿Cuántos tipos diferentes de conexiones de medios se utilizan en esta topología de red? 4

h. ¿Por qué no hay un ícono de conexión para la tecnología inalámbrica en la categoría Connections? El técnico de red no realiza las conexiones inalámbricas físicamente. En cambio, los dispositivos se encargan de negociar la conexión y de activar el enlace físico.

Paso 2: Explicar la finalidad de los dispositivos

a. En Packet Tracer, el dispositivo Server-PT puede funcionar como servidor. Las computadoras de escritorio y portátiles no pueden funcionar como servidores. ¿Esto sucede en el mundo real? No. Según lo que estudió hasta ahora, explique el modelo cliente-servidor. En las redes modernas, un hosts pueden actuar como un cliente, un servidor o ambos. El software instalado en el host determina qué función tiene en la red. Los servidores son hosts que tienen instalado software que les permite proporcionar información y servicios, como correo electrónico o páginas Web, a otros hosts en la red. Los clientes son hosts que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida. Sin embargo, un cliente también se puede configurar como servidor simplemente al instalar software de servidor.

b. Enumere, al menos, dos funciones de los dispositivos intermediarios. Regenerar y retransmitir señales de datos; mantener información sobre qué rutas existen a través de la red y de la internetwork; notificar a otros dispositivos de los errores y las fallas de comunicación; direccionar datos a través de rutas alternativas cuando hay una falla de enlace; clasificar y direccionar mensajes según las prioridades de QoS; permitir o denegar el flujo de datos según la configuración de seguridad.

c. Enumere, al menos, dos criterios para elegir un tipo de medio de red. La distancia en la cual el medio puede transportar exitosamente una señal. El ambiente en el cual se instalará el medio La cantidad de datos y la velocidad a la que se deben transmitir El costo de los medios y de la instalación.

Paso 3: Comparar redes LAN y WAN

a. Explique la diferencia entre una LAN y una WAN, y dé ejemplos de cada una. Las redes LAN proporcionan acceso a los usuarios finales en una pequeña área geográfica. Una oficina doméstica o un campus son ejemplos de redes LAN. Las redes WAN proporcionan acceso a los usuarios en un área geográfica extensa a través de grandes distancias, que pueden ir de pocos a miles de kilómetros. Una red de área metropolitana e Internet son ejemplos de redes WAN. La intranet de una compañía también puede conectar varios sitios remotos mediante una WAN.

b. ¿Cuántas WAN ve en la red de Packet Tracer? Hay dos: la WAN de Internet y la de intranet.

c. ¿Cuántas LAN ve? Hay tres, que se identifican fácilmente porque cada una tiene un límite y una etiqueta.

d. En esta red de Packet Tracer, Internet está simplificada en gran medida y no representa ni la estructura ni la forma de Internet propiamente dicha. Describa Internet brevemente. Internet se utiliza sobre todo cuando necesitamos comunicarnos con un recurso en otra red. Internet es una malla global de redes interconectadas (internetworks).

e. ¿Cuáles son algunas de las formas más comunes que utiliza un usuario doméstico para conectarse a Internet? Cable, DSL, dial-up, datos móviles y satélite.

f. ¿Cuáles son algunas de las formas más comunes que utilizan las empresas para conectarse a Internet en su área? Línea arrendada dedicada, Metro-E, DSL, cable, satélite.

Desafío

Ahora que tuvo la oportunidad de explorar la red representada en esta actividad de Packet Tracer, es posible que haya adquirido algunas habilidades que quiera poner en práctica o tal vez desee tener la oportunidad de analizar esta red en mayor detalle. Teniendo en cuenta que la mayor parte de lo que ve y experimenta en Packet Tracer supera su nivel de habilidad en este momento, los siguientes son algunos desafíos que tal vez quiera probar. No se preocupe si no puede completarlos todos. Muy pronto se convertirá en un usuario y diseñador de redes experto en Packet Tracer.

- Agregue un dispositivo final a la topología y conéctelo a una de las LAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para enviar datos a otros usuarios finales? ¿Puede proporcionar la información? ¿Hay alguna manera de verificar que conectó correctamente el dispositivo?
- Agregue un nuevo dispositivo intermediario a una de las redes y conéctelo a uno de las LAN o WAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para funcionar como intermediario de otros dispositivos en la red?
- Abra una nueva instancia de Packet Tracer. Cree una nueva red con, al menos, dos redes LAN conectadas mediante una WAN. Conecte todos los dispositivos. Investigue la actividad de Packet Tracer original para ver qué más necesita hacer para que la nueva red esté en condiciones de funcionamiento. Registre sus comentarios y guarde el archivo de Packet Tracer. Tal vez desee volver a acceder a la red cuando domine algunas habilidades más.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Descripción general del programa Packet Tracer	Paso 1c	4	
	Paso 2f	6	
Total de la parte 1		**10**	
Parte 2: Exploración de LAN, WAN e Internet	Paso 1b	5	
	Paso 1c	5	
	Paso 1d	5	
	Paso 1e	5	
	Paso 1f	5	
	Paso 1g	5	
	Paso 1h	6	
	Paso 2a	6	
	Paso 2b	6	
	Paso 2c	6	
	Paso 3a	6	
	Paso 3b	6	
	Paso 3c	6	
	Paso 3d	6	
	Paso 3e	6	
	Paso 3f	6	
Total de la parte 2		**90**	
Puntuación total		**100**	

Packet Tracer: Navegación de IOS (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Objetivos

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

Parte 2: Exploración de los modos EXEC

Parte 3: Configuración del comando clock

Información básica

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

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

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

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

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

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

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

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

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

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

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

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

¿Cuál es el parámetro de bits por segundo? 9600

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

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

¿Cuál es la petición de entrada que aparece en la pantalla? S1>

Paso 3: Examine la ayuda de IOS.

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

```
S1> ?
```

¿Qué comando comienza con la letra "C"? conectar

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

```
S1> t?
```

¿Qué comandos se muestran? telnet terminal traceroute

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

```
S1> te?
```

¿Qué comandos se muestran? telnet terminal

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

Parte 2: Exploración de los modos EXEC

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

Paso 1: Ingrese al modo EXEC privilegiado.

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

```
S1> ?
```

¿Qué información de la que se muestra describe el comando **enable**? Active los comandos privilegiados.

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

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

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

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

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

"te" no proporciona suficientes caracteres para formar un comando único; por lo tanto, los caracteres continuarán apareciendo, y se le solicitará al usuario que introduzca más caracteres para formar el comando único. Hay más de un comando que comienza con las letras "te".

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

Cambia de S1> a S1#, que indica el modo EXEC privilegiado.

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

```
S1# ?
```

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

5: clear clock configure connect copy

Paso 2: Ingresar en el modo de configuración global

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

```
S1# configure
```

¿Cuál es el mensaje que se muestra?

Configuring from terminal, memory, or network [terminal]? (Configurando desde terminal, memoria o red [terminal]?)

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

¿En qué cambia la petición de entrada? S1(config)#

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

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

Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock

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

```
S1# show clock
```

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

UTC Mon Mar 1 1993 (UTC lun 1 de marzo de 1993), precedido por las horas, los minutos y segundos desde que el dispositivo se inició. El año es 1993.

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

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

¿Qué información aparece en pantalla? % Incomplete command.

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

```
S1# clock ?
```

¿Qué información aparece en pantalla? set Configura la hora y la fecha

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

```
S1# clock set ?
```

¿Qué información se solicita? hh:mm:ss Hora actual

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

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

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

El resultado devuelve la solicitud de más información:

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

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

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

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

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

Paso 2: Explorar los mensajes adicionales del comando

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

b. Emita el siguiente comando y registre los mensajes:

```
S1# cl
```

¿Qué información se devolvió? % Ambiguous command: “cl”

```
S1# clock
```

¿Qué información se devolvió? % Incomplete command.

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

¿Qué información se devolvió?

```
S1#clock set 25:00:00
              ^
% Invalid input detected at '^' marker.
```

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

¿Qué información se devolvió?

```
S1#clock set 15:00:00 32
                       ^
% Invalid input detected at '^' marker.
```

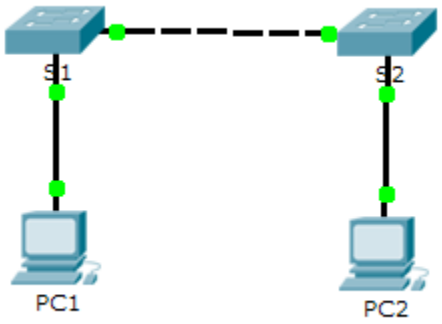

Tabla de calificación sugerida

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

Packet Tracer: Configuración de los parámetros iniciales del switch (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Verificar la configuración predeterminada del switch

Parte 2: Establecer una configuración básica del switch

Parte 3: Configurar un título de MOTD

Parte 4: Guardar los archivos de configuración en la NVRAM

Parte 5: Configurar el S2

Información básica

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

Parte 1: Verificar la configuración predeterminada del switch

Paso 1: Entre al modo privilegiado.

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

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

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

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

```
Switch> enable
Switch#
```

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

Paso 2: Examine la configuración actual del switch.

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

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

b. Responda las siguientes preguntas:

¿Cuántas interfaces FastEthernet tiene el switch? 24

¿Cuántas interfaces Gigabit Ethernet tiene el switch? 2

¿Cuál es el rango de valores que se muestra para las líneas vty? 0 -15

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

¿Por qué el switch responde con `startup-config is not present`? Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.

Parte 2: Crear una configuración básica del switch

Paso 1: Asignar un nombre a un switch

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

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

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

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

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

¿Por qué se requiere el comando **login**? Para que el proceso de control de contraseñas funcione, se necesitan los comandos **login** y **password**.

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

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

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

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

Paso 4: Proporcionar un acceso seguro al modo privilegiado

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

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

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

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

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

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

```
User Access Verification
Password:
```

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

d. Introduzca el comando para acceder al modo privilegiado.

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

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

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

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

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

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

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



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

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

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

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

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

```
S1# show run
```

b. ¿Qué se muestra como contraseña **secreta de enable**? 1mERr$ILwq/b7kc.7X/ejA4Aosn0

c. ¿Por qué la contraseña **secreta de enable** se ve diferente de lo que se configuró? El comando enable secret se muestra encriptado, mientras que la contraseña de enable aparece en texto no cifrado.

Paso 8: Encriptar las contraseñas de consola y de enable

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

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

Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma encriptada en el archivo de configuración? Explique por qué. El comando service password-encryption encripta todas las contraseñas actuales y futuras.

Parte 3: Configurar un título de MOTD

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

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

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

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

¿Cuándo se muestra este mensaje? El mensaje se muestra cuando alguien accede al switch a través del puerto de consola.

¿Por qué todos los switches deben tener un mensaje MOTD? Cada switch debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).

Parte 4: Guardar los archivos de configuración en la NVRAM

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

Paso 2: Guardar el archivo de configuración

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

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

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

Paso 3: Examinar el archivo de configuración de inicio

¿Qué comando muestra el contenido de la NVRAM? **show startup-configuration**

¿Todos los cambios realizados están grabados en el archivo? Sí, es igual a la configuración en ejecución.

Parte 5: Configurar S2

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

Configure el S2 con los siguientes parámetros:

a. Nombre del dispositivo: **S2**

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

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

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

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

e. Encripte todas las contraseñas de texto no cifrado.

f. Asegúrese de que la configuración sea correcta.

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

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#enable password c1$c0
S2(config)#enable secret itsasecret
```



```
S2(config)#banner motd $any text here$
S2(config)#service password-encryption
S2(config)#do wr
```

Tabla de calificación sugerida

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

Packet Tracer: Implementación de conectividad básica

(version para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

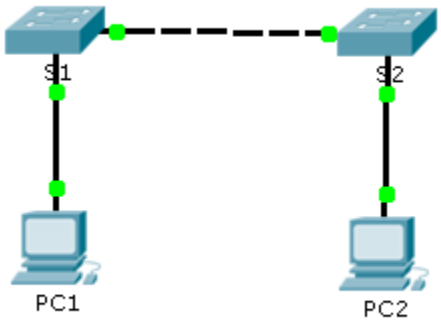


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Objetivos

Parte 1: Realizar una configuración básica en S1 y S2

Paso 2: Configurar la PC

Parte 3: Configurar la interfaz de administración de switches

Información básica

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

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

Complete los siguientes pasos en el S1 y el S2.

Paso 1: Configurar un nombre de host en el S1

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

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

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

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

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

Paso 3: Verificar la configuración de contraseñas para el S1

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

Una vez que salga del modo EXEC del usuario, el switch le solicitará una contraseña para acceder a la interfaz de consola y le solicitará una contraseña por segunda vez para acceder al modo EXEC privilegiado. También puede usar el comando **show run** para ver las contraseñas.

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

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

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

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

¿Qué comando emite para realizar este paso?

```
S1(config)#exit (or end)
S1#copy run start
```

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

Parte 2: Configurar las PC

Configure la PC1 y la PC2 con direcciones IP.

Paso 1: Configurar ambas PC con direcciones IP

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

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

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

Paso 2: Probar la conectividad a los switches

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

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

```
Packet Tracer PC Command Line 1.0
```



```
PC> ping 192.168.1.253
```

¿Tuvo éxito? ¿Por qué o por qué no?

No debería realizarse correctamente, porque los switches no están configurados con una dirección IP.

Parte 3: Configurar la interfaz de administración de switches

Configure el S1 y el S2 con una dirección IP.

Paso 1: Configurar el S1 con una dirección IP

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

Para conectarse de forma remota a un switch, es necesario asignarle una dirección IP. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1.

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

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

¿Por qué debe introducir el comando **no shutdown**? El comando **no shutdown** habilita administrativamente el estado activo de la interfaz.

Paso 2: Configurar el S2 con una dirección IP

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

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

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

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

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

Paso 5: Verificar la conectividad de la red

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

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

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

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

d. Haga ping a la dirección IP del S1.

e. Haga ping a la dirección IP del S2.

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

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

Tabla de calificación sugerida

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

Packet Tracer: Reto de habilidades de integración

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Objetivos

- Configurar los nombres de host y las direcciones IP en dos switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Usar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones de los dispositivos.
- Utilizar los comandos de IOS para guardar la configuración en ejecución.
- Configurar dos dispositivos host con direcciones IP.
- Verificar la conectividad entre los dos dispositivos finales de PC.

Situación

Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante Cisco IOS y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

Requisitos

- Use una conexión de consola para acceder a cada switch.
- Nombre los switches **[[S1Name]]** y **[[S2Name]]**.
- Use la contraseña **[[LinePW]]** para todas las líneas.
- Use la contraseña secreta **[[SecretPW]]**.
- Encripte todas las contraseñas de texto no cifrado.
- Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos.

Nota: haga clic en **Check Results** (Verificar resultados) para ver su progreso. Haga clic en **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Si hace clic en esto antes de completar la actividad, se perderán todas las configuraciones.

Índice de isomorfos: [[indexNames]][[indexPWs]][[indexAdds]][[indexTopos]]

Notas para el instructor

La siguiente información se incluye solo en la versión para el instructor.

En esta actividad, se utilizan variables que se generan aleatoriamente cada vez que se abre la actividad o se hace clic en el botón de Reset Activity. Si bien en las tablas que se encuentran a continuación se muestra la asignación de nombres de dispositivos a esquemas de direcciones específicos, los nombres y las direcciones no se corresponden de manera exclusiva. Por ejemplo, un estudiante podría obtener los nombres de dispositivos presentados en la situación 1 con el direccionamiento que se muestra en la situación 2. Además, el estudiante recibirá una de tres versiones de la topología.

Escenario 1

Dispositivo	Interfaz	Dirección	Máscara de subred
Clase-A	VLAN 1	128.107.20.10	255.255.255.0
Clase-B	VLAN1	128.107.20.15	255.255.255.0
Estudiante 1	NIC	128.107.20.25	255.255.255.0
Estudiante 2	NIC	128.107.20.30	255.255.255.0

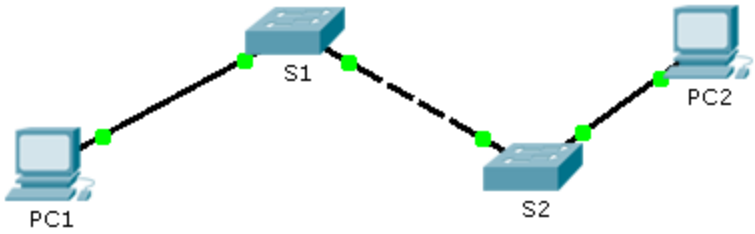
Escenario 2

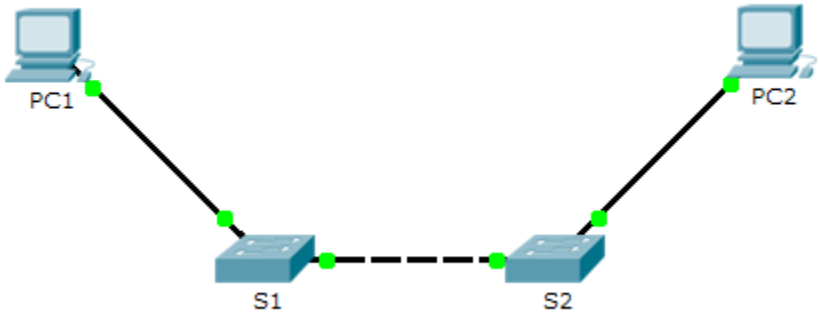
Dispositivo	Interfaz	Dirección	Máscara de subred
Aula 145	VLAN 1	172.16.5.35	255.255.255.0
Aula 146	VLAN 1	172.16.5.40	255.255.255.0
Gerente	NIC	172.16.5.50	255.255.255.0
Recepción	NIC	172.16.5.60	255.255.255.0

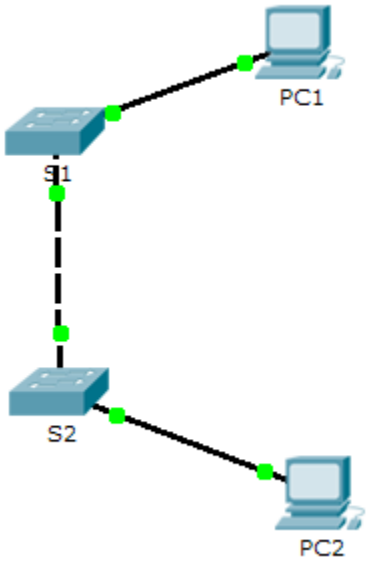
Escenario 3

Dispositivo	Interfaz	Dirección	Máscara de subred
ASw-1	VLAN 1	10.10.10.100	255.255.255.0
ASw-2	VLAN 1	10.10.10.150	255.255.255.0
Usuario 01	NIC	10.10.10.4	255.255.255.0
Usuario 02	NIC	10.10.10.5	255.255.255.0

Isomorfos de la topología



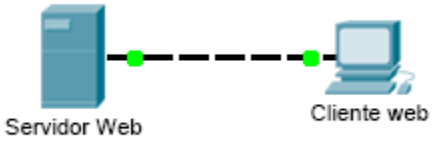




Packet Tracer: Investigación de los modelos TCP/IP y OSI en acción (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Examinar el tráfico Web HTTP

Parte 2: Mostrar elementos de la suite de protocolos TCP/IP

Información básica

Esta actividad de simulación tiene como objetivo proporcionar una base para comprender la suite de protocolos TCP/IP y la relación con el modelo OSI. El modo de simulación le permite ver el contenido de los datos que se envían a través de la red en cada capa.

A medida que los datos se desplazan por la red, se dividen en partes más pequeñas y se identifican de modo que las piezas se puedan volver a unir cuando lleguen al destino. A cada pieza se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data units]) y se la asocia a una capa específica de los modelos TCP/IP y OSI. El modo de simulación de Packet Tracer le permite ver cada una de las capas y la PDU asociada. Los siguientes pasos guían al usuario a través del proceso de solicitud de una página Web desde un servidor Web mediante la aplicación de explorador Web disponible en una PC cliente.

Aunque gran parte de la información mostrada se analizará en mayor detalle más adelante, esta es una oportunidad de explorar la funcionalidad de Packet Tracer y de ver el proceso de encapsulación.

Parte 1: Examinar el tráfico Web HTTP

En la parte 1 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para generar tráfico Web y examinar HTTP.

Paso 1: Cambie del modo de tiempo real al modo de simulación.

En la esquina inferior derecha de la interfaz de Packet Tracer, hay fichas que permiten alternar entre el modo **Realtime** (Tiempo real) y **Simulation** (Simulación). PT siempre se inicia en el modo **Realtime**, en el que los protocolos de red operan con intervalos realistas. Sin embargo, una excelente característica de Packet Tracer permite que el usuario “detenga el tiempo” al cambiar al modo de simulación. En el modo de simulación, los paquetes se muestran como sobres animados, el tiempo se desencadena por eventos y el usuario puede avanzar por eventos de red.

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

b. Seleccione **HTTP** de **Event List Filters** (Filtros de lista de eventos).

1) Es posible que HTTP ya sea el único evento visible. Haga clic en **Edit Filters** (Editar filtros) para mostrar los eventos visibles disponibles. Alterne la casilla de verificación **Show All/None** (Mostrar todo/ninguno) y observe cómo las casillas de verificación se desactivan y se activan, o viceversa, según el estado actual.
2) Haga clic en la casilla de verificación **Show all/None** (Mostrar todo/ninguno) hasta que se desactiven todas las casillas y luego seleccione **HTTP**. Haga clic en cualquier lugar fuera del cuadro **Edit Filters** (Editar filtros) para ocultarlo. Los eventos visibles ahora deben mostrar solo HTTP.

Paso 2: Genere tráfico web (HTTP).

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

Nota: el servidor Web y el cliente Web se muestran en el panel de la izquierda. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha cuando aparece la flecha de dos puntas.

a. Haga clic en **Web Client** (Cliente Web) en el panel del extremo izquierdo.

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

c. En el campo de dirección URL, introduzca **www.osi.local** y haga clic en **Go** (Ir).

Debido a que el tiempo en el modo de simulación se desencadena por eventos, debe usar el botón **Capture/Forward** (Capturar/avanzar) para mostrar los eventos de red.

d. Haga clic en **Capture/Forward** cuatro veces. Debe haber cuatro eventos en la lista de eventos.

Observe la página del explorador Web del cliente Web. ¿Cambió algo?

El servidor Web devolvió la página Web.

Paso 3: Explorar el contenido del paquete HTTP

a. Haga clic en el primer cuadro coloreado debajo de la columna **Event List** > **Info** (Lista de eventos > Información). Quizá sea necesario expandir el **panel de simulación** o usar la barra de desplazamiento que se encuentra directamente debajo de la **lista de eventos**.

Se muestra la ventana **PDU Information at Device: Web Client** (Información de PDU en dispositivo: cliente Web). En esta ventana, solo hay dos fichas, **OSI Model** (Modelo OSI) y **Outbound PDU Details** (Detalles de PDU saliente), debido a que este es el inicio de la transmisión. A medida que se analizan más eventos, se muestran tres fichas, ya que se agrega la ficha **Inbound PDU Details** (Detalles de PDU entrante). Cuando un evento es el último evento del stream de tráfico, solo se muestran las fichas **OSI Model** e **Inbound PDU Details**.

b. Asegúrese de que esté seleccionada la ficha **OSI Model**. En la columna **Out Layers** (Capas de salida), asegúrese de que el cuadro **Layer 7** (Capa 7) esté resaltado.

¿Cuál es el texto que se muestra junto a la etiqueta **Layer 7**? HTTP

¿Qué información se indica en los pasos numerados directamente debajo de los cuadros **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida)?

"1. The HTTP client sends a HTTP request to the server." ("El cliente HTTP envía una solicitud de HTTP al servidor").

c. Haga clic en **Next Layer** (Capa siguiente). Layer 4 (Capa 4) debe estar resaltado. ¿Cuál es el valor de **Dst Port** (Puerto de dest.)? 80

d. Haga clic en **Next Layer** (Capa siguiente). Layer 3 (Capa 3) debe estar resaltado. ¿Cuál es valor de **Dest. IP** (IP de dest.)? 192.168.1.254

e. Haga clic en **Next Layer** (Capa siguiente). ¿Qué información se muestra en esta capa? El encabezado Ethernet II de capa 2 y las direcciones MAC de entrada y salida.

f. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente).

La información que se indica debajo de **PDU Details** (Detalles de PDU) refleja las capas dentro del modelo TCP/IP.

Nota: la información que se indica en la sección **Ethernet II** proporciona información aun más detallada que la que se indica en Layer 2 (Capa 2) en la ficha **OSI Model**. **Outbound PDU Details** (Detalles de PDU saliente) proporciona información más descriptiva y detallada. Los valores de **DEST MAC** (MAC DE DEST.) y de **SRC MAC** (MAC DE ORIGEN) en la sección **Ethernet II** de **PDU Details** (Detalles de PDU) aparecen en la ficha **OSI Model**, en Layer 2, pero no se los identifica como tales.

¿Cuál es la información frecuente que se indica en la sección **IP** de **PDU Details** comparada con la información que se indica en la ficha **OSI Model**? ¿Con qué capa se relaciona? SRC IP (IP DE ORIG.) y DST IP (IP DE DEST.) en la capa 3

¿Cuál es la información frecuente que se indica en la sección **TCP** de **PDU Details** comparada con la información que se indica en la ficha **OSI Model**, y con qué capa se relaciona? SRC PORT (PUERTO DE ORIG.) y DEST PORT (PUERTO DE DEST.) en la capa 4

¿Cuál es el **host** que se indica en la sección **HTTP** de **PDU Details**? ¿Con qué capa se relacionaría esta información en la ficha **OSI Model**? www.osi.local, capa 7

g. Haga clic en el siguiente cuadro coloreado en la columna **Event List** > **Info** (Lista de eventos > Información). Solo la capa 1 está activa (sin atenuar). El dispositivo mueve la trama desde el búfer y la coloca en la red.

h. Avance al siguiente cuadro **Info** (Información) de HTTP dentro de la **lista de eventos** y haga clic en el cuadro coloreado. Esta ventana contiene las columnas **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida). Observe la dirección de la flecha que está directamente debajo de la columna **In Layers**; esta apunta hacia arriba, lo que indica la dirección en la que se transfiere la información. Desplácese por estas capas y tome nota de los elementos vistos anteriormente. En la parte superior de la columna, la flecha apunta hacia la derecha. Esto indica que el servidor ahora envía la información de regreso al cliente.

Compare la información que se muestra en la columna **In Layers** con la de la columna **Out Layers**: ¿cuáles son las diferencias principales? Se intercambiaron los puertos de origen y destino, las direcciones IP de origen y destino, y las direcciones MAC.

i. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). Desplácese hasta la sección **HTTP**.

¿Cuál es la primera línea del mensaje HTTP que se muestra? HTTP/1.1 200 OK: esto significa que la solicitud se realizó correctamente y que se entregó la página desde el servidor.

j. Haga clic en el último cuadro coloreado de la columna **Info**. ¿Cuántas fichas se muestran con este evento y por qué?

Solo dos, una para OSI Model y una para Inbound PDU Details, ya que este es el dispositivo receptor.

Parte 2: Mostrar elementos de la suite de protocolos TCP/IP

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer para ver y examinar algunos de los otros protocolos que componen la suite TCP/IP.

Paso 1: Ver eventos adicionales

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

b. En la sección Event List Filters > Visible Events (Filtros de lista de eventos > Eventos visibles), haga clic en **Show All** (Mostrar todo).

¿Qué tipos de eventos adicionales se muestran? Según si se produjo alguna comunicación antes de iniciar la simulación original, ahora debe haber entradas para ARP, DNS, TCP y HTTP. Es posible que no se puedan mostrar las entradas de ARP, según lo que haya hecho el estudiante antes de pasar al modo de simulación. Si la actividad se inicia desde cero, se muestran todas esas.

Estas entradas adicionales cumplen diversas funciones dentro de la suite TCP/IP. Si el protocolo de resolución de direcciones (ARP) está incluido, busca direcciones MAC. El protocolo DNS es responsable de convertir un nombre (por ejemplo, **www.osi.local**) a una dirección IP. Los eventos de TCP adicionales son responsables de la conexión, del acuerdo de los parámetros de comunicación y de la desconexión de las sesiones de comunicación entre los dispositivos. Estos protocolos se mencionaron anteriormente y se analizarán en más detalle a medida que avance el curso. Actualmente, hay más de 35 protocolos (tipos de evento) posibles para capturar en Packet Tracer.

c. Haga clic en el primer evento de DNS en la columna **Info**. Examine las fichas **OSI Model** y **PDU Detail**, y observe el proceso de encapsulación. Al observar la ficha **OSI Model** con el cuadro **Layer 7** resaltado, se incluye una descripción de lo que ocurre, inmediatamente debajo de **In Layers** y **Out Layers**: (“1. The DNS client sends a DNS query to the DNS server.” [“El cliente DNS envía una consulta DNS al servidor DNS”]). Esta información es muy útil para ayudarlo a comprender qué ocurre durante el proceso de comunicación.

d. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿Qué información se indica en **NAME**: (NOMBRE:) en la sección DNS QUERY (CONSULTA DNS)?

www.osi.local

e. Haga clic en el último cuadro coloreado **Info** de DNS en la lista de eventos. ¿Qué dispositivo se muestra?

El cliente Web.

¿Cuál es el valor que se indica junto a **ADDRESS**: (DIRECCIÓN:) en la sección DNS ANSWER (RESPUESTA DE DNS) de **Inbound PDU Details**?

192.168.1.254, la dirección del servidor Web.

f. Busque el primer evento de **HTTP** en la lista y haga clic en el cuadro coloreado del evento de **TCP** que le sigue inmediatamente a este evento. Resalte **Layer 4** (Capa 4) en la ficha **OSI Model** (Modelo OSI). En la lista numerada que está directamente debajo de **In Layers** y **Out Layers**, ¿cuál es la información que se muestra en los elementos 4 y 5?

4. La conexión TCP se realizó correctamente. 5. El dispositivo establece el estado de la conexión en ESTABLISHED (ESTABLECIDA).

El protocolo TCP administra la conexión y la desconexión del canal de comunicación, además de tener otras responsabilidades. Este evento específico muestra que SE ESTABLECIÓ el canal de comunicación.

g. Haga clic en el último evento de TCP. Resalte Layer 4 (Capa 4) en la ficha **OSI Model** (Modelo OSI). Examine los pasos que se indican directamente a continuación de **In Layers** y **Out Layers**. ¿Cuál es el propósito de este evento, según la información proporcionada en el último elemento de la lista (debe ser el elemento 4)? CERRAR la conexión.

Desafío

En esta simulación, se proporcionó un ejemplo de una sesión Web entre un cliente y un servidor en una red de área local (LAN). El cliente realiza solicitudes de servicios específicos que se ejecutan en el servidor. Se debe configurar el servidor para que escuche puertos específicos y detecte una solicitud de cliente. (Sugerencia: observe Layer 4 [Capa 4] en la ficha **OSI Model** para obtener información del puerto).

Sobre la base de la información que se analizó durante la captura de Packet Tracer, ¿qué número de puerto escucha el **servidor Web** para detectar la solicitud Web? La primera PDU HTTP que solicita el cliente Web muestra el puerto 80 en el puerto DST (DESTINO) de capa 4.

¿Qué puerto escucha el **servidor Web** para detectar una solicitud de DNS? La primera PDU DNS que solicita el cliente Web muestra que el puerto de destino de capa 4 es el puerto 53.

Tabla de calificación sugerida

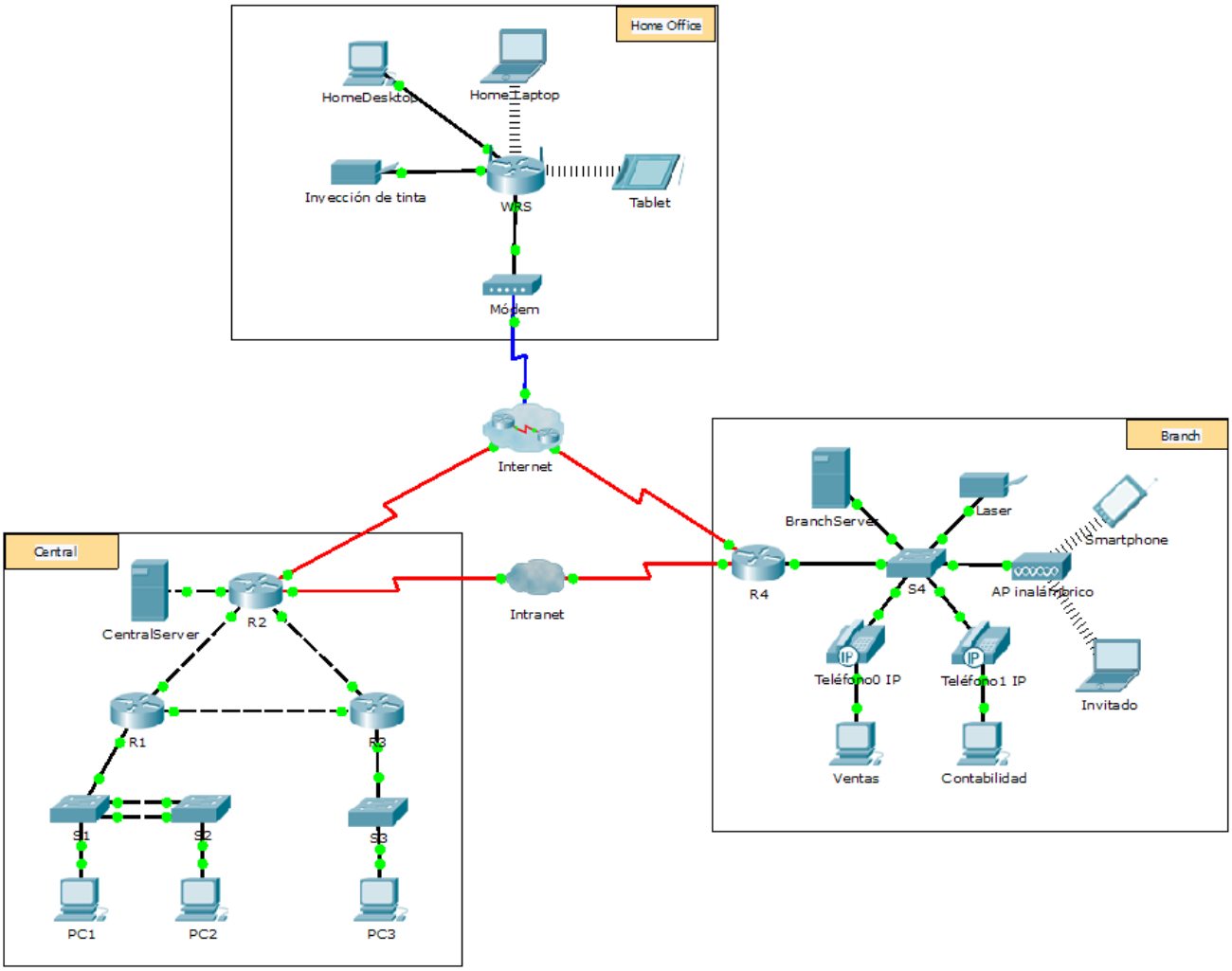
Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar el tráfico Web HTTP	Paso 2d	5	
	Paso 3b-1	5	
	Paso 3b-2	5	
	Paso 3c	5	
	Paso 3d	5	
	Paso 3e	5	
	Paso 3f-1	5	
	Paso 3f-2	5	
	Paso 3f-3	5	
	Paso 3h	5	
	Paso 3i	5	
	Paso 3j	5	
Total de la parte 1		**60**	
Parte 2: Mostrar elementos de la suite de protocolos TCP/IP	Paso 1b	5	
	Paso 1d	5	
	Paso 1e-1	5	
	Paso 1e-2	5	
	Paso 1f	5	
	Paso 1g	5	
Total de la parte 2		**30**	
Desafío	Lo1	5	
	2	5	
Total de la parte 3		**10**	
Puntuación total		**100**	

Packet Tracer: Exploración de una red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

En esta actividad, se utiliza una topología compleja y un dominio del nivel superior ficticio (.pta) para evitar conflictos con la nomenclatura para Internet. Dado que PT no reenvía las solicitudes de DNS, se crearon las mismas entradas en cada servidor DNS para que el tráfico DNS pueda seguir siendo local cuando es importante hacerlo. Para abordar el uso de direccionamiento privado RFC 1918, se utiliza NAT en la oficina doméstica y en la sucursal, a fin de evitar cualquier concepto erróneo.

Topología



Objetivos

Parte 1: Examinar el tráfico de internetwork en la sucursal

Parte 2: Examinar el tráfico de internetwork a la central

Parte 3: Examinar el tráfico de Internet desde la sucursal

Información básica

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

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

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

Parte 1: Examinar el tráfico de internetwork en la sucursal

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

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

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

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

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

Paso 2: Generar tráfico mediante un explorador Web

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

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

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

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

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

La solicitud de DNS de la dirección IP de branchserver.pt.pta.

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

La información de capa 2, específicamente la dirección MAC de destino.

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

Todos los dispositivos recibieron una solicitud de ARP.

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

El servidor DNS recibe una consulta DNS. La consulta del nombre se resuelve de forma local.

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

172.16.0.3, la dirección de Branchserver.

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

Establecido

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

Dos capas, porque son dispositivos de capa 2.

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

El cliente HTTP recibe una respuesta de HTTP del servidor. Muestra la página en el explorador Web.

Parte 2: Examinar el tráfico de internetwork a la central

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

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

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

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

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

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

Sales PC ya conoce la dirección MAC del servidor DNS.

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

Al observar la información proporcionada, ¿qué se puede determinar sobre los resultados de DNS?
El servidor DNS pudo resolver el nombre de dominio para centralserver.pt.pta.

f. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante). Desplácese hasta la sección **DNS ANSWER** (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta?
10.10.10.2.

g. Los eventos siguientes son eventos de **ARP**. Haga clic en el cuadro coloreado Info del último evento de **ARP**. Haga clic en la ficha **Inbound PDU Details** y observe la dirección MAC. Sobre la base de la información en la sección de ARP, ¿qué dispositivo proporciona la respuesta de ARP? El router R4, el dispositivo de gateway.

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

Es la dirección MAC del router R4.

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

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

Parte 3: Examinar el tráfico de Internet desde la sucursal

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

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

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

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

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

Hay muchos más eventos de DNS. Dado que la entrada de DNS no es local, se reenvía hacia un servidor en Internet.

d. Observe algunos de los dispositivos a través de los que se transfieren los eventos de **DNS** en el camino hacia un servidor DNS. ¿Dónde se encuentran estos dispositivos? En la nube de Internet. Se debe mostrar a los estudiantes que esos dispositivos se pueden ver haciendo clic en la nube y luego en el enlace Back (Atrás) para regresar.

e. Haga clic en el último evento de **DNS**. Haga clic en la ficha **Inbound PDU Details** y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para **www.netacad.pta**? 216.146.46.11

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

Hay tres routers (ISP-Tier3a, ISP-Tier3b y R4); sin embargo, hay cuatro eventos de HTTP que los atraviesan.

g. Haga clic en el evento de **TCP** anterior al último evento de **HTTP**. Según la información que se muestra, ¿cuál es el propósito de este evento? Cerrar la conexión TCP a 216.146.46.11.

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

Tabla de calificación sugerida

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

Packet Tracer: Conexión de una LAN por cable y una LAN inalámbrica (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

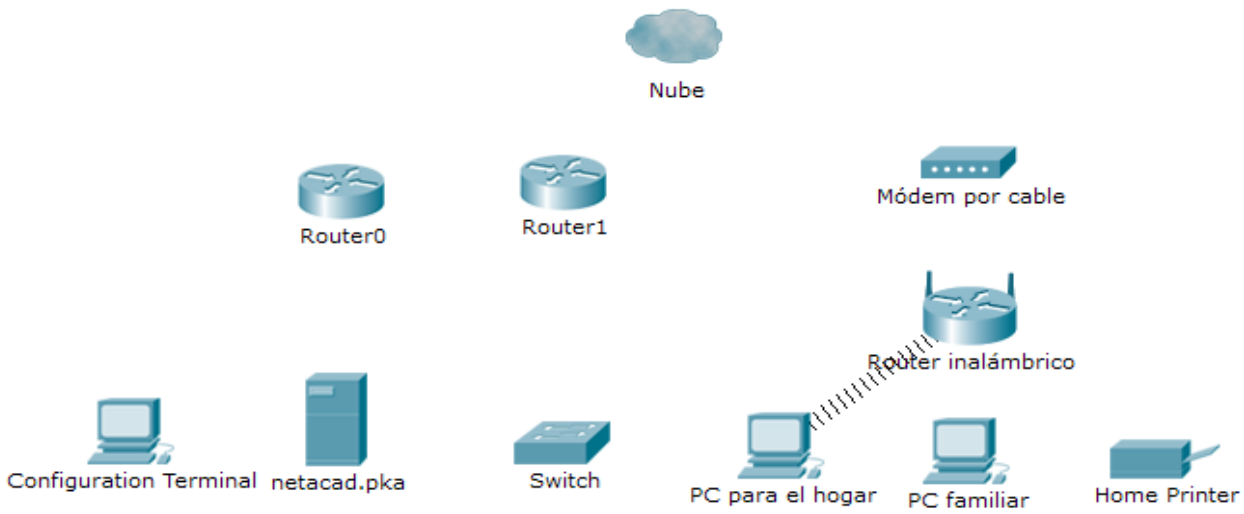


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Conectar a
Nube	Eth6	No aplicable	Fa0/0
	Coax7	No aplicable	Port0
Módem por cable	Port0	No aplicable	Coax7
	Puerto1	No aplicable	Internet
Router0	Consola	No aplicable	RS232
	Fa0/0	192.168.2.1/24	Eth6
	Fa0/1	10.0.0.1/24	Fa0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	Fa1/0	172.16.0.1/24	Fa0/1
Router inalámbrico	Internet	192.168.2.2/24	Puerto 1
	Eth1	192.168.1.1	Fa0
PC familiar	Fa0	192.168.1.102	Eth1
Switch	Fa0/1	172.16.0.2	Fa1/0
Netacad.pka	Fa0	10.0.0.1	Fa0/1
Terminal de configuración	RS232	No aplicable	Consola

Objetivos

Parte 1: Conectarse a la nube

Parte 2: Conectar el Router0

Parte 3: Conectar los dispositivos restantes

Parte 4: Verificar las conexiones

Parte 5: Examinar la topología física

Información básica

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

Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0

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

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

Paso 2: Conectar la nube al módem por cable

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

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

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

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

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

Paso 2: Conectar el Router0 a netacad.pka

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

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

Paso 3: Conectar el Router0 a la terminal de configuración

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

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

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

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

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

Paso 2: Conectar el módem por cable al router inalámbrico

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

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

Paso 3: Conectar el router inalámbrico a la PC familiar

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

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

Parte 4: Verificar las conexiones

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

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

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

Paso 2: Hacer ping al switch desde la PC doméstica

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

Paso 3: Abrir el Router0 desde la terminal de configuración

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

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

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

Parte 5: Examinar la topología física

Paso 1: Examinar la nube

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

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

f. Haga clic en el ícono **Cloud** (Nube). ¿Cuántos cables están conectados al switch en el bastidor azul? 2

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

Paso 2: Examinar la red principal

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

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

Paso 3: Examinar la red secundaria

j. Haga clic en el ícono **Secondary Network** (Red secundaria). Mantenga el puntero del mouse sobre los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo? Los cables de fibra vienen en pares, uno para transmitir y otro para recibir.

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

Paso 4: Examinar la red doméstica

l. ¿Por qué hay una malla ovalada que cubre la red doméstica? Representa el alcance de la red inalámbrica.

m. Haga clic en el ícono **Home Network** (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo? Por lo general, las redes domésticas no incluyen bastidores.

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

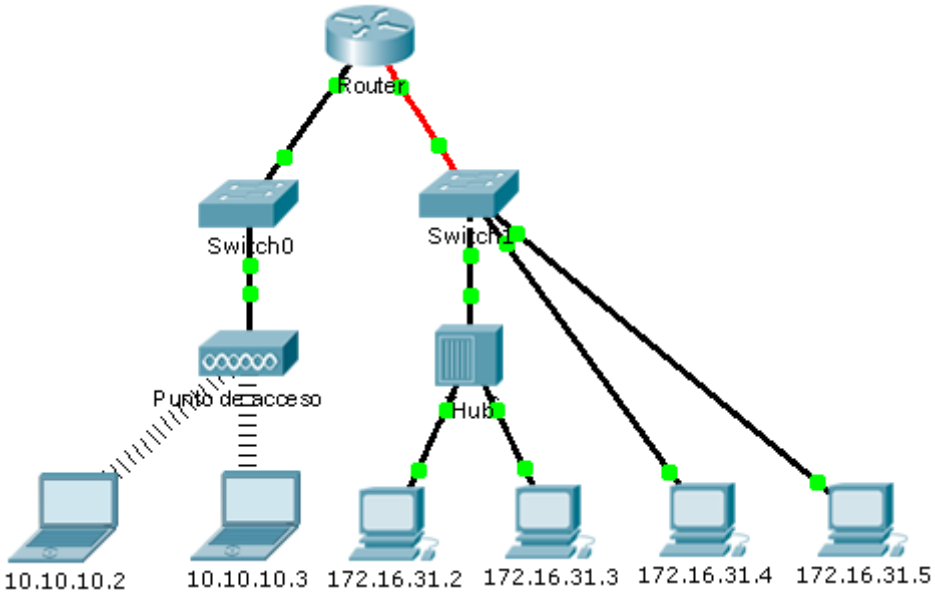
Tabla de calificación sugerida

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

Packet Tracer: Identificación de direcciones MAC y direcciones IP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Recopilar información de la PDU

Parte 2: Preguntas de reflexión

Información básica

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

Parte 1: Recopilar información de la PDU

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

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

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

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

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

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

- Dirección MAC de destino: 00D0:BA8E:741A
- Dirección MAC de origen: 000C:85CC:1DA7
- Dirección IP de origen: 172.16.31.2
- Dirección IP de destino: 10.10.10.3
- En el dispositivo: PC

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

Formato de hoja de cálculo de ejemplo

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

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

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

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

Parte 2: Preguntas de reflexión

Responda las siguientes preguntas relacionadas con la información reunida:

1. ¿Se utilizaron diferentes tipos de cables para conectar los dispositivos? Sí, de cobre y de fibra.
2. ¿Los cables cambiaron el manejo de la PDU de alguna forma? No
3. ¿El **hub** perdió la información que se le entregó? No
4. ¿Qué hace el **hub** con las direcciones MAC y las direcciones IP? Nada.
5. ¿El **punto de acceso inalámbrico** hizo algo con la información que se le entregó? Sí. La volvió a empaquetar según el estándar inalámbrico 802.11.
6. ¿Se perdió alguna dirección MAC o IP durante la transferencia inalámbrica? No

7. ¿Cuál fue la capa OSI más alta que utilizaron el **hub** y el **punto de acceso**? Capa 1
8. ¿El **hub** o el **punto de acceso** reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? Sí
9. Al examinar la ficha **PDU Details** (Detalles de PDU), ¿que dirección MAC aparecía primero, la de origen o la de destino? Destino
10. ¿Por qué las direcciones MAC aparecen en este orden? Si el destino aparece primero en la lista, un switch puede comenzar a reenviar una trama a una dirección MAC conocida más rápidamente.
11. ¿Había un patrón para el direccionamiento MAC en la simulación? No
12. ¿Los switches reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? No
13. Cada vez que se enviaba la PDU entre las redes 10 y 172, había un punto donde las direcciones MAC cambiaban repentinamente. ¿Dónde ocurrió eso? En el router.
14. ¿Qué dispositivo utiliza las direcciones MAC que comienzan con 00D0? El router.
15. ¿A qué dispositivos pertenecen las otras direcciones MAC? Al emisor y al receptor.
16. ¿Las direcciones IPv4 de envío y recepción cambian en alguna de las PDU? No
17. Si sigue la respuesta a un ping, a veces denominado *pong*, ¿las direcciones IPv4 de envío y recepción cambian? Sí
18. ¿Cuál es el patrón para el direccionamiento IPv4 en esta simulación? Cada puerto de router requiere un conjunto de direcciones que no se superpongan.
19. ¿Por qué es necesario asignar diferentes redes IP a los diferentes puertos de un router? La función de un router es interconectar diferentes redes IP.
20. Si esta simulación fuera configurada con IPv6 en vez de IPv4, ¿cuál sería la diferencia? Las direcciones IPv4 se reemplazarían con direcciones IPv6, pero todo lo demás sería igual.

Tabla de calificación sugerida

Hay 20 preguntas que valen cinco puntos cada una para obtener una posible puntuación de 100.

Packet Tracer: Revisión de la tabla ARP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

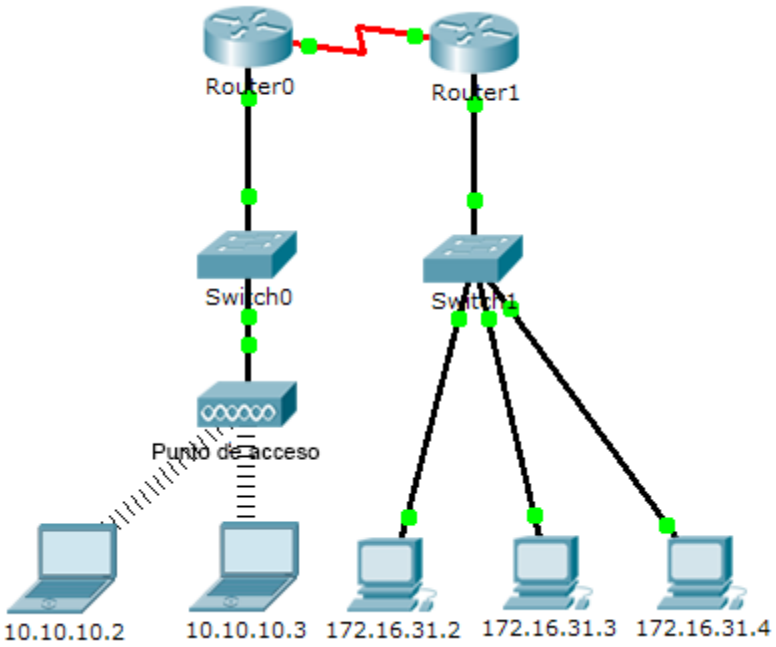


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gig0/0	0001.6458.2501	Gig1/1
	Se0/0/0	No aplicable	No aplicable
Router1	Gig0/0	00E0.F7B1.8901	Gig1/1
	Se0/0/0	No aplicable	No aplicable
10.10.10.2.	Inalámbrico	0060.2F84.4AB6	Fa0/2
10.10.10.3	Inalámbrico	0060.4706.572B	Fa0/2
172.16.31.2	Fa0	000C.85CC.1DA7	Fa0/1
172.16.31.3	Fa0	0060.7036.2849	Fa0/2
172.16.31.4	Gig0	0002.1640.8D75	Fa0/3

Objetivos

Parte 1: Examinar una solicitud de ARP

Parte 2: Examinar una tabla de direcciones MAC del switch

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Información básica

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

Parte 1: Examinar una solicitud de ARP

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

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

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

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

d. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. La PDU ARP mueve el **Switch1**, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior? No

e. Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**? 3

f. ¿Cuál es la dirección IP del dispositivo que aceptó la PDU? 172.16.31.3

g. Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino? El origen se transformó en el destino, FFFF.FFFF.FFFF se convirtió en la dirección MAC de 172.16.31.3.

h. Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP? 1

Paso 2: Revisar la tabla ARP

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

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

c. Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC? 172.16.31.3

d. En general, ¿cuándo emite un dispositivo final una solicitud de ARP? Cuando no conoce la dirección MAC del receptor.

Parte 2: Examinar una tabla de direcciones MAC del switch

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

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

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

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

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

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

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

c. ¿Por qué hay dos direcciones MAC asociadas a un puerto? Porque ambos dispositivos se conectan a un puerto a través del punto de acceso.

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

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

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

c. Escriba **arp -a**. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP? 172.16.31.1

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

e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen? 2

f. Haga clic en **Capture/Forward** (Capturar/avanzar). Haga clic en la PDU que ahora se encuentra en el **Switch1**. ¿Cuál es la dirección IP de destino de la solicitud de ARP? 172.16.31.1

g. La dirección IP de destino no es 10.10.10.1. ¿Por qué? La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

Paso 2: Examinar la tabla ARP en el Router1

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

b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué? Ninguna, este comando significa algo totalmente distinto que el comando show mac address-table de un switch.

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

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

Tabla de calificación sugerida

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

Packet Tracer: Configuración de switches de capa 3

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

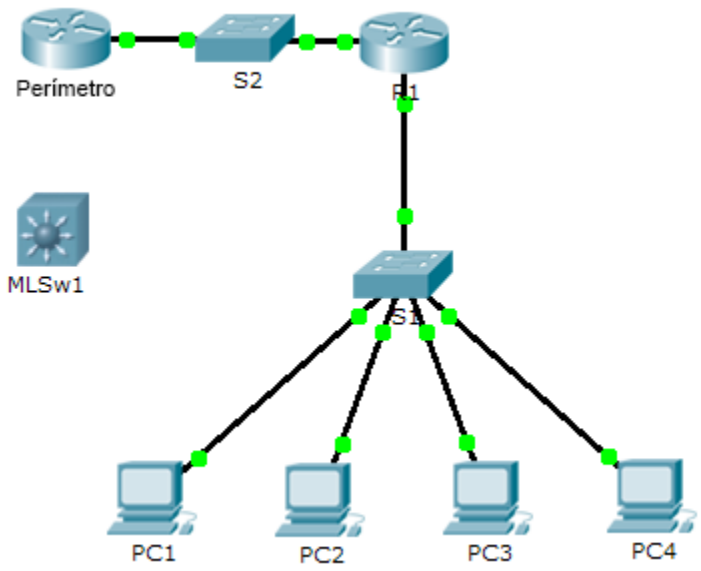


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0	172.16.31.1	255.255.255.0
	G0/1	192.168.0.2	255.255.255.0
MLSw1	G0/1	192.168.0.2	255.255.255.0
	VLAN 1	172.16.31.1	255.255.255.0

Objetivos

Parte 1: Documentar la configuración actual de la red

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

Situación

El administrador de red reemplaza el router y el switch actuales por un nuevo switch de capa 3. Como técnico de red, su trabajo consiste en configurar el switch y ponerlo en funcionamiento. Trabajará después del horario laboral para minimizar los inconvenientes para la empresa.

Nota: esta actividad comienza con una puntuación de 8/100, debido a que ya se calificaron las conexiones de los dispositivos para las PC. En la parte 2, eliminará y restaurará estas conexiones. La puntuación se incluye para verificar que haya restaurado correctamente las conexiones.

Parte 1: Documentar la configuración actual de la red

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

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

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

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

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

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

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

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

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

d. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/1** y active el puerto.

e. Ingrese al modo de configuración de interfaz para **interface VLAN1**.

f. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/0** y active el puerto.

g. Guarde la configuración.

Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

Nota: por lo general, los siguientes pasos se llevarían a cabo después del horario laboral o cuando el tráfico en la red de producción está en su volumen más bajo. Para minimizar el tiempo de inactividad, el nuevo equipo debe estar totalmente configurado y listo para implementar.

a. Haga clic en un área vacía de la pantalla para anular la selección de todos los dispositivos.

b. Use la herramienta **Delete** (Eliminar) para eliminar todas las conexiones o simplemente elimine **R1**, **S1** y **S2**.

c. Seleccione los cables adecuados para completar lo siguiente:

- Conectar **MLSw1 GigabitEthernet 0/1** a **Edge GigabitEthernet 0/0**.
- Conectar las PC a los puertos Fast Ethernet en **MLSw1**.

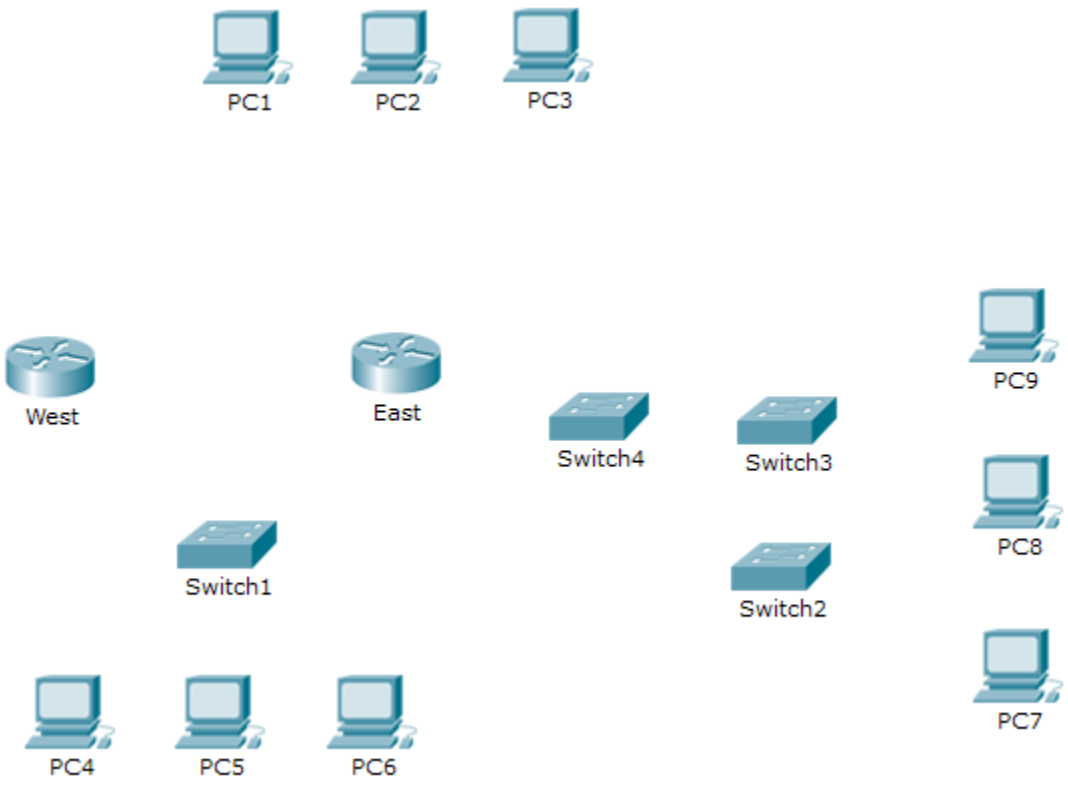
d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.

Nota: espere hasta que las luces de enlace anaranjadas cambien a color verde.

Packet Tracer: Exploración de dispositivos de internetworking (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Identificar las características físicas de los dispositivos de internetworking

Parte 2: Seleccionar los módulos correctos para la conectividad

Parte 3: Conectar los dispositivos

Información básica

En esta actividad, explorará las diversas opciones disponibles en los dispositivos de internetworking. También deberá determinar qué opciones proporcionan la conectividad necesaria al conectar varios dispositivos. Finalmente, agregará los módulos correctos y conectará los dispositivos.

Nota: la calificación de esta actividad es una combinación de la puntuación automatizada de Packet Tracer y las respuestas que registró para las preguntas que se formularon en las instrucciones. Consulte la Suggested Scoring Rubric que se encuentra al final de esta actividad y consulte al instructor para determinar su puntuación final.

Parte 1: Identificar las características físicas de los dispositivos de internetworking

Paso 1: Identificar los puertos de administración de un router Cisco

a. Haga clic en el router **East** (Este). La ficha **Physical** (Capa física) debe estar activa.

b. Acerque el elemento y expanda la ventana para ver todo el router.

c. ¿Qué puertos de administración se encuentran disponibles? Los puertos auxiliar y de consola

Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay? Hay dos interfaces WAN y dos interfaces Gigabit Ethernet.

b. Haga clic en la ficha **CLI** e introduzca los siguientes comandos:

```
East> show ip interface brief
```

El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican? 4

c. Introduzca los siguientes comandos:

```
East> show interface gigabitethernet 0/0
```

¿Cuál es el ancho de banda predeterminado de esta interfaz? 1 000 000 Kbit

```
East> show interface serial 0/0/0
```

¿Cuál es el ancho de banda predeterminado de esta interfaz? 1544 Kbit

Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

Paso 3: Identificar las ranuras de expansión de módulos en los switches

a. ¿Cuántas ranuras de expansión se encuentran disponibles para agregar más módulos al router **East**? 1

b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles? Cada uno tiene cinco ranuras disponibles.

Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

a. Haga clic en **East** y, a continuación, haga clic en la ficha **Physical**. En el lado izquierdo, debajo de la etiqueta **Modules** (Módulos), se ven las opciones disponibles para expandir las capacidades del router. Haga clic en cada módulo. Se muestra una imagen y una descripción en la parte inferior. Familiarícese con estas opciones.

1) Debe conectar las PC 1, 2 y 3 al router **East**, pero no cuenta con los fondos necesarios para adquirir un nuevo switch. ¿Qué módulo puede usar para conectar las tres PC al router **East**? Módulo HWIC-4ESW

2) ¿Cuántos hosts puede conectar al router mediante este módulo? 4

b. Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**? PT-SWITCH-NM-1FGE

Paso 2: Agregar los módulos correctos y encender los dispositivos

a. Haga clic en **East** e intente insertar el módulo adecuado del paso 1a.

b. Debe aparecer el mensaje `Cannot add a module when the power is on` (No se puede agregar un módulo cuando el dispositivo está encendido). Las interfaces para este modelo de router no son intercambiables en caliente. Se debe apagar el dispositivo. Haga clic en el interruptor de alimentación que se encuentra a la derecha del logotipo de Cisco para apagar **East**. Inserte el módulo adecuado del paso 1a. Cuando haya terminado, haga clic en el interruptor de alimentación para encender **East**.

Nota: si inserta el módulo incorrecto y debe quitarlo, arrastre el módulo hasta su imagen en la esquina inferior derecha y suelte el botón del mouse.

c. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo.

¿En qué ranura se insertó? GigabitEthernet5/1

e. Haga clic en el router **West** (Oeste). La ficha **Physical** (Capa física) debe estar activa. Instale el módulo adecuado que agregará una interfaz serial a la ranura para tarjetas de interfaz WAN de alta velocidad mejoradas (**EHWIC 0**) de la derecha. Puede cubrir las ranuras sin utilizar para evitar que ingrese polvo al router (optativo).

f. Use el comando adecuado para verificar que se hayan instalado las nuevas interfaces seriales.

Parte 3: Conectar los dispositivos

Esta puede ser la primera actividad que realiza en la que se le solicita conectar dispositivos. Si bien es posible que no conozca el propósito de los distintos tipos de cables, use la tabla que se encuentra a continuación y siga estas pautas para conectar correctamente todos los dispositivos:

a. Seleccione el tipo de cable adecuado.

b. Haga clic en el primer dispositivo y seleccione la interfaz especificada.

c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.

d. Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

Ejemplo: para conectar **East** al **Switch1**, seleccione el tipo de cable de **cobre de conexión directa**. Haga clic en **East** y elija **GigabitEthernet0/0**. Luego, haga clic en **Switch1** y elija **GigabitEthernet1/1**. Su puntuación ahora debe ser de 4/52.

Nota: a los efectos de esta actividad, se deshabilitaron las luces de enlace. Los dispositivos no están configurados con ningún direccionamiento IP, de modo que no puede probar la conectividad.

Dispositivo	Interfaz	Tipo de cable	Dispositivo	Interfaz
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet1/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet1/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0

Switch1	FastEthernet0/1	Cable de cobre de conexión directa	PC4	FastEthernet0
Switch1	FastEthernet0/2	Cable de cobre de conexión directa	PC5	FastEthernet0
Switch1	FastEthernet0/3	Cable de cobre de conexión directa	PC6	FastEthernet0
Switch4	GigabitEthernet1/2	Cross-Over de cobre	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fibra	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Cable de cobre de conexión directa	PC7	FastEthernet0
Switch2	FastEthernet1/1	Cable de cobre de conexión directa	PC8	FastEthernet0
Switch2	FastEthernet2/1	Cable de cobre de conexión directa	PC9	FastEthernet0
East	Serial0/0/0	DCE serial (conectar primero a East)	West	Serial0/0/0

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Identificar las características físicas de los dispositivos de internetworking	Paso 1c	4	
	Paso 2a	4	
	Paso 2b	4	
	Paso 2c, pregunta 1	4	
	Paso 2c, pregunta 2	4	
	Paso 3a	4	
	Paso 3b	4	
Total de la parte 1		**28**	
Parte 2: Seleccionar los módulos correctos para la conectividad	Paso 1a, pregunta 1	5	
	Paso 1a, pregunta 2	5	
	Paso 1b	5	
	Paso 2d	5	
Total de la parte 2		**20**	
Puntuación de Packet Tracer		**52**	
Puntuación total		**100**	

Packet Tracer: Configuración inicial del router

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Objetivos

Parte 1: Verificar la configuración predeterminada del router

Parte 2: Configurar y verificar la configuración inicial del router

Parte 3: Guardar el archivo de configuración en ejecución

Información básica

En esta actividad, configurará los parámetros básicos del router. Proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También configurará mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten a los usuarios no autorizados que el acceso está prohibido. Finalmente, verificará y guardará la configuración en ejecución.

Parte 1: Verificar la configuración predeterminada del router

Paso 1: Establecer una conexión de consola al R1

a. Elija un cable de **consola** de las conexiones disponibles.

b. Haga clic en **PCA** y seleccione **RS 232**.

c. Haga clic en **R1** y seleccione **Console** (Consola).

d. Haga clic en **PCA** > ficha **Desktop** (Escritorio) > **Terminal**.

e. Haga clic en **OK** (Aceptar) y presione **Entrar**. Ahora puede configurar **R1**.

Paso 2: Ingresar al modo privilegiado y examinar la configuración actual

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

a. Introduzca el modo EXEC privilegiado introduciendo el comando **enable.**

```
Router> enable
Router#
```

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

b. Introduzca el comando **show running-config**:

```
Router# show running-config
```

c. Responda las siguientes preguntas:

¿Cuál es el nombre de host del router? Router

¿Cuántas interfaces Fast Ethernet tiene el router? 4

¿Cuántas interfaces Gigabit Ethernet tiene el router? 2

¿Cuántas interfaces seriales tiene el router? 2

¿Cuál es el rango de valores que se muestra para las líneas vty? 0 - 4

d. Muestre el contenido actual de la NVRAM.

```
Router# show startup-config
startup-config is not present
```

¿Por qué el router responde con el mensaje `startup-config is not present`? Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.

Parte 2: Configurar y verificar la configuración inicial del router

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

Paso 1: Configurar los parámetros iniciales de R1

Nota: si tiene dificultad para recordar los comandos, consulte el contenido de este tema. Los comandos son los mismos que configuró en un switch.

a. Establezca **R1** como nombre de host.

b. Utilice las siguientes contraseñas:

1) Consola: **letmein**

2) EXEC privilegiado, sin encriptar: **cisco**

3) EXEC privilegiado, encriptado: **itsasecret**

c. Encripte todas las contraseñas de texto no cifrado.

d. Texto del mensaje del día: `Unauthorized access is strictly prohibited` (El acceso no autorizado queda terminantemente prohibido).

Nota: la actividad se configura con una expresión normal para que solo se detecte la palabra “access” en el comando **banner motd** del alumno.

Paso 2: Verificar los parámetros iniciales de R1

a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza? show running-config

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:

```
R1 con0 is now available


Press RETURN to get started.
```

c. Presione **Entrar**; debería ver el siguiente mensaje:

```
Unauthorized access is strictly prohibited.


User Access Verification


Password:
```

¿Por qué todos los routers deben tener un mensaje del día (MOTD)? Cada router debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).

Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?
`R1(config-line)# login`

d. Introduzca las contraseñas necesarias para regresar al modo EXEC privilegiado.

¿Por qué la contraseña **secreta de enable** permitiría el acceso al modo EXEC privilegiado y **la contraseña de enable** dejaría de ser válida? La **contraseña secreta de enable** sobrescribe la contraseña de enable. Si ambas están configuradas en el router, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique. El comando service password-encryption encripta todas las contraseñas actuales y futuras.

Parte 3: Guardar el archivo de configuración en ejecución

Paso 1: Guarde el archivo de configuración en la NVRAM.

a. Configuró los parámetros iniciales de **R1**. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM? `copy running-config startup-config`

¿Cuál es la versión más corta e inequívoca de este comando? `copy r s`

¿Qué comando muestra el contenido de la NVRAM? `show startup-configuration or show start`

b. Verifique que todos los parámetros configurados estén registrados. Si no fuera así, analice el resultado y determine qué comandos no se introdujeron o se introdujeron incorrectamente. También puede hacer clic en **Check Results** (Verificar resultados) en la ventana de instrucción.

Paso 2: Puntos extra optativos: guarde el archivo de configuración de inicio en la memoria flash.

Aunque aprenderá más sobre la administración del almacenamiento flash de un router en los siguientes capítulos, le puede interesar saber ahora que puede guardar el archivo de configuración de inicio en la memoria flash como procedimiento de respaldo adicional. De manera predeterminada, el router seguirá cargando la configuración de inicio desde la NVRAM, pero si esta se daña, puede restablecer la configuración de inicio copiándola de la memoria flash.

Complete los siguientes pasos para guardar la configuración de inicio en la memoria flash.

a. Examine el contenido de la memoria flash mediante el comando **show flash**:

```
R1# show flash
```

¿Cuántos archivos hay almacenados actualmente en la memoria flash? 3

¿Cuál de estos archivos cree que es la imagen de IOS? c1900-universalk9-mz.SPA.151-4.M4.bin

¿Por qué cree que este archivo es la imagen de IOS? Las respuestas pueden variar, pero hay dos pistas: la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo.

b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

```
R1# copy startup-config flash
Destination filename [startup-config]
```

El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione **Entrar**; de lo contrario, escriba un nombre adecuado y presione la tecla **Entrar**.

c. Utilice el comando **show flash** para verificar que el archivo de configuración de inicio esté almacenado en la memoria flash.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Verificar la configuración predeterminada del router	Paso 2c	10	
	Paso 2d	2	
Total de la parte 1		**12**	
Parte 2: Configurar y verificar la configuración inicial del router	Paso 2a	2	
	Paso 2c	5	
	Paso 2d	6	
Total de la parte 2		**13**	
Parte 3: Guardar el archivo de configuración en ejecución	Paso 1a	5	
	Paso 2a (puntos extra)	5	
Total de la parte 3		**10**	
Puntuación de Packet Tracer		**80**	
Puntuación total (con los puntos extra)		**105**	

Packet Tracer: Conexión de un router a una LAN

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

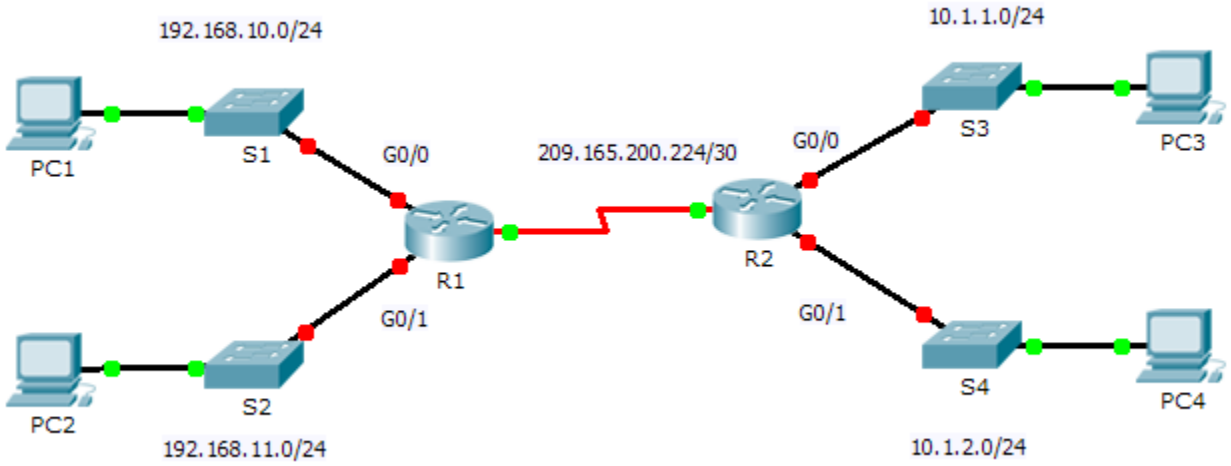


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	No aplicable
	S0/0/0	209.165.200.226	255.255.255.252	No aplicable
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Objetivos

Parte 1: Mostrar la información del router

Paso 2: Configurar las interfaces del router

Paso 3: Verificar la configuración

Información básica

En esta actividad, utilizará diversos comandos **show** para mostrar el estado actual del router. Después utilizará la Tabla de direccionamiento para configurar las interfaces Ethernet del router. Finalmente, utilizará comandos para verificar y probar las configuraciones.

Nota: los routers en esta actividad están parcialmente configurados. Algunas de las configuraciones no se incluyen en este curso, pero se proporcionan para ayudarlo a utilizar los comandos de verificación.

Nota: las interfaces seriales ya están configuradas y activas. Además, el enrutamiento se configuró mediante EIGRP. Esto se hace para que esta actividad 1) sea coherente con los ejemplos que se muestran en el capítulo, y (2) esté lista para proporcionar resultados completos de los comandos **show** cuando el estudiante configure y active las interfaces Ethernet.

Parte 1: Mostrar la información del router

Paso 1: Mostrar la información de la interfaz en el R1.

Nota: haga clic en un dispositivo y, a continuación, en la ficha **CLI** para acceder a la línea de comandos directamente. La contraseña de consola es **cisco**. La contraseña de EXEC privilegiado es **class**.

a. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router? `show` interfaces

b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0? show interface serial 0/0/0

c. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

   1) ¿Cuál es la dirección IP configurada en el **R1**? 209.165.200.225/30

   2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0? 1544 kbits

d. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:

   1) ¿Cuál es la dirección IP en el **R1**? No hay una dirección IP configurada en la interfaz GigabitEthernet 0/0.

   2) ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0? 000d.bd6c.7d01

   3) ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0? 1 000 000 kbits

Paso 2: Mostrar una lista de resumen de las interfaces en el R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas? show ip interface brief

b. Introduzca el comando en cada router y responda las siguientes preguntas:

   1) ¿Cuántas interfaces seriales hay en **R1** y **R2**? Cada router tiene 2 interfaces seriales.

   2) ¿Cuántas interfaces Ethernet hay en **R1** y **R2**? R1 tiene seis interfaces Ethernet y R2 tiene dos interfaces Ethernet.

   3) ¿Son iguales todas las interfaces Ethernet en el **R1**? Si no es así, explique las diferencias. No lo son. Hay dos interfaces Gigabit Ethernet y cuatro interfaces Fast Ethernet. Las interfaces Gigabit Ethernet admiten velocidades de hasta 1 000 000 000 bits, y las interfaces Fast Ethernet admiten velocidades de hasta 1 000 000 bits.

Paso 3: Mostrar la tabla de enrutamiento en el R1

a. ¿Qué comando muestra el contenido de la tabla de enrutamiento? show ip route

b. Introduzca el comando en el **R1** y responda las siguientes preguntas:

1) ¿Cuántas rutas conectadas hay (utilizan el código C)? 1
2) ¿Qué ruta se indica? 209.165.200.224/30
3) ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento? Un router solo envía paquetes a redes indicadas en la tabla de enrutamiento. Si una red no aparece en la lista, el paquete se descarta.

Parte 2: Configurar las interfaces del router

Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1

a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
```

b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.

```
R1(config-if)# description LAN connection to S1
```

c. Ahora, el **R1** debe poder hacer ping a la PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

a. Utilice la información en la Addressing Table para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:
   1) Introduzca la dirección IP y active la interfaz.
   2) Configure una descripción apropiada.

b. Verifique las configuraciones de las interfaces.

Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM

Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó? copy run start

Parte 3: Verificar la configuración

Paso 1: Utilizar los comandos de verificación para revisar la configuración de la interfaz

a. Utilice el comando **show ip interface brief** en **R1** y **R2** para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.

¿Cuántas interfaces en **R1** y **R2** están configuradas con direcciones IP y tienen el estado “up/up” (activa/activa)? Tres en cada router.

¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando? La máscara de subred

¿Qué comandos puede utilizar para verificar esta parte de la configuración? `show run, show interfaces, show ip protocols`

b. Utilice el comando **show ip route** en **R1** y **R2** para ver las tablas de enrutamiento actuales y responda las siguientes preguntas:

1) ¿Cuántas rutas conectadas (utilizan el código **C**) ve en cada router? 3

2) ¿Cuántas rutas EIGRP (utilizan el código **D**) ve en cada router? 2

3) Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y de rutas descubiertas dinámicamente (EIGRP) debe ser igual a la cantidad total de LAN y WAN. ¿Cuántas LAN y WAN hay en la topología? 5

4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? sí

Nota: si su respuesta es “no”, falta una configuración necesaria. Revise los pasos de la parte 2.

Paso 2: Probar la conectividad de extremo a extremo a través de la red

Ahora debería poder hacer ping desde cualquier PC a cualquier otra PC en la red. Además, debería poder hacer ping a las interfaces activas de los routers. Por ejemplo, las siguientes pruebas deberían realizarse correctamente:

- Desde la línea de comandos en la PC1, haga ping a la PC4.
- Desde la línea de comandos en el R2, haga ping a la PC2.

Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Mostrar la información del router	Paso 1a	2	
	Paso 1b	2	
	Paso 1c	4	
	Paso 1d	6	
	Paso 2a	2	
	Paso 2b	6	
	Paso 3a	2	
	Paso 3b	6	
Total de la parte 1		**30**	
Paso 2: Configurar las interfaces del router	Paso 3	2	
Total de la parte 2		**2**	
Paso 3: Verificar la configuración	Paso 1a	6	
	Paso 1b	8	
Total de la parte 3		**14**	
Puntuación de Packet Tracer		**54**	
Puntuación total (con los puntos extra)		**100**	

Packet Tracer: Resolución de problemas del gateway predeterminado (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

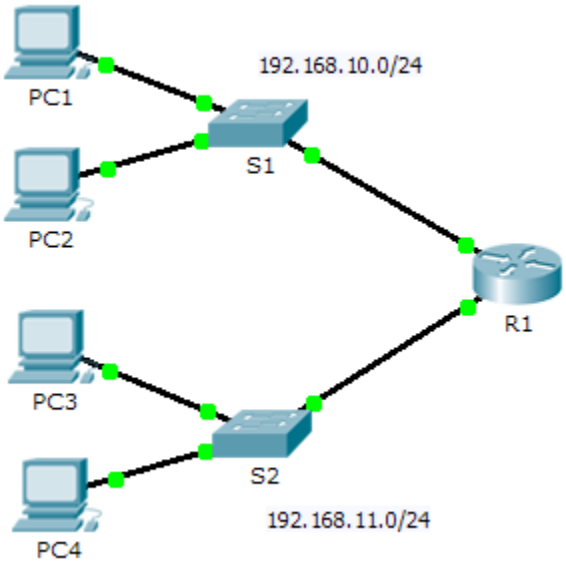


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Objetivos

Parte 1: Verificar el registro de la red y descartar problemas

Parte 2: Implementar, verificar y documentar las soluciones

Información básica

Para que un dispositivo se comunique a través de varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se utiliza cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local a la que el host está conectado. En esta actividad, terminará de documentar la red. A continuación, verificará la documentación de la red mediante la puesta a prueba de la conectividad de extremo a extremo y la resolución de problemas. El método de resolución de problemas que utilizará consta de los siguientes pasos:

1) Verificar la documentación de la red y utilizar pruebas para descartar problemas.
2) Determinar cuál es la solución adecuada para un problema dado.
3) Implementar la solución.
4) Realizar pruebas para verificar que se haya resuelto el problema.
5) Documentar la solución.

A lo largo de sus estudios de CCNA, encontrará distintas descripciones del método de resolución de problemas, así como distintas formas de probar y documentar problemas y soluciones. Esto es intencional. No existe un estándar o una plantilla establecida para la resolución de problemas. Cada organización desarrolla procesos y estándares de documentación exclusivos (incluso si ese proceso consiste en no tener ninguno). No obstante, todas las metodologías de resolución de problemas eficaces generalmente incluyen los pasos anteriores.

Nota: si usted es experto en la configuración de gateway predeterminado, es posible que esta actividad parezca más compleja de lo debido. Lo más probable es que pueda descubrir y solucionar todos los problemas de conectividad más rápido que si siguiera estos procedimientos. No obstante, a medida que avance con sus estudios, las redes y los problemas que encuentre serán cada vez más complejos. En tales situaciones, la única forma eficaz de descartar y resolver problemas es aplicar un enfoque metódico como el que se usa en esta actividad.

Parte 1: Verificar el registro de la red y descartar problemas

En la parte 1 de esta actividad, completará la documentación y realizará pruebas de conectividad para detectar problemas. Además, determinará la solución adecuada y la implementará en la parte 2.

Paso 1: Verificar el registro de la red y descartar cualquier problema

a. Para que pueda probar una red con eficacia, debe contar con la documentación completa. Observe que falta determinada información en la **tabla de direccionamiento**. Complete la **tabla de direccionamiento** con la información de gateway predeterminado que falta para los switches y las PC.

b. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local está en funcionamiento.

   Un plan de verificación puede ser tan simple como una lista de pruebas de conectividad. Use las siguientes pruebas para verificar la conectividad local y descartar cualquier problema de acceso. El primer problema ya se documentó, pero debe implementar y verificar la solución durante la parte 2.

Documentación de prueba y verificación

Prueba	¿Se realizó correctamente?	Problemas	Solución	Verificado
PC1 a PC2	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	
PC1 a S1				
PC1 a R1				

Nota: esta tabla es un ejemplo; debe crear su propio documento. Puede usar lápiz y papel para dibujar una tabla, o puede utilizar un editor de texto o una hoja de cálculo. Consulte al instructor si necesita más orientación.

c. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y documente cualquier problema. Esto se conoce frecuentemente como *conectividad de extremo a extremo*. Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad total.

Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

Paso 2: Determinar cuál es la solución adecuada para el problema

a. Con sus conocimientos sobre la forma en que operan las redes y sus aptitudes para configurar dispositivos, busque la causa del problema. Por ejemplo, el S1 no es la causa del problema de conectividad entre la PC1 y la PC2. Las luces de enlace son de color verde, y ninguna configuración en el S1 provocaría que no pase el tráfico entre la PC1 y la PC2. Por lo tanto, el problema debe de estar en la PC1, en la PC2 o en ambas.

b. Verifique el direccionamiento del dispositivo para asegurarse de que coincida con el registro de la red. Por ejemplo, la dirección IP para la PC1 es incorrecta, como se verificó con el comando **ipconfig**.

c. Sugiera una solución con la que usted crea que se resolverá el problema y documéntela. Por ejemplo, cambiar la dirección IP de la PC1 para que coincida con la documentación.

Nota: por lo general, hay más de una solución. Sin embargo, una práctica recomendada de resolución de problemas es implementar de a una solución por vez. Implementar más de una solución podría presentar problemas adicionales en una situación más compleja.

Parte 2: Implementar, verificar y documentar las soluciones

En la parte 2 de esta actividad, implementará las soluciones que identificó en la parte 1. Luego, verificará si la solución funcionó. Es posible que deba volver a la parte 1 para terminar de descartar todos los problemas.

Paso 1: Implementar soluciones para abordar los problemas de conectividad

Consulte la documentación en la parte 1. Elija el primer problema e implemente la solución que sugirió. Por ejemplo, corrija la dirección IP en la PC1.

Paso 2: Verificar si ahora el problema está resuelto

a. Verifique si la solución que propuso solucionó el problema realizando la prueba que usó para identificarlo. Por ejemplo, ¿la PC1 puede ahora hacer ping a la PC2?

b. Si el problema se resolvió, indíquelo en la documentación. Por ejemplo, en la tabla anterior, con colocar una simple marca de verificación en la columna “Verificado” sería suficiente.

Paso 3: Verificar si se resolvieron todos los problemas

a. Si todavía tiene un problema pendiente con una solución que aún no se implementó, vuelva al paso 1 de la parte 2.

b. Si se solucionaron todos los problemas actuales, ¿también solucionó todos los problemas de conectividad remota (por ejemplo, que la PC1 pueda hacer ping a la PC4)? Si la respuesta es negativa, vuelva al paso 1c de la parte 1 para probar la conectividad remota.

Problemas

- La PC1 no puede hacer ping a la PC2, porque la PC1 tiene una dirección IP que no pertenece a la red a la que está conectada.
- Los dispositivos no pueden hacer ping al S2, y el S2 no puede hacer ping a ningún dispositivo porque le falta una dirección IP.
- Los dispositivos remotos no pueden hacer ping a la PC4, porque la PC4 tiene configurado un gateway predeterminado incorrecto.
- Los dispositivos remotos no pueden hacer ping al S1, porque le falta la configuración de gateway predeterminado.

Tabla de calificación sugerida

Tarea	Posibles puntos	Puntos obtenidos
Completar el registro de la red	**20**	
Documentar los problemas y las soluciones	**45**	
Puntuación de Packet Tracer (problemas resueltos)	**35**	
Puntuación total	**100**	

Packet Tracer: Reto de habilidades de integración

(Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0	[[R1G0Add]]	255.255.255.0	No aplicable
	G0/1	[[R1G1Add]]	255.255.255.0	No aplicable
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0	[[R1G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0	[[R1G0Add]]
[[PC3Name]]	NIC	[[PC3Add]]	255.255.255.0	[[R1G1Add]]
[[PC4Name]]	NIC	[[PC4Add]]	255.255.255.0	[[R1G1Add]]

Objetivos

- Terminar el registro de la red.
- Realizar la configuración básica de dispositivos en un router y un switch.
- Verificar la conectividad y resolver cualquier problema.

Situación

La administradora de la red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración básica de un router y un switch utilizando Cisco IOS. Luego, verificará la configuración realizada por usted, así como la configuración de los dispositivos existentes, probando la conectividad de extremo a extremo.

Nota: después de completar esta actividad, puede elegir hacer clic en el botón **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Entre los aspectos variables se incluyen los nombres de dispositivo, los esquemas de direccionamiento IP y la topología.

Requisitos

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre **[[R1Name]]** al router y **[[S2Name]]** al segundo switch. No podrá acceder a **[[S1Name]]**.
- Utilice **cisco** como contraseña de EXEC del usuario para todas las líneas.

- Utilice **class** como contraseña de EXEC privilegiado.
- Encripte todas las contraseñas de texto no cifrado.
- Configure un aviso apropiado.
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **[[S2Name]]**.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
- Resuelva cualquier problema y regístrelo.
- Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo.

Nota: haga clic en el botón **Check Results** (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón **Reset Activity** para generar un nuevo conjunto de requisitos.

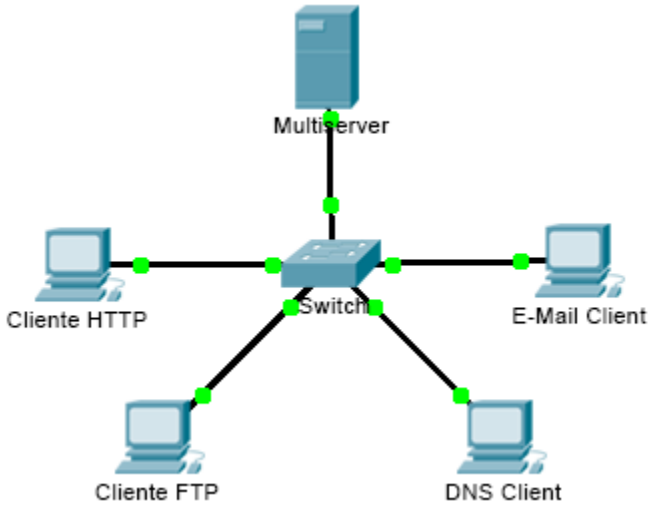
ID: [[indexNames]][[indexAdds]][[indexTopos]]

Esta actividad está configurada con un error que el estudiante deberá corregir para obtener la mayor puntuación. La dirección IP en [[PC4Name]] está en la subred incorrecta y no coincide con la dirección IP en la tabla de direccionamiento. Las respuestas correctas dependen de la situación que el alumno recibió para trabajar. La contraseña para acceder al asistente de la actividad es **PT_ccna5**.

Simulación de Packet Tracer: Comunicaciones TCP y UDP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Generar tráfico de red en modo de simulación

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Información básica

El objetivo de esta actividad de simulación es proporcionar una base para comprender en detalle los protocolos TCP y UDP. El modo de simulación permite ver la funcionalidad de los diferentes protocolos.

A medida que los datos se trasladan por la red, se dividen en partes más pequeñas y se identifican de forma tal que se puedan volver a juntar. A cada una de estas partes se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data unit]) y se la asocia a una capa específica. El modo de simulación de Packet Tracer le permite al usuario ver cada uno de los protocolos y las PDU asociadas. Los pasos que se detallan a continuación guían al usuario en el proceso de solicitud de servicios mediante diversas aplicaciones disponibles en una PC cliente.

Esta actividad proporciona la oportunidad de explorar la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función que cumplen los números de puerto para determinar qué aplicación local solicita o envía los datos.

Parte 1: Generar tráfico de red en modo de simulación

Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

Para reducir la cantidad de tráfico de red que se ve en la simulación, realice lo siguiente:

a. Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ping 192.168.1.255**. Esto toma unos segundos, ya que todos los dispositivos en la red responden a **MultiServer**.

c. Cierre la ventana de **MultiServer**.

Paso 2: Genere tráfico web (HTTP).

a. Cambie a modo de simulación.

b. Haga clic en **HTTP Client** (Cliente HTTP) y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Explorador Web).

c. En el campo de dirección URL, introduzca **192.168.1.254** y haga clic en **Go** (Ir). En la ventana de simulación, aparecerán sobres (PDU).

d. Minimice (pero no cierre) la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP

a. Haga clic en **FTP Client** (Cliente FTP) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

b. Introduzca el comando **ftp 192.168.1.254**. En la ventana de simulación, aparecerán PDU.

c. Minimice (pero no cierre) la ventana de configuración de **FTP Client**.

Paso 4: Generar tráfico DNS

a. Haga clic en **DNS Client** (Cliente DNS) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

b. Introduzca el comando **nslookup multiserver.pt.ptu**. En la ventana de simulación, aparecerá una PDU.

c. Minimice (pero no cierre) la ventana de configuración de **DNS Client**.

Paso 5: Generar tráfico de correo electrónico

a. Haga clic en **E-Mail Client** (Cliente de correo electrónico) y, a continuación, haga clic en la ficha **Desktop** y seleccione la herramienta **E Mail** (Correo electrónico).

b. Haga clic en **Compose** (Redactar) e introduzca la siguiente información:

1) **To:** (Para:) usuario@multiserver.pt.ptu.

2) **Subject:** (Asunto:) personalice el campo de asunto.

3) **E-Mail Body:** (Cuerpo del correo electrónico:) personalice el correo electrónico.

c. Haga clic en **Send** (Enviar).

d. Minimice (pero no cierre) la ventana de configuración de **E-Mail Client**.

Paso 6: Verifique que se haya generado tráfico y que esté preparado para la simulación.

Cada equipo cliente debe tener PDU enumeradas en el panel de simulación.

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Paso 1: Examinar la multiplexación a medida que el tráfico cruza la red

Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

a. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.

b. Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?

Están almacenadas en el switch.

c. Haga clic en **Capture/Forward** seis veces. Todos los clientes deberían haber recibido una respuesta. Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado. ¿Cómo se denomina este proceso?

Multiplexación.

d. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?

Representan diferentes protocolos.

e. Haga clic en **Back** ocho veces. Esto restablecerá la simulación.

NOTA: no haga clic en **Reset Simulation** (Restablecer simulación) en ningún momento durante esta actividad; si lo hace, deberá repetir los pasos de la parte 1.

Paso 2: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor

a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**:

1) Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrar todos/ninguno).

2) Seleccione **HTTP** y **TCP**. Haga clic en cualquier lugar fuera del cuadro Edit Filters (Editar filtros) para ocultarlo. En Visible Events (Eventos visibles), ahora solo se deberían mostrar las PDU de **HTTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en **HTTP Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

TCP

¿Estas comunicaciones se consideran confiables?

Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025 (puede ser diferente), 80, 0, 0 SYN

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **HTTP Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

80, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1. SYN cambió por SYN+ACK.

g. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación HTTP. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).

h. ¿Qué información se indica ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?

1025, 80, 1, 1. PSH+ACK: los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de acuse de recibo son 1.

i. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 3: Examine el tráfico FTP cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **FTP Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

TCP

¿Estas comunicaciones se consideran confiables?

Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025, 21, 0, 0. SYN

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

21, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

1025, 21, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

h. Cierre la PDU y haga clic en **Capture/Forward** hasta que una segunda PDU vuelva a **FTP Client**. La PDU es de un color diferente.

i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?

Puede decir “Username ok, need password” (Nombre de usuario correcto, se necesita contraseña) o “Welcome to PT Ftp server” (Bienvenido al servidor FTP de PT).

j. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 4: Examine el tráfico DNS cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS** y **UDP**.

b. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

UDP

¿Estas comunicaciones se consideran confiables?

No

d. Registre los valores de **SRC PORT** (Puerto de origen) y **DEST PORT** (Puerto de destino). ¿Por qué no hay números de secuencia ni de acuse de recibo?

1025, 53. Porque UDP no necesita establecer una conexión confiable.

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

53, 1025. Los puertos de origen y destino están invertidos.

g. ¿Cómo se llama la última sección de la **PDU**?

DNS ANSWER (Respuesta DNS)

h. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 5: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **E-mail Client**. Haga clic en el sobre de PDU para abrirlo.

c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico?

TCP

¿Estas comunicaciones se consideran confiables?

Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025, 25, 0, 0. SYN

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva a **E-Mail Client** con una marca de verificación.

f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

25, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

1025, 25, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1. ACK

h. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).

i. ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos **PDU** anteriores?

1025, 25, 1, 1. PSH+ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

j. ¿Qué protocolo de correo electrónico se relaciona con el puerto TCP 25? ¿Qué protocolo se relaciona con el puerto TCP 110?

SMTP. POP3.

k. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 6: Examinar el uso de números de puerto del servidor

a. Para ver las sesiones TCP activas, siga estos pasos en una secuencia rápida:

   1) Pase nuevamente al modo **Realtime** (Tiempo real).

   2) Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **netstat**. ¿Qué protocolos se indican en la columna izquierda? TCP

   ¿Qué números de puerto utiliza el servidor? Las respuestas varían, pero los estudiantes pueden ver los tres: 21, 25 y 80. Definitivamente deben ver el puerto 21.

c. ¿En qué estados están las sesiones?

   La respuesta varía. Entre los posibles estados se incluyen CLOSED (Cerrada), ESTABLISHED (Establecida), LAST_ACK (Último acuse de recibo).

d. Repita el comando **netstat** varias veces hasta que vea solo una sola sesión con el estado ESTABLISHED. ¿Para qué servicio aún está abierta la conexión? FTP

   ¿Por qué esta sesión no se cierra como las otras tres? (Sugerencia: revise los clientes minimizados)

   El servidor está esperando una contraseña del cliente.

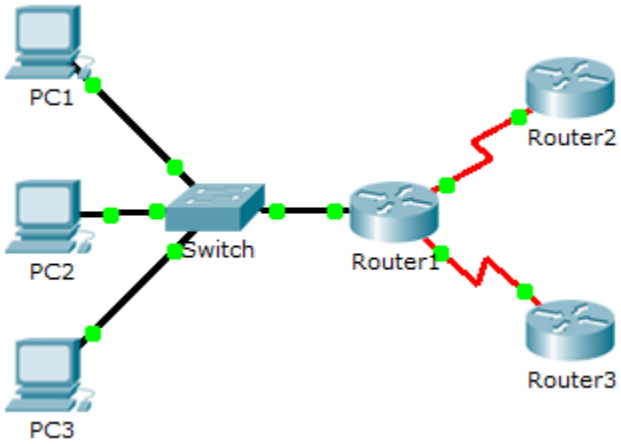
Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP	Paso 1	15	
	Paso 2	15	
	Paso 3	15	
	Paso 4	15	
	Paso 5	15	
	Paso 6	25	
Puntuación total		**100**	

Packet Tracer: Investigación del tráfico unicast, broadcast y multicast (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Generar tráfico de unicast

Parte 2: Generar tráfico de broadcast

Parte 3: Investigar el tráfico de multicast

Información básica/situación

En esta actividad, se examina el comportamiento de unicast, broadcast y multicast. La mayoría del tráfico de una red es unicast. Cuando una PC envía una solicitud de eco ICMP a un router remoto, la dirección de origen en el encabezado del paquete IP es la dirección IP de la PC emisora. La dirección de destino en el encabezado del paquete IP es la dirección IP de la interfaz del router remoto. El paquete se envía sólo al destino deseado.

Mediante el comando **ping** o la característica Add Complex PDU (Agregar PDU compleja) de Packet Tracer, puede hacer ping directamente a las direcciones de broadcast para ver el tráfico de broadcast.

Para el tráfico de multicast, consultará el tráfico de EIGRP. Los routers Cisco utilizan EIGRP para intercambiar información de enrutamiento entre routers. Los routers que utilizan EIGRP envían paquetes a la dirección multicast 224.0.0.10, que representa el grupo de routers EIGRP. Si bien estos paquetes son recibidos por otros dispositivos, todos los dispositivos (excepto los routers EIGRP) los descartan en la capa 3, sin requerir otro procesamiento.

Parte 1: Generar tráfico de unicast

Paso 1: Utilizar el comando ping para generar tráfico

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ping 10.0.3.2**. El ping debe tener éxito.

Paso 2: Ingrese al modo de simulación.

a. Haga clic en la ficha **Simulation** (Simulación) para ingresar al modo de simulación.

b. Haga clic en **Edit Filters** (Editar filtros) y verifique que solo los eventos ICMP y EIGRP estén seleccionados.

c. Haga clic en **PC1** e introduzca el comando **ping 10.0.3.2**.

Paso 3: Examinar el tráfico de unicast

La PDU en la **PC1** es una solicitud de eco de ICMP dirigida a la interfaz serial en el **Router3**.

a. Haga clic en **Capture/Forward** (Capturar/avanzar) varias veces y observe mientras se envía la solicitud de eco al **Router3** y la respuesta de eco se envía a la **PC1**. Deténgase cuando la primera respuesta de eco llegue a la PC1.

¿Qué dispositivos atravesó el paquete con la transmisión de unicast?

De la PC1 al Switch1, después al Router1 y, finalmente, al Router3, y viceversa.

b. En la sección Simulation Panel Event List (Lista de eventos del panel de simulación), la última columna incluye un cuadro de color que proporciona acceso a información detallada sobre un evento. Haga clic en el cuadro de color de la última columna para obtener el primer evento. Se abre la ventana PDU Information (Información de PDU).

¿En qué capa comienza esta transmisión y por qué?

En la capa 3, porque está específicamente relacionada con IP e ICMP.

c. Examine la información de la Capa 3 para todos los eventos. Observe que las direcciones IP de origen y de destino son direcciones unicast que hacen referencia a la PC1 y a la interfaz serial del Router3.

¿Cuáles son los dos cambios que ocurren en la capa 3 cuando un paquete llega al Router3?

Las direcciones IP de origen y destino se intercambian, y el tipo de mensaje ICMP ahora es 0.

d. Haga clic en **Reset Simulation** (Restablecer simulación).

Parte 2: Generar tráfico de broadcast

Paso 1: Agregar una PDU compleja

a. Haga clic en **Add Complex PDU** (Agregar una PDU compleja). Este ícono se ubica en la barra de herramientas de la derecha y muestra un sobre abierto.

b. Pase el cursor del mouse sobre la topología, y el puntero cambiará por un sobre con un signo más (+).

c. Haga clic en **PC1** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de diálogo **Create Complex PDU** (Crear una PDU compleja). Introduzca los siguientes valores:

- Dirección IP de destino: **255.255.255.255** (dirección de broadcast)
- Número de secuencia: 1
- Tiempo de intento único: **0**

Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP y OTHER.

d. Haga clic en **Create PDU** (Crear PDU). Este paquete de broadcast de prueba ahora aparece en **Simulation Panel Event List** .También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para la Situación 0.

e. Haga clic en **Capture/Forward** dos veces. Este paquete se envía al switch y después se transmite por broadcast a la **PC2**, la **PC3**, y el **Router1**. Examine la información de la Capa 3 para todos los eventos. Observe que la dirección IP de destino es 255.255.255.255, que es la dirección IP de broadcast que configuró cuando creó la PDU compleja.

Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

La PDU se convierte en un unicast que contesta a la PC1.

f. Haga clic en **Capture/Forward** nuevamente. ¿La PDU de broadcast se reenvía en algún momento al Router2 o al Router3? ¿Por qué?

No. El broadcast limitado debe permanecer dentro de la red local, a menos que el router esté establecido para reenviar.

g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en **Delete** (Eliminar) debajo de **Scenario 0** (Situación 0).

Parte 3: Investigar el tráfico de multicast

Paso 1: Examinar el tráfico que generan los protocolos de enrutamiento

a. Haga clic en **Capture/Forward** (Capturar/avanzar). Los paquetes EIGRP están en el Router1 a la espera de que se los transmita por multicast a través de cada interfaz.

b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en **Capture/Forward**. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes a las PC.

c. Haga clic en **Capture/Forward** hasta que vea que el paquete EIGRP llega a las PC.

¿Qué hacen los hosts con los paquetes?

Los hosts rechazan y descartan los paquetes.

Examine la información de las capas 3 y 4 para todos los eventos EIGRP.

¿Cuál es la dirección de destino de cada uno de los paquetes?

224.0.0.10, la dirección IP de multicast para el protocolo de enrutamiento EIGRP.

d. Haga clic en uno de los paquetes entregados a una de las PC. ¿Qué sucede con esos paquetes?

Los paquetes se descartan y no se realiza ningún procesamiento adicional.

Según el tráfico que generan los tres tipos de paquetes IP, ¿cuáles son las principales diferencias en la entrega?

El paquete unicast atraviesa la red destinado a un dispositivo específico, el broadcast se envía a cada dispositivo en la red de área local y el multicast se envía a todos los dispositivos, pero solo lo procesan aquellos que forman parte del grupo multicast.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Tráfico de unicast	Paso 3a	10	
	Paso 3b	10	
	Paso 3c	10	
Total de la parte 1		**30**	
Parte 2: Tráfico de broadcast	Paso 1c	10	
	Paso 1e	10	
	Paso 1f	10	
Total de la parte 2		**30**	
Parte 3: Tráfico de multicast	Paso 1c, p1	10	
	Paso 1c, p2	10	
	Paso 1d, p1	10	
	Paso 1d, p2	10	
Total de la parte 3		**40**	
Puntuación total		**100**	

Packet Tracer: Configuración de direccionamiento IPv6

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

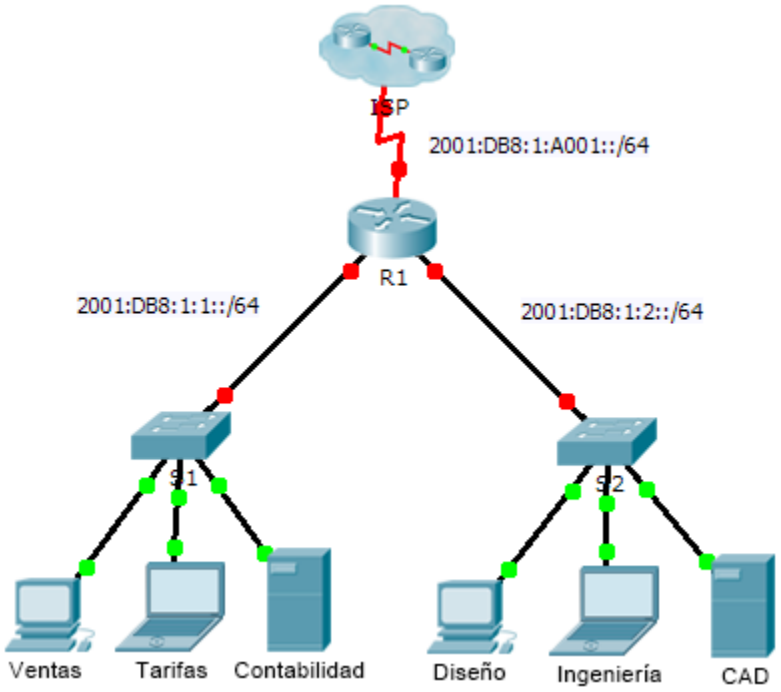


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:1:1::1/64	No aplicable
	G0/1	2001:DB8:1:2::1/64	No aplicable
	S0/0/0	2001:DB8:1:A001::2/64	No aplicable
	Link-local	FE80::1	No aplicable
Ventas	NIC	2001:DB8:1:1::2/64	FE80::1
Tarifas	NIC	2001:DB8:1:1::3/64	FE80::1
Contabilidad	NIC	2001:DB8:1:1::4/64	FE80::1
Diseño	NIC	2001:DB8:1:2::2/64	FE80::1
Ingeniería	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objetivos

Parte 1: Configurar el direccionamiento IPv6 en el router

Parte 2: Configurar el direccionamiento IPv6 en los servidores

Parte 3: Configurar el direccionamiento IPv6 en los clientes

Parte 4: Probar y verificar la conectividad de red

Información básica

En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación de las direcciones IPv6.

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

a. Introduzca el comando de configuración global ipv6 unicast-routing. Este comando se debe configurar para habilitar el router para que reenvíe paquetes IPv6. Este comando se analizará en otro semestre.

```
R1(config)# ipv6 unicast-routing
```

Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

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

b. Ingrese al modo EXEC privilegiado.

c. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/0.

d. Configure la dirección IPv6 con el siguiente comando:

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

e. Configure la dirección IPv6 link-local con el siguiente comando:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

f. Active la interfaz.

Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/1.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.

c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Paso 4: Configurar el direccionamiento IPv6 en Serial0/0/0

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para Serial0/0/0.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.

c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Parte 2: Configurar el direccionamiento IPv6 en los servidores

Paso 1: Configurar el direccionamiento IPv6 en el servidor de contabilidad

a. Haga clic en **Accounting** (Contabilidad) y, a continuación, en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

b. Establezca la **dirección IPv6 2001:DB8:1:1::4** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

Paso 2: Configurar el direccionamiento IPv6 en el servidor CAD

Repita los pasos 1a a 1c para el servidor **CAD**. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Parte 3: Configurar el direccionamiento IPv6 en los clientes

Paso 1: Configurar el direccionamiento IPv6 en los clientes de ventas y facturación

a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:1::3** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

d. Repita los pasos 1a a 1c para **Sales** (Ventas). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:2::3** con el prefijo **/64**.

c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

d. Repita los pasos 1a a 1c para **Design** (Diseño). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

Parte 4: Probar y verificar la conectividad de la red

Paso 1: Abrir las páginas Web del servidor de los clientes

a. Haga clic en **Sales** y, a continuación, en la ficha **Desktop**. Si es necesario, cierre la ventana **IP Configuration**.

b. Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.

c. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.

d. Repita los pasos 1a a 1d para el resto de los clientes.

Paso 2: Hacer ping al ISP

a. Abra una ventana de configuración de cualquier equipo cliente haciendo clic en el ícono.

b. Haga clic en la ficha **Desktop** > **Command Prompt** (Símbolo del sistema).

c. Pruebe la conectividad al ISP con el siguiente comando:

```
PC> ping 2001:DB8:1:A001::1
```

d. Repita el comando **ping** con otros clientes hasta que se haya verificado la conectividad completa.

Packet Tracer: Verificación del direccionamiento IPv4 e IPv6 (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

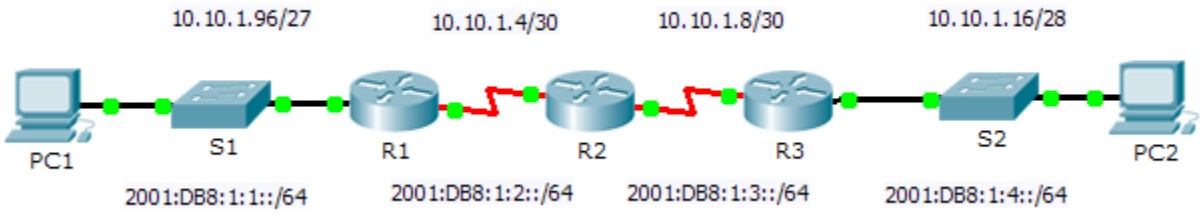


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.1.97	255.255.255.224	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
	Link-local	FE80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
	Link-local	FE80::2		No aplicable
R3	G0/0	10.10.1.17	255.255.255.240	No aplicable
		2001:DB8:1:4::1/64		No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
	Link-local	FE80::3		No aplicable
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
		2001:DB8:1:1::A/64		FE80::1
PC2	NIC	10.10.1.20	255.255.255.240	10.10.1.17
		2001:DB8:1:4::A/64		FE80::3

Objetivos

Parte 1: Completar la documentación de la tabla de direccionamiento

Parte 2: Probar la conectividad mediante el comando ping

Parte 3: Descubrir la ruta mediante su rastreo

Información básica

La técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. En esta actividad, investigará la implementación de una técnica dual-stack incluidos la documentación de la configuración de IPv4 e IPv6 para dispositivos finales, la prueba de conectividad para IPv4 e IPv6 mediante el comando **ping** y el rastreo de la ruta de extremo a extremo para IPv4 e IPv6.

Parte 1: Completar la documentación de la tabla de direccionamiento

Paso 1: Usar el comando ipconfig para verificar el direccionamiento IPv4

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

c. Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

Paso 2: Usar el comando ipv6config para verificar el direccionamiento IPv6

a. En la **PC1**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

b. En la **PC2**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

Parte 2: Probar la conectividad mediante el comando ping

Paso 1: Usar el comando ping para verificar la conectividad IPv4

a. Desde la **PC1**, haga ping a la dirección IPv4 de la **PC2**. ¿El resultado fue satisfactorio? Sí

b. Desde la **PC2**, haga ping a la dirección IPv4 de la **PC1**. ¿El resultado fue satisfactorio? Sí

Paso 2: Usar el comando ping para verificar la conectividad IPv6

a. Desde la **PC1**, haga ping a la dirección IPv6 de la **PC2**. ¿El resultado fue satisfactorio? Sí

b. Desde la **PC2**, haga ping a la dirección IPv6 de la **PC1**. ¿El resultado fue satisfactorio? Sí

Parte 3: Descubrir la ruta mediante su rastreo

Paso 1: Usar el comando tracert para descubrir la ruta IPv4

a. Desde la **PC1**, rastree la ruta a la **PC2**.

```
PC> tracert 10.10.1.20
```

¿Qué direcciones se encontraron a lo largo de la ruta? 10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20

¿Con qué interfaces se asocian las cuatro direcciones? G0/0 del R1, S0/0/0 en el R2, S0/0/01 en el R3, NIC de la PC2

b. Desde la **PC2**, rastree la ruta a la **PC1**.

¿Qué direcciones se encontraron a lo largo de la ruta? 10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100

¿Con qué interfaces se asocian las cuatro direcciones? G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1

Paso 2: Usar el comando tracert para descubrir la ruta IPv6

a. Desde la **PC1**, rastree la ruta a la dirección IPv6 de la **PC2**.

```
PC> tracert 2001:DB8:1:4::A
```

¿Qué direcciones se encontraron a lo largo de la ruta? 2001:DB8:1:1::1, 2001:DB8:1:2::1, 2001:DB8:1:3::2, 2001:DB8:1:4::A

¿Con qué interfaces se asocian las cuatro direcciones? G0/0 del R1, S0/0/0 del R2, S0/0/1 del R3, NIC de la PC2

b. Desde la **PC2**, rastree la ruta a la dirección IPv6 de la **PC1**.

¿Qué direcciones se encontraron a lo largo de la ruta? 2001:DB8:1:4::1, 2001:DB8:1:3::1, 2001:DB8:1:2::2, 2001:DB8:1:1::A

¿Con qué interfaces se asocian las cuatro direcciones? Ga0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Completar la documentación de la tabla de direccionamiento	Paso 1b	10	
	Paso 1d	10	
	Paso 2a	10	
	Paso 2b	10	
Total de la parte 1		**40**	
Parte 2: Probar la conectividad mediante el comando ping	Paso 1a	7	
	Paso 1b	7	
	Paso 2a	7	
	Paso 2b	7	
Total de la parte 2		**28**	
Parte 3: Descubrir la ruta mediante su rastreo	Paso 1a	8	
	Paso 1b	8	
	Paso 2a	8	
	Paso 2b	8	
Total de la parte 3		**32**	
Puntuación total		**100**	

Packet Tracer: Ping y rastreo para probar rutas

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

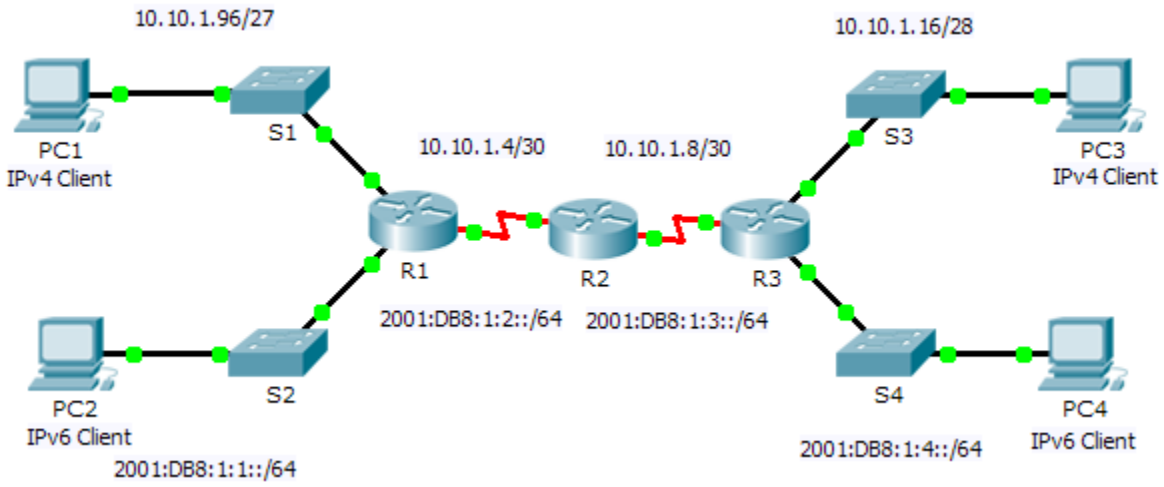


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	2001:DB8:1:1::1/64		No aplicable
	G0/1	10.10.1.97	255.255.255.224	No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
	Link-local	FE80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
	Link-local	FE80::2		No aplicable
R3	G0/0	2001:DB8:1:4::1/64		No aplicable
	G0/1	10.10.1.17	255.255.255.240	No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
	Link-local	FE80::3		No aplicable
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:DB8:1:1::2/64		FE80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:DB8:1:4::2/64		FE80::1

Objetivos

Parte 1: Probar y restaurar la conectividad IPv4

Parte 2: Probar y restaurar la conectividad IPv6

Situación

En esta actividad, hay problemas de conectividad. Además de recopilar y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad.

Nota: la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

Parte 1: Probar y restaurar la conectividad IPv4

Paso 1: Usar los comandos ipconfig y ping para verificar la conectividad

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

c. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

e. Pruebe la conectividad entre la **PC1** y la **PC3**. El ping debe fallar.

Paso 2: Localice el origen de la falla de conectividad.

a. Desde la **PC1**, introduzca el comando necesario para rastrear la ruta a la **PC3**. ¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.97

b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

c. Desde la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**. ¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.17

d. Introduzca **Ctrl**+**C** para detener el rastreo.

e. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **ENTRAR** e inicie sesión en el router.

f. Introduzca el comando **show ip interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv4 en el router. Una se debió haber registrado en el paso 2a. ¿Cuál es la otra? 10.10.1.6

g. Introduzca el comando **show ip route** para obtener una lista de las redes a las que está conectado el router. Observe que hay dos redes conectadas a la interfaz **Serial0/0/1**. ¿Cuáles son? 10.10.1.6/32, 10.10.1.4/30

h. Repita los pasos 2e a 2g con el **R3** y escriba las respuestas aquí. 10.10.1.10, 10.10.1.8/30, 10.10.1.10/32

Observe cómo cambia la interfaz serial para el R3.

i. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error? La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.

b. ¿Qué solución propondría para corregir el problema? Configurar la dirección IP correcta en la interfaz Serial 0/0/0 del R2 (10.10.1.5).

Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada.

a. Desde la **PC1**, pruebe la conectividad a la **PC3**.

b. Desde la **PC3**, pruebe la conectividad a la **PC1**. ¿Se resolvió el problema? Sí

Paso 6: Documentar la solución.

Parte 2: Probar y restaurar la conectividad IPv6

Paso 1: Usar los comandos ipv6config y ping para verificar la conectividad

a. Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

b. Introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

c. Haga clic en **PC4** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

d. Introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

e. Pruebe la conectividad entre la **PC2** y la **PC4**. El ping debe fallar.

Paso 2: Localice el origen de la falla de conectividad.

a. Desde la **PC2**, introduzca el comando necesario para rastrear la ruta a la **PC4**. ¿Cuál es la última dirección IPv6 correcta que se alcanzó? 2001:DB8:1:3::2

b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

c. Desde la **PC4**, introduzca el comando necesario para rastrear la ruta a la **PC2**. ¿Cuál es la última dirección IPv6 correcta que se alcanzó? No se alcanzó ninguna dirección IPv6.

d. Introduzca **Ctrl**+**C** para detener el rastreo.

e. Haga clic en **R3** y, a continuación, haga clic en la ficha **CLI**. Presione **ENTRAR** e inicie sesión en el router.

f. Introduzca el comando **show ipv6 interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv6 en el router. Una debe coincidir con la dirección de gateway registrada en el paso 1d. ¿Hay alguna discrepancia? Sí

g. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error? La PC4 utiliza una configuración de gateway predeterminado incorrecta.

b. ¿Qué solución propondría para corregir el problema? Configurar la PC4 con la dirección de gateway predeterminado correcta: FE80::3.

Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada.

a. Desde la **PC2**, pruebe la conectividad a la **PC4**.

b. Desde la **PC4**, pruebe la conectividad a la **PC2**. ¿Se resolvió el problema? Sí

Paso 6: Documentar la solución.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Probar y restaurar la conectividad entre la PC1 y la PC3	Paso 1b	5	
	Paso 1d	5	
	Paso 2a	5	
	Paso 2c	5	
	Paso 2f	5	
	Paso 2g	5	
	Paso 2h	5	
	Paso 3a	5	
	Paso 3b	5	
Total de la parte 1		**45**	
Parte 2: Probar y restaurar la conectividad entre la PC2 y la PC4	Paso 1b	5	
	Paso 1d	5	
	Paso 2a	5	
	Paso 2c	5	
	Paso 2f	5	
	Paso 3a	5	
	Paso 3b	5	
Total de la parte 2		**35**	
Puntuación de Packet Tracer		**20**	
Puntuación total		**100**	

Packet Tracer: Resolución de problemas de direccionamiento IPv4 e IPv6 (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

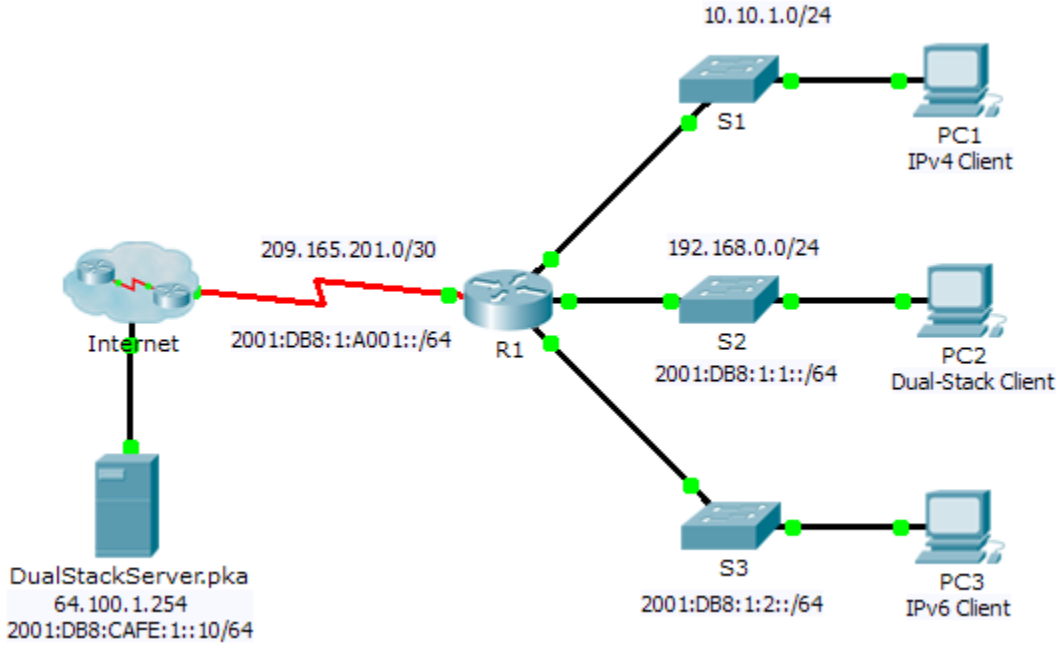


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.1.1	255.255.255.0	No aplicable
	Ga0/1	192.168.0.1	255.255.255.0	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	G0/2	2001:DB8:1:2::1/64		No aplicable
	S0/0/0	209.165.201.2	255.255.255.252	No aplicable
		2001:DB8:1:A001::2/64		No aplicable
	Link-local	FE80::1		No aplicable
Servidor dual-stack	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
		2001:DB8:1:1::2/64		FE80::1
PC3	NIC	2001:DB8:1:2::2/64		FE80::1

Objetivos

Parte 1: Resolver el primer problema

Parte 2: Resolver el segundo problema

Parte 3: Resolver el tercer problema

Situación

Usted es un técnico de red que trabaja para una compañía que decidió migrar de IPv4 a IPv6. Mientras tanto, debe admitir ambos protocolos (dual-stack). Tres compañeros de trabajo llamaron al soporte técnico para resolver algunos problemas, pero no recibieron suficiente asistencia. El soporte técnico le elevó el problema a usted, un técnico de soporte de nivel 2. Su trabajo es localizar el origen de los problemas e implementar las soluciones adecuadas.

Parte 1: Resolver el primer problema

Un cliente que usa la **PC1** se queja de que no puede acceder a la página Web **dualstackserver.pka**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC1	
Problema: No puede acceder a la página Web dualstackserver.pka.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IP cuando se utiliza **ipconfig**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando **ping**?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando **tracert**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el servidor mediante **nslookup**?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Considerar las causas probables de la falla

a. Observe las pruebas que se realizaron. De ser posible, analice con sus colegas técnicos de red (compañeros de curso) las situaciones que podrían ser la causa de este problema.

b. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

Haga una lista de factores que se podrían cambiar para solucionar este problema. Comience con la solución que tenga más posibilidades de funcionar.

Paso 4: Implemente el plan.

Pruebe la solución más probable de la lista. Si ya se probó, pase a la siguiente solución.

Paso 5: Verificar que la solución haya resuelto el problema

a. Repita las pruebas de la solicitud de soporte técnico. ¿Se solucionó el problema?

b. Si el problema persiste, revierta el cambio en caso de no estar seguro de que sea correcto y vuelva al paso 4.

Paso 6: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas. La dirección DNS IPv4 de la PC1 es incorrecta.

Parte 2: Resolver el segundo el problema

Un cliente que usa la PC2 se queja de que no puede acceder a los archivos ubicados en **DualStackServer.pka** en 2001:DB8:CAFE:1::10.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC2	
Problema: No puede acceder al servicio FTP de 2001:DB8:CAFE:1:10.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza **ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando **ping**?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando **tracert**?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas. La dirección de gateway IPv6 de DualStackServer.pka es incorrecta

Parte 3: Resolver el tercer problema

Un cliente que usa la **PC1** se queja de que no se puede comunicar con la **PC2**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del usuario por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC3	
Problema: No se puede comunicar con la PC2.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IP cuando se utiliza **ipconfig**?	Sí
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza **ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv4 mediante **ping**?	No
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv6 mediante **ping**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv4 mediante **tracert**?	No
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv6 mediante **tracert**?	Sí
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas. La dirección de gateway IPv4 de la PC2 es incorrecta.

Packet Tracer: Reto de habilidades de integración

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

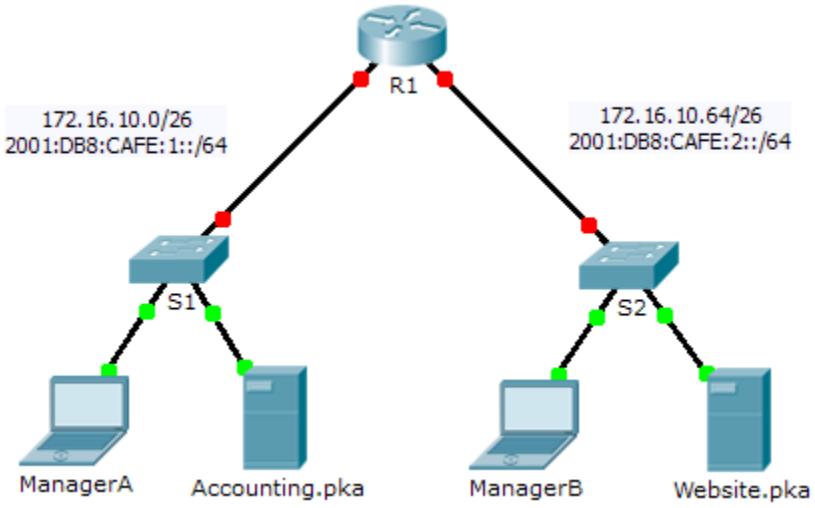


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	172.16.10.1	255.255.255.192	No aplicable
		2001:DB8:CAFE:1::1/64		No aplicable
	G0/1	172.16.10.65	255.255.255.192	No aplicable
		2001:DB8:CAFE:2::1/64		No aplicable
	Link-local	FE80::1		No aplicable
S1	VLAN1	172.16.10.62	255.255.255.192	172.16.10.1
S2	VLAN1	172.16.10.126	255.255.255.192	172.16.10.65
ManagerA	NIC	172.16.10.3	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::3/64		FE80::1
Accounting.pka	NIC	172.16.10.2	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::2/64		FE80::1
ManagerB	NIC	172.16.10.67	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::3/64		FE80::1
Website.pka	NIC	172.16.10.66	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::2/64		FE80::1

Situación

Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el resto del esquema de direccionamiento de acuerdo con la tabla de direccionamiento abreviada y verificar la conectividad.

Requisitos

- Complete el registro de la **tabla de direccionamiento**.
- Configure direccionamiento IPv4 e IPv6 en el **R1**.
- Configure direccionamiento IPv4 en el **S1**. El **S2** ya está configurado.
- Configure direccionamiento IPv4 e IPv6 en **ManagerA**. El resto de los clientes ya están configurados.
- Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios Web en **Accounting.pka** y **Website.pka**.

Tabla de calificación sugerida

Packet Tracer tienen una puntuación de 80 puntos. Completar la **tabla de direccionamiento** vale 20 puntos.

Packet Tracer: Situación de división en subredes 1

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

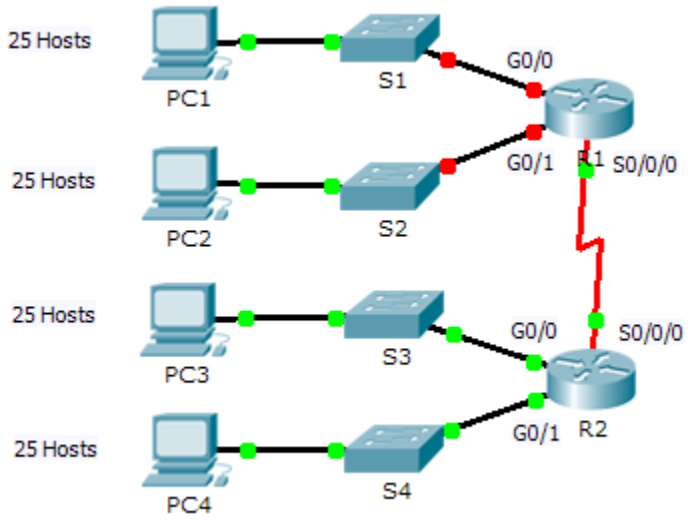


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.100.1	255.255.255.224	No aplicable
	G0/1	192.168.100.33	255.255.255.224	No aplicable
	S0/0/0	192.168.100.129	255.255.255.224	No aplicable
R2	G0/0	192.168.100.65	255.255.255.224	No aplicable
	G0/1	192.168.100.97	255.255.255.224	No aplicable
	S0/0/0	192.168.100.158	255.255.255.224	No aplicable
S1	VLAN 1	192.168.100.2	255.255.255.224	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.224	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.224	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.224	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.224	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.224	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.224	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.224	192.168.100.97

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 192.168.100.0/24 para que cree una subred y proporcione el direccionamiento IP para la red que se muestra en la topología. Cada LAN de la red necesita espacio suficiente para alojar, como mínimo, 25 direcciones para dispositivos finales, el switch y el router. La conexión entre las redes R1 y R2 requiere una dirección IP para cada extremo del enlace.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida en subredes la red 192.168.100.0/24 en la cantidad adecuada de subredes.

a. Según la topología, ¿cuántas subredes se necesitan? 5

b. ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología? 3

c. ¿Cuántas subredes se crean? 8

d. ¿Cuántos hosts utilizables se crean por subred? 30

Nota: si su respuesta es menor que los 25 hosts requeridos, tomó prestados demasiados bits.

e. Calcule el valor binario para las primeras cinco subredes. La primera subred ya se muestra.

```
Net 0: 192 . 168 . 100 .  0   0   0   0   0   0   0   0
```



```
Net 1: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 192 . 168 . 100 .  0   0   1   0   0   0   0   0

Net 2: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 192 . 168 . 100 .  0   1   0   0   0   0   0   0

Net 3: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 192 . 168 . 100 .  0   1   1   0   0   0   0   0

Net 4: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 192 . 168 . 100 .  1   0   0   0   0   0   0   0
```

f. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

```
11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1   1   1   0   0   0   0   0
   255  .   255  .   255  . ______
   255  .   255  .   255  .  224
```

g. Complete la **tabla de subredes** con el valor decimal de todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas.

Tabla de subredes

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255
8				
9				
10				

Paso 2: Asigne las subredes a la red que se muestra en la topología.

a. Asigne la subred 0 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R1: 192.168.100.0 /27

b. Asigne la subred 1 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R1: 192.168.100.32 /27

c. Asigne la subred 2 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R2: 192.168.100.64 /27

d. Asigne la subred 3 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R2: 192.168.100.96 /27

e. Asigne la subred 4 al enlace WAN entre el R1 y el R2: 192.168.100.128 /27

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

a. Asigne las primeras direcciones IP utilizables al R1 para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables al R2 para los enlaces LAN. Asigne la última dirección IP utilizable para el enlace WAN.

c. Asigne las segundas direcciones IP utilizables a los switches.

d. Asigne las últimas direcciones IP utilizables a los hosts.

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.

Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Diseñar un esquema de direccionamiento IP	Paso 1a	1	
	Paso 1b	1	
	Paso 1c	1	
	Paso 1d	1	
	Paso 1e	4	
	Paso 1f	2	
Completar la tabla de subredes	Paso 1g	10	
Asignar subredes	Paso 2	10	
Documentar el direccionamiento	Paso 3	40	
Total de la parte 1		**70**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

Packet Tracer: Situación de división en subredes 2

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

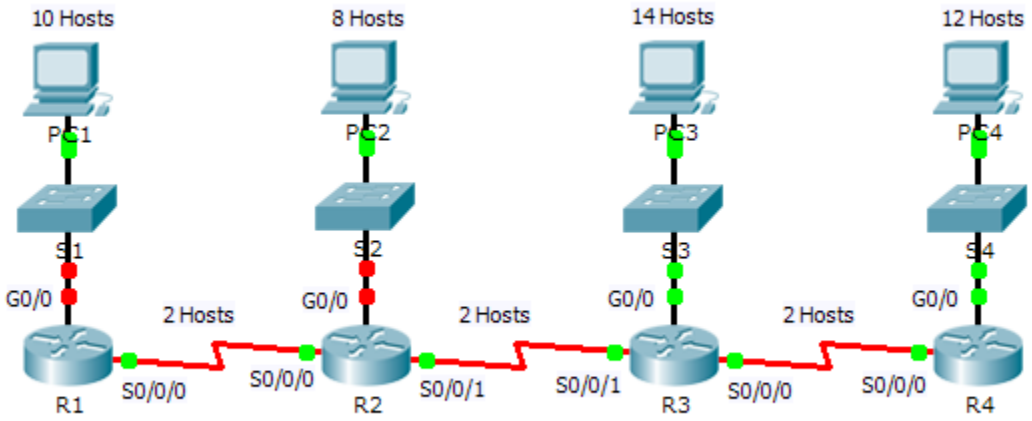


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.1.1	255.255.255.240	No aplicable
	S0/0/0	172.31.1.65	255.255.255.240	No aplicable
R2	G0/0	172.31.1.17	255.255.255.240	No aplicable
	S0/0/0	172.31.1.78	255.255.255.240	No aplicable
	S0/0/1	172.31.1.81	255.255.255.240	No aplicable
R3	G0/0	172.31.1.33	255.255.255.240	No aplicable
	S0/0/0	172.31.1.97	255.255.255.240	No aplicable
	S0/0/1	172.31.1.94	255.255.255.240	No aplicable
R4	G0/0	172.31.1.49	255.255.255.240	No aplicable
	S0/0/0	172.31.1.110	255.255.255.240	No aplicable
S1	VLAN 1	172.31.1.2	255.255.255.240	172.31.1.1
S2	VLAN 1	172.31.1.18	255.255.255.240	172.31.1.17
S3	VLAN 1	172.31.1.34	255.255.255.240	172.31.1.33
S4	VLAN 1	172.31.1.50	255.255.255.240	172.31.1.49
PC1	NIC	172.31.1.14	255.255.255.240	172.31.1.1
PC2	NIC	172.31.1.30	255.255.255.240	172.31.1.17
PC3	NIC	172.31.1.46	255.255.255.240	172.31.1.33
PC4	NIC	172.31.1.62	255.255.255.240	172.31.1.49

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 172.31.1.0 /24 para que la divida en subredes y proporcione direccionamiento IP para la red que se muestra en la topología. Las direcciones de host requeridas para cada enlace WAN y LAN se muestran en la topología.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida la red 172.31.1.0/24 en subredes de acuerdo con la cantidad máxima de hosts que requiere la subred más extensa.

a. Según la topología, ¿cuántas subredes se necesitan? 7

b. ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología? 4

c. ¿Cuántas subredes se crean? 16

d. ¿Cuántas direcciones de host utilizables se crean por subred? 14

Nota: si su respuesta es menor que el máximo de 14 hosts que requiere la LAN del R3, tomó prestados demasiados bits.

e. Calcule el valor binario para las primeras cinco subredes. La subred cero ya se muestra.

```
Net 0: 172 . 31 . 1 .  0   0   0   0   0   0   0   0

Net 1: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 172 . 31 . 1 .  0   0   0   1   0   0   0   0

Net 2: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 172 . 31 . 1 .  0   0   1   0   0   0   0   0

Net 3: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 172 . 31 . 1 .  0   0   1   1   0   0   0   0

Net 4: 172 . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 172 . 31 . 1 .  0   1   0   0   0   0   0   0
```

f. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

```
11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1   1   1   1   0   0   0   0
   255  .   255  .   255  . ______
   255  .   255  .   255  .  240
```

g. Complete la **tabla de subredes** con todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. La primera subred ya se completó. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas.

Tabla de subredes

Número de subred	IP de subred	Primera IP de host utilizable	Última IP de host utilizable	Dirección de broadcast
0	172.31.1.0	172.31.1.1	172.31.1.14	172.16.1.15
1	172.31.1.16	172.31.1.17	172.31.1.30	172.31.1.31
2	172.31.1.32	172.31.1.33	172.31.1.46	172.31.1.47
3	172.31.1.48	172.31.1.49	172.31.1.62	172.31.1.63
4	172.31.1.64	172.31.1.65	172.31.1.78	172.31.1.79
5	172.31.1.80	172.31.1.81	172.31.1.94	172.31.1.95
6	172.31.1.96	172.31.1.97	172.31.1.110	172.31.1.111
7	172.31.1.112	172.31.1.113	172.31.1.126	172.31.1.127
8	172.31.1.128	172.31.1.129	172.31.1.142	172.31.1.143
9	172.31.1.144	172.31.1.145	172.31.1.158	172.31.1.159
10	172.31.1.160	172.31.1.161	172.31.1.174	172.31.1.175
11	172.31.1.176	172.31.1.177	172.31.1.190	172.31.1.191
12	172.31.1.192	172.31.1.193	172.31.1.206	172.31.1.207
13	172.31.1.208	172.31.1.209	172.31.1.222	172.31.1.223
14	172.31.1.224	172.31.1.225	172.31.1.238	172.31.1.239
15	172.31.1.240	172.31.1.241	172.31.1.254	172.31.1.255

Paso 2: Asigne las subredes a la red que se muestra en la topología.

Cuando asigne las subredes, tenga en cuenta que es necesario el enrutamiento para permitir que la información se envíe a través de la red.

a. Asigne la subred 0 a la LAN del R1: 172.31.1.0 /28

b. Asigne la subred 1 a la LAN del R2: 172.31.1.16/28

c. Asigne la subred 2 a la LAN del R3: 172.31.1.32/28

d. Asigne la subred 3 a la LAN del R4: 172.31.1.48/28

e. Asigne la subred 4 al enlace entre el R1 y el R2: 172.31.1.64/28

f. Asigne la subred 5 al enlace entre el R2 y el R3: 172.31.1.80/28

g. Asigne la subred 6 al enlace entre el R3 y el R4: 172.31.1.96/28

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

a. Asigne las primeras direcciones IP utilizables a los routers para cada uno de los enlaces LAN.

b. Utilice el siguiente método para asignar las direcciones IP de los enlaces WAN:

- Para el enlace WAN entre el R1 y el R2, asigne la primera dirección IP utilizable al R1 y la última dirección IP utilizable al R2.
- Para el enlace WAN entre el R2 y el R3, asigne la primera dirección IP utilizable al R2 y la última dirección IP utilizable al R3.
- Para el enlace WAN entre el R3 y el R4, asigne la primera dirección IP utilizable al R3 y la última dirección IP utilizable al R4.

c. Asigne las segundas direcciones IP utilizables a los switches.

d. Asigne las últimas direcciones IP utilizables a los hosts.

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1 y el R2

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.

Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el R2, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Diseñar un esquema de direccionamiento IP	Paso 1a	1	
	Paso 1b	1	
	Paso 1c	1	
	Paso 1d	1	
	Paso 1e	4	
	Paso 1f	2	
Completar la tabla de subredes	Paso 1g	10	
Asignar subredes	Paso 2	10	
Documentar el direccionamiento	Paso 3	40	
Total de la parte 1		**70**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

Packet Tracer: Diseño e implementación de un esquema de direccionamiento VSLM (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0	[[R1G0Add]]	[[R1G0Sub]]	No aplicable
	G0/1	[[R1G1Add]]	[[R1G1Sub]]	No aplicable
	S0/0/0	[[R1S0Add]]	[[R1S0Sub]]	No aplicable
[[R2Name]]	G0/0	[[R2G0Add]]	[[R2G0Sub]]	No aplicable
	G0/1	[[R2G1Add]]	[[R2G1Sub]]	No aplicable
	S0/0/0	[[R2S0Add]]	[[R2S0Sub]]	No aplicable
[[S1Name]]	VLAN 1	[[S1Add]]	[[S1Sub]]	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	[[S2Sub]]	[[R1G1Add]]
[[S3Name]]	VLAN 1	[[S3Add]]	[[S3Sub]]	[[R2G0Add]]
[[S4Name]]	VLAN 1	[[S4Add]]	[[S4Sub]]	[[R2G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	[[PC1Sub]]	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	[[PC2Sub]]	[[R1G1Add]]
[[PC3Name]]	NIC	[[PC3Add]]	[[PC3Sub]]	[[R2G0Add]]
[[PC4Name]]	NIC	[[PC4Add]]	[[PC4Sub]]	[[R2G1Add]]

Objetivos

Parte 1: Examinar los requisitos de la red

Parte 2: Diseñar el esquema de direccionamiento VLSM

Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

Información básica

En esta actividad, se le proporciona una dirección de red /24 para diseñar un esquema de direccionamiento VLSM. Sobre la base de un conjunto de requisitos, asignará subredes y direccionamiento, configurará los dispositivos y verificará la conectividad.

Parte 1: Examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias

Dividirá la dirección de red [[DisplayNet]] en subredes. La red tiene los siguientes requisitos:

- La LAN de **[[S1Name]]** requerirá **[[HostReg1]]** direcciones IP de host.
- La LAN de **[[S2Name]]** requerirá **[[HostReg2]]** direcciones IP de host.
- La LAN de **[[S3Name]]** requerirá **[[HostReg3]]** direcciones IP de host.
- La LAN de **[[S4Name]]** requerirá **[[HostReg4]]** direcciones IP de host.

¿Cuántas subredes se necesitan en la topología de la red? 5

Paso 2: Determinar la información de máscara de subred para cada subred

a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S1Name]]**?

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S2Name]]**?

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S3Name]]**?

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S4Name]]**?

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para la conexión entre **[[R1Name]]** y **[[R2Name]]**?

Parte 2: Diseñar el esquema de direccionamiento VLSM

Paso 1: Dividir la red [[DisplayNet]] según la cantidad de hosts por subred

a. Use la primera subred para la LAN más extensa.

b. Use la segunda subred para la segunda LAN más extensa.

c. Use la tercera subred para la tercera LAN más extensa.

d. Use la cuarta subred para la cuarta LAN más extensa.

e. Use la quinta subred para admitir la conexión entre **[[R1Name]]** y **[[R2Name]]**.

Paso 2: Registrar las subredes VLSM

Complete la **tabla de subredes** con las descripciones de las subred (p. ej., LAN de [[S1Name]]), la cantidad de hosts necesarios, la dirección de red para la subred, la primera dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Tabla de subredes

Nota: las respuestas correctas para esta tabla varían según la situación recibida. Consulte las notas para el instructor que se encuentran al final de estas instrucciones para obtener más información. El formato que se usa aquí sigue el utilizado por el estudiante en **Diseño e implementación de un esquema de direccionamiento VLSM**.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Dirección de broadcast

Paso 3: Documente el esquema de direccionamiento.

a. Asigne las primeras direcciones IP utilizables a **[[R1Name]]** para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables a **[[R2Name]]** para los dos enlaces LAN. Asigne la última dirección IP utilizable para el enlace WAN.

c. Asigne las segundas direcciones IP utilizables a los switches.

d. Asigne las últimas direcciones IP utilizables a los hosts.

Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN de [[R1Name]]

Paso 2: Configurar el direccionamiento IP en [[S3Name]], incluido el gateway predeterminado

Paso 3: Configurar el direccionamiento IP en [[PC4Name]], incluido el gateway predeterminado

Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde [[R1Name]], [[S3Name]] y [[PC4Name]]. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar los requisitos de la red	Paso 1	1	
	Paso 2	4	
Total de la parte 1		**5**	
Parte 2: Diseñar el esquema de direccionamiento VLSM			
Completar la tabla de subredes		25	
Documentar el direccionamiento		40	
Total de la parte 2		**65**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

ID:[[indexAdds]][[indexNames]][[indexTopos]]

Notas para el instructor:

Las siguientes tablas de direccionamiento representan las tres situaciones de direccionamiento posibles que puede recibir el estudiante. Observe que la columna Dispositivo es independiente del esquema de direccionamiento. Por ejemplo, un estudiante podría recibir los nombres de dispositivos de la situación 1 y el esquema de direccionamiento de la situación 3. Además, las tres topologías posibles también son independientes de los nombres de los dispositivos y del esquema de direccionamiento (haga clic en Reset [Restablecer] en la actividad para ver las distintas topologías). Por lo tanto, en esta actividad se utilizan tres variables independientes con tres valores posibles cada una, con lo que se obtiene un total de 27 combinaciones posibles. (3 nombres de dispositivos x 3 esquemas de direccionamiento x 3 topologías = 27 isomorfos).

Situación 1: Dirección de red 10.11.48.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN Host-D	60	10.11.48.0/26	10.11.48.1	10.11.48.62	10.11.48.63
LAN Host-B	30	10.11.48.64/27	10.11.48.65	10.11.48.94	10.11.48.95
LAN Host-A	14	10.11.48.96/28	10.11.48.97	10.11.48.110	10.11.48.111
LAN Host-C	6	10.11.48.112/29	10.11.48.113	10.11.48.118	10.11.48.119
Enlace WAN	2	10.11.48.120/30	10.11.48.121	10.11.48.122	10.11.48.123

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Edificio1	G0/0	10.11.48.97	255.255.255.240	No aplicable
	G0/1	10.11.48.65	255.255.255.224	No aplicable
	S0/0/0	10.11.48.121	255.255.255.252	No aplicable
Edificio2	G0/0	10.11.48.113	255.255.255.248	No aplicable
	G0/1	10.11.48.1	255.255.255.192	No aplicable
	S0/0/0	10.11.48.122	255.255.255.252	No aplicable
ASW1	VLAN 1	10.11.48.98	255.255.255.240	10.11.48.97
ASW2	VLAN 1	10.11.48.66	255.255.255.224	10.11.48.65
ASW3	VLAN 1	10.11.48.114	255.255.255.248	10.11.48.113
ASW4	VLAN 1	10.11.48.2	255.255.255.192	10.11.48.1
Host A	NIC	10.11.48.110	255.255.255.240	10.11.48.97
Host B	NIC	10.11.48.94	255.255.255.224	10.11.48.65
Host C	NIC	10.11.48.118	255.255.255.248	10.11.48.113
Host D	NIC	10.11.48.62	255.255.255.192	10.11.48.1

Edificio 1

```
en
conf t
int g0/0
ip add 10.11.48.97 255.255.255.240
no shut
int g0/1
ip add 10.11.48.65 255.255.255.224
no shut
```

ASW3

```
en
conf t
int vlan 1
ip add 10.11.48.114 255.255.255.248
no shut
ip def 10.11.48.113
```

Situación 2: Dirección de red 172.31.103.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
PC-A LAN	27	172.31.103.0/27	172.31.103.1	172.31.103.30	172.31.103.31
PC-B LAN	25	172.31.103.32/27	172.31.103.33	172.31.103.62	172.31.103.63
PC-C LAN	14	172.31.103.64/28	172.31.103.65	172.31.103.78	172.31.103.79
PC-D LAN	8	172.31.103.80/28	172.31.103.81	172.31.103.94	172.31.103.95
Enlace WAN	2	172.31.103.96/30	172.31.103.97	172.31.103.98	172.31.103.99

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Branch1	G0/0	172.31.103.1	255.255.255.224	No aplicable
	G0/1	172.31.103.33	255.255.255.224	No aplicable
	S0/0/0	172.31.103.97	255.255.255.252	No aplicable
Branch2	G0/0	172.31.103.65	255.255.255.240	No aplicable
	G0/1	172.31.103.81	255.255.255.240	No aplicable
	S0/0/0	172.31.103.98	255.255.255.252	No aplicable
Sala 114	VLAN 1	172.31.103.2	255.255.255.224	172.31.103.1
Sala 279	VLAN 1	172.31.103.34	255.255.255.224	172.31.103.33
Sala 312	VLAN 1	172.31.103.66	255.255.255.240	172.31.103.65
Sala 407	VLAN 1	172.31.103.82	255.255.255.240	172.31.103.81
PC-A	NIC	172.31.103.30	255.255.255.224	172.31.103.1
PC-B	NIC	172.31.103.62	255.255.255.224	172.31.103.33
PC-C	NIC	172.31.103.78	255.255.255.240	172.31.103.65
PC-D	NIC	172.31.103.94	255.255.255.240	172.31.103.81

Sucursal 1

```
en
conf t
int g0/0
ip add 172.31.103.1 255.255.255.224
no shut
int g0/1
```

```
ip add 172.31.103.33 255.255.255.224
no shut
```

Sala 312

```
en
conf t
int vlan 1
ip add 172.31.103.66 255.255.255.240
no shut
ip def 172.31.103.65
```

Situación 3: Dirección de red 192.168.72.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN User-4	58	192.168.72.0/26	192.168.72.1	192.168.72.62	192.168.72.63
LAN User-3	29	192.168.72.64/27	192.168.72.65	192.168.72.94	192.168.72.95
LAN User-2	15	192.168.72.96/27	192.168.72.97	192.168.72.126	192.168.72.127
LAN User-1	7	192.168.72.128/28	192.168.72.129	192.168.72.142	192.168.72.143
Enlace WAN	2	192.168.72.144/30	192.168.72.145	192.168.72.146	192.168.72.147

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Sitio remoto 1	G0/0	192.168.72.129	255.255.255.240	No aplicable
	G0/1	192.168.72.97	255.255.255.224	No aplicable
	S0/0/0	192.168.72.145	255.255.255.252	No aplicable
Sitio remoto 2	G0/0	192.168.72.65	255.255.255.224	No aplicable
	G0/1	192.168.72.1	255.255.255.192	No aplicable
	S0/0/0	192.168.72.146	255.255.255.252	No aplicable
Sw1	VLAN 1	192.168.72.130	255.255.255.240	192.168.72.129
Sw2	VLAN 1	192.168.72.98	255.255.255.224	192.168.72.97
Sw3	VLAN 1	192.168.72.66	255.255.255.224	192.168.72.65
Sw4	VLAN 1	192.168.72.2	255.255.255.192	192.168.72.1
Usuario 1	NIC	192.168.72.142	255.255.255.240	192.168.72.129
Usuario 2	NIC	192.168.72.126	255.255.255.224	192.168.72.97
Usuario 3	NIC	192.168.72.94	255.255.255.224	192.168.72.65
Usuario 4	NIC	192.168.72.62	255.255.255.192	192.168.72.1

Sitio remoto 1

```
en
conf t
int g0/0
ip add 192.168.72.129 255.255.255.240
no shut
int g0/1
```

```
      ip add 192.168.72.97 255.255.255.224
      no shut
```

Sw-3

```
      en
      conf t
      int vlan 1
      ip add 192.168.72.66 255.255.255.224
      no shut
      ip def 192.168.72.65
```

Packet Tracer: Implementación de un esquema de direccionamiento IPv6 dividido en subredes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

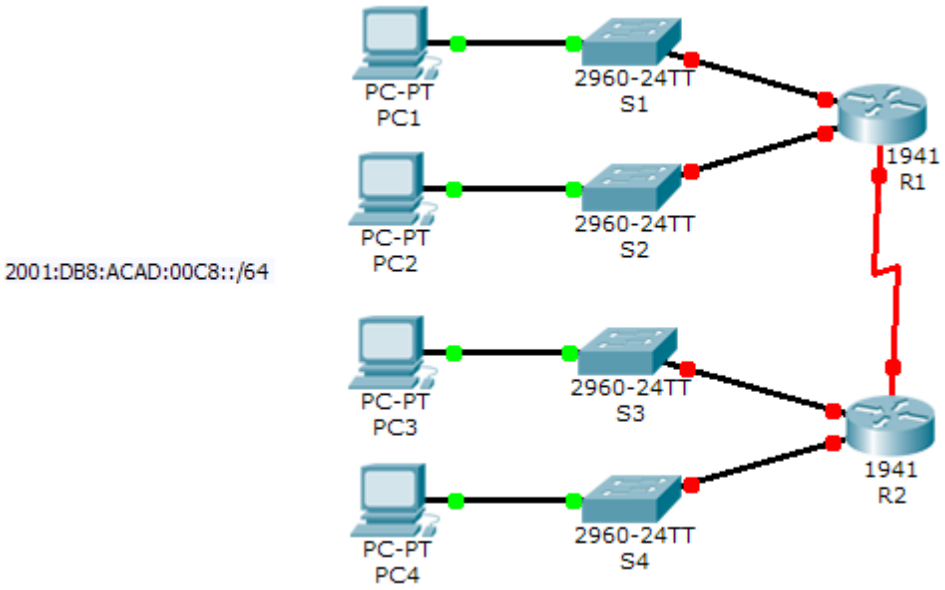


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Link-Local
R1	G0/0	2001:DB:ACAD:00C8::1/64	FE80::1
	G0/1	2001:DB:ACAD:00C9::1/64	FE80::1
	S0/0/0	2001:DB:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB:ACAD:00CA::1/64	FE80::2
	G0/1	2001:DB:ACAD:00CB::1/64	FE80::2
	S0/0/0	2001:DB:ACAD:00CC::2/64	FE80::2
PC1	NIC	Configuración automática	
PC2	NIC	Configuración automática	
PC3	NIC	Configuración automática	
PC4	NIC	Configuración automática	

Objetivos

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Situación

El administrador de red desea que asigne cinco subredes IPv6 /64 a la red que se muestra en la topología. Su tarea consiste determinar las subredes IPv6, asignar direcciones IPv6 a los routers y configurar las PC para que reciban automáticamente el direccionamiento IPv6. El último paso es verificar la conectividad entre los hosts IPv6.

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Paso 1: Determinar la cantidad de subredes necesarias

Comience con la subred IPv6 2001:DB:ACAD:00C8::/64 y asígnela a la LAN del R1 conectada a GigabitEthernet 0/0, como se muestra en la **tabla de subredes**. Para el resto de las subredes IPv6, incremente la dirección de la subred 2001:DB:ACAD:00C8::/64 de a 1 y complete la **tabla de subredes** con las direcciones de la subred IPv6.

Tabla de subredes

Descripción de la subred	Dirección de subred
R1 G0/0 LAN	2001:DB:ACAD:00C8::0/64
R1 G0/1 LAN	2001:DB:ACAD:00C9::0/64
R2 G0/0 LAN	2001:DB:ACAD:00CA::0/64
R2 G0/1 LAN	2001:DB:ACAD:00CB::0/64
Enlace WAN	2001:DB:ACAD:00CC::0/64

Paso 2: Asignar el direccionamiento IPv6 a los routers

a. Asigne las primeras direcciones IPv6 al R1 para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IPv6 al R2 para las dos LAN. Asigne la segunda dirección IPv6 para el enlace WAN.

c. Registre el esquema de direccionamiento IPv6 en la **tabla de direccionamiento**.

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Paso 1: Configurar el direccionamiento IPv6 en los routers

Nota: esta red ya está configurada con algunos comandos de IPv6 que se abordan en un curso posterior. En este punto de sus estudios, solo necesita saber cómo configurar la dirección IPv6 en una interfaz.

Configure el R1 y el R2 con las direcciones IPv6 que especificó en la **tabla de direccionamiento** y active las interfaces.

```
Router(config-if)# ipv6 address ipv6-address/prefix
Router(config-if)# ipv6 address ipv6-link-local link-local
```


Paso 2: Configurar las PC para que reciban el direccionamiento IPv6 automáticamente

Configure las cuatro PC para que tengan configuración automática. Luego, cada una debe recibir automáticamente las direcciones IPv6 completas de los routers.

Paso 3: Verificar la conectividad entre las PC

Cada PC debe ser capaz de hacer ping a las otras PC y a los routers.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6	Tabla de subredes	30	
	Tabla de direccionamiento	30	
	Total de la parte 1	**60**	
	Puntuación de Packet Tracer	**40**	
	Puntuación total	**100**	

Packet Tracer: Reto de habilidades de integración

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

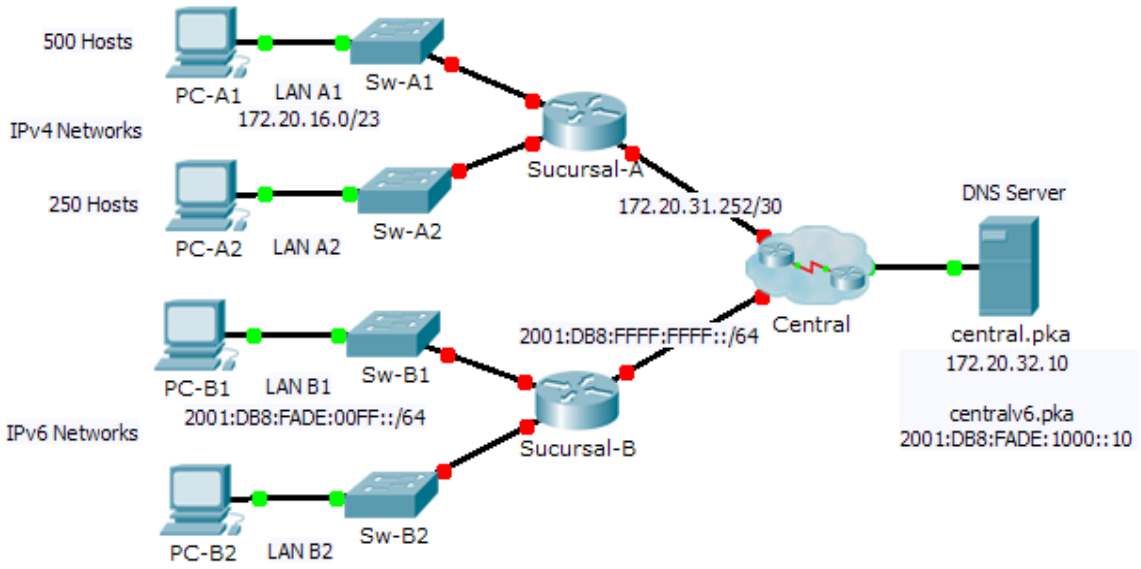


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
Sucursal-A	G0/0	172.20.16.1	255.255.254.0	No aplicable
	G0/1	172.20.18.1	255.255.255.0	No aplicable
	G0/2	172.20.31.254	255.255.255.252	No aplicable
Sucursal-B	G0/0	2001:DB8:FADE:00FF::1/64		No aplicable
	G0/1	2001:DB8:FADE:0100::1/64		No aplicable
	G0/2	2001:DB8:FFFF:FFFF::2/64		No aplicable
PC-A1	NIC	172.20.17.254	255.255.254.0	172.20.16.1
PC-A2	NIC	172.20.18.254	255.255.255.0	172.20.18.1
PC-B1	NIC	2001:DB8:FADE:00FF::10/64		FE80::B
PC-B2	NIC	2001:DB8:FADE:0100::10/64		FE80::B

Situación

Como técnico de redes familiarizado con implementaciones de direccionamiento IPv4 e IPv6, ya está preparado para tomar una infraestructura de red existente y aplicar sus conocimientos y habilidades a finalizar la configuración. En esta actividad, el administrador de red ya configuró algunos comandos en los routers. **No borre ni modifique esas configuraciones**. Su tarea consiste en completar el esquema de direccionamiento IPv4 e IPv6, implementar el direccionamiento IPv4 e IPv6 y verificar la conectividad.

Requisitos

- Configure los parámetros iniciales en **Sucursal-A** y **Sucursal-B**, incluidos el nombre de host, el aviso, las líneas y las contraseñas. Utilice **cisco** como contraseña de EXEC del usuario y **class** como contraseña de EXEC privilegiado. Encripte todas las contraseñas.
- LAN A1 utiliza la subred 172.20.16.0/23. Asigne la siguiente subred disponible a LAN A2 para admitir un máximo de 250 hosts.
- LAN B1 utiliza la subred 2001:DB8:FADE:00FF::/64. Asigne la siguiente subred disponible a la B2 de LAN.
- Termine de registrar el esquema de direccionamiento en la **tabla de direccionamiento** con las siguientes pautas:
  - Asigne la primera dirección IP a la interfaz del router para LAN A1, LAN A2, LAN B1 y LAN B2.
  - Para las redes IPv4, asigne la última dirección IPv4 a las PC.
  - Para las redes IPv6, asigne la 16.ª dirección IPv6 a las PC.
- Configure el direccionamiento de los routers según los registros. Incluya una descripción adecuada para cada interfaz del router. **Sucursal-B** utiliza FE80::B como dirección link-local.
- Configure el direccionamiento de las PC según los registros. Las direcciones del servidor DNS para IPv4 e IPv6 se muestran en la topología.
- Verifique la conectividad entre las PC IPv4 y entre las PC IPv6.
- Verifique que las PC IPv4 puedan acceder a la página Web en **central.pka**.
- Verifique que las PC IPv6 puedan acceder a la página Web en **centralv6.pka**.

Tabla de calificación sugerida

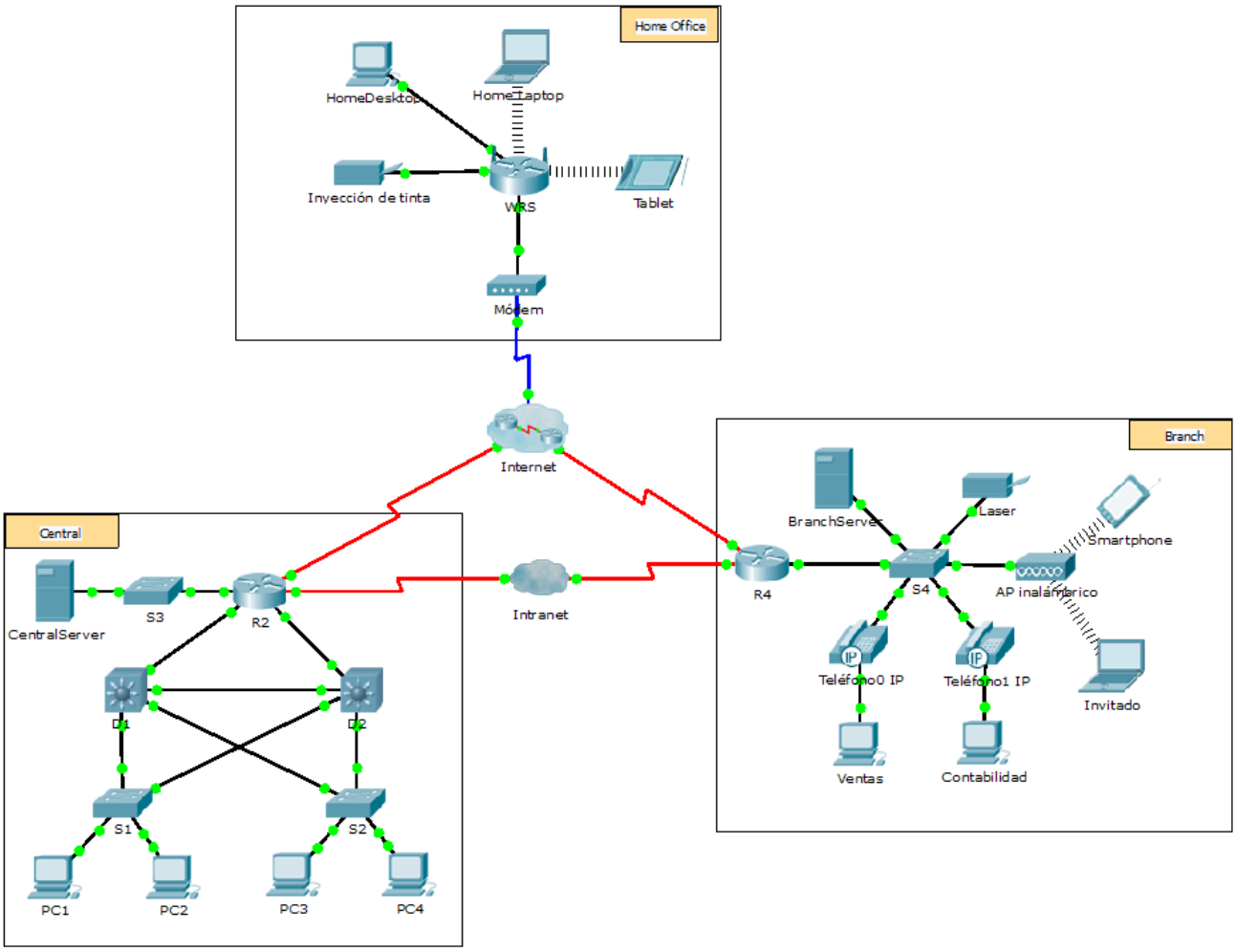
Sección de la actividad	Posibles puntos	Puntos obtenidos
Registro de la tabla de direccionamiento	**25**	
Puntuación de Packet Tracer	**75**	
Puntuación total	**100**	

Packet Tracer: Servidores Web y de correo electrónico

(version para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Configurar y verificar los servicios Web

Parte 2: Configurar y verificar los servicios de correo electrónico

Información básica

En esta actividad, configurará los servicios HTTP y de correo electrónico mediante el servidor simulado de Packet Tracer. Luego, configurará clientes para que accedan a los servicios HTTP y de correo electrónico.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de HTTP y de correo electrónico tiene sus propias instrucciones exclusivas de configuración e instalación.

Parte 1: Configurar y verificar los servicios Web

Paso 1: Configurar servicios Web en CentralServer y BranchServer

a. Haga clic en **CentralServer** y, a continuación, haga clic en la ficha **Config** > **HTTP**.

b. Haga clic en **On** (Activar) para habilitar HTTP y HTTP seguro (HTTPS).

c. Optativo: personalice el código HTML.

d. Repita desde el paso 1a hasta el paso 1c en **BranchServer**.

Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web

Existen muchos dispositivos terminales en esta red, pero para este paso, use **PC3**.

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Escritorio > Explorador Web).

b. En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.

c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.

d. En el cuadro de dirección URL, introduzca **centralserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **CentralServer**.

e. En el cuadro de dirección URL, introduzca **branchserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.

f. ¿Qué protocolo traduce los nombres **centralserver.pt.pka** y **branchserver.pt.pka** por direcciones IP?
Servicio de nombres de dominios (DNS, Domain Name Service)

Parte 2: Configurar y verificar los servicios de correo electrónico en los servidores

Paso 1: Configurar CentralServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **CentralServer** y, a continuación, seleccione la ficha **Config**, seguida del botón **EMAIL** (Correo electrónico).

b. Haga clic en **On** para habilitar SMTP y POP3.

c. Establezca el nombre de dominio **centralserver.pt.pka** y haga clic en **Set** (Establecer).

d. Cree un usuario denominado **usuario-de-central** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.

Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **BranchServer** y, a continuación, haga clic en la ficha **Config** > **EMAIL**.

b. Haga clic en **On** para habilitar SMTP y POP3**.**

c. Establezca el nombre de dominio **branchserver.pt.pka** y haga clic en **Set**.

d. Cree un usuario denominado **usuario-de-sucursal** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.

Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **E Mail** (Correo electrónico).

b. Introduzca los siguientes valores en los campos correspondientes:

   1) Your Name (Su nombre): **Usuario de central**

   2) Email Address (Dirección de correo electrónico): **usuario-de-central@centralserver.pt.pka**

   3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**

   4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**

   5) User Name (Nombre de usuario): **usuario-de-central**

   6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).

Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

a. Haga clic en **Sales** (Ventas) y, a continuación, haga clic en la ficha **Desktop** > **E Mail**.

b. Introduzca los siguientes valores en los campos correspondientes:

   1) Your Name (Su nombre): **Usuario de sucursal**

   2) Email Address (Dirección de correo electrónico): **usuario-de-sucursal@branchserver.pt.pka**

   3) Incoming Mail Server (Servidor de correo entrante): **172.16.0.3**

   4) Outgoing Mail Server (Servidor de correo saliente): **172.16.0.3**

   5) User Name (Nombre de usuario): **usuario-de-sucursal**

   6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).

e. Esta actividad debe completarse en un 100%. No cierre la ventana de configuración de Sales ni la ventana del explorador de correo.

Paso 5: Envíe un correo electrónico desde el cliente Sales y el cliente PC3.

a. Desde la ventana del **explorador de correo** de **Sales**, haga clic en **Compose** (Redactar).

b. Introduzca los siguientes valores en los campos correspondientes:

   1) To (Para): **usuario-de-central@centralserver.pt.pka**

   2) Subject (Asunto): *Personalice el asunto*.

   3) **Email** body (Cuerpo del correo electrónico): *Personalice el correo electrónico*.

c. Haga clic en **Send** (Enviar).

d. Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

e. Haga clic en **Receive** (Recibir). Aparece un correo electrónico proveniente de Sales. Haga doble clic en el correo electrónico.

f. Haga clic en **Reply** (Responder), personalice una respuesta y haga clic en **Send**.

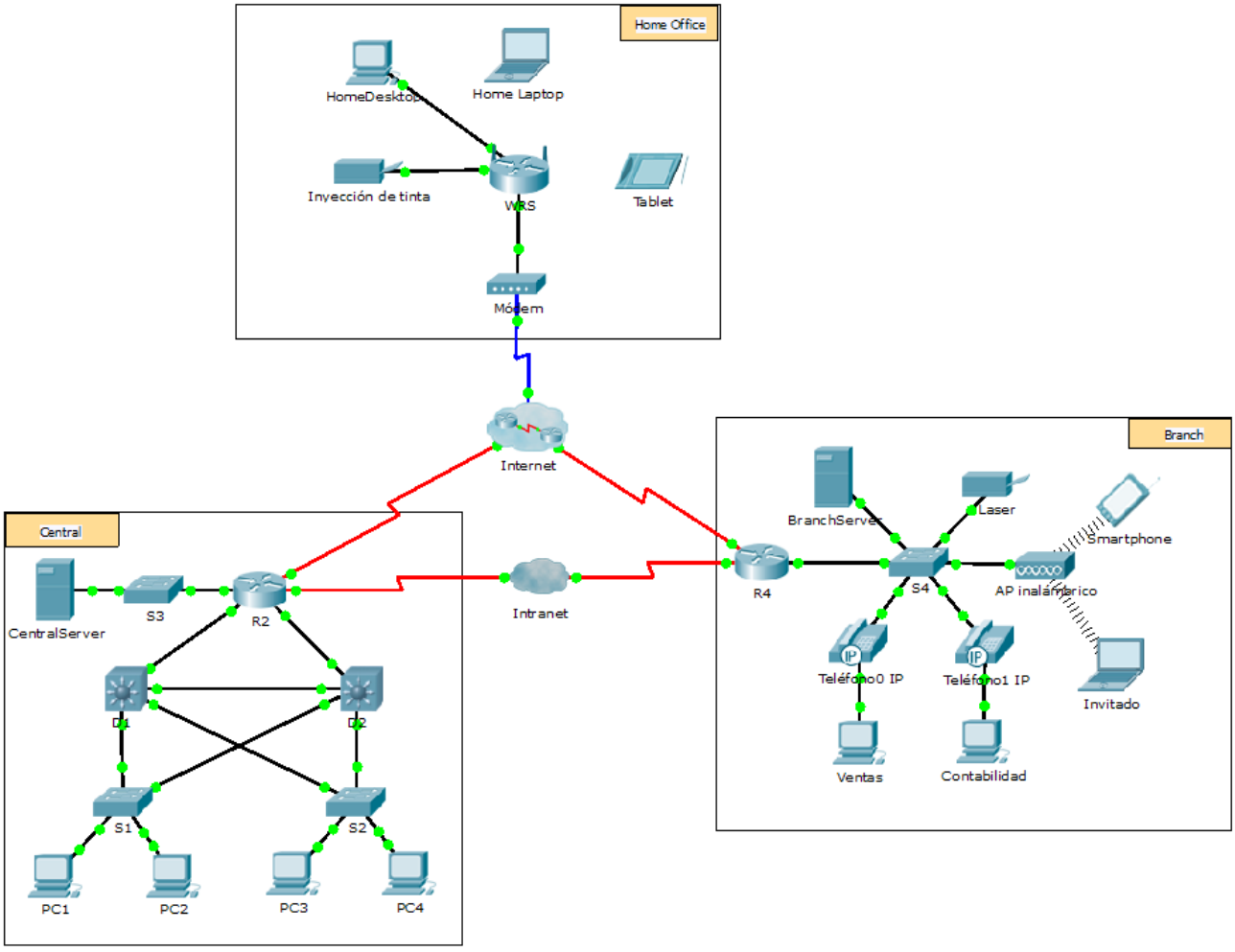
g. Verifique que **Sales** haya recibido la respuesta.

Packet Tracer: Servidores de DHCP y servidores DNS

(version para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Configurar el direccionamiento IPv4 estático

Parte 2: Configurar y verificar los registros DNS

Información básica

En esta actividad, configurará y verificará el direccionamiento IP estático y el direccionamiento DHCP. A continuación, configurará un servidor DNS para que asigne direcciones IP a los nombres de sitios Web.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de DHCP y DNS tiene sus propias instrucciones exclusivas de configuración e instalación.

Parte 1: Configurar el direccionamiento IPv4 estático

Paso 1: Configurar la impresora de inyección de tinta con direccionamiento IPv4 estático

Las PC de oficinas domésticas necesitan conocer la dirección IPv4 de una impresora para enviarle información. Por lo tanto, la impresora debe utilizar una dirección IPv4 estática (invariable).

a. Haga clic en **Inkjet** (Inyección de tinta) y, a continuación, haga clic en la ficha **Config**, en la que se muestran los parámetros de Global Settings (Configuración global).

b. Asigne de manera estática la dirección de gateway **192.168.0.1** y la dirección de servidor DNS **64.100.8.8**.

c. Haga clic en **FastEthernet0** y asigne de manera estática la dirección IP **192.168.0.2** y la dirección de máscara de subred **255.255.255.0**.

d. Cierre la ventana Inkjet.

Paso 2: Configurar WRS para que proporcione servicios de DHCP

a. Haga clic en **WRS** y, a continuación, haga clic en la ficha **GUI** y maximice la ventana.

b. Se muestra la ventana Basic Setup (Configuración básica) de manera predeterminada. Configure los siguientes parámetros en la sección Network Setup (Configuración de red):

   1) Cambie la Dirección IP a **192.168.0.1**.

   2) Establezca la máscara de subred **255.255.255.0**.

   3) Habilite el servidor de DHCP.

   4) Establezca la dirección DNS estática 1 **64.100.8.8**.

   5) Desplácese hasta la parte inferior y haga clic en **Save** (Guardar).

c. Cierre la ventana **WRS**.

Paso 3: Solicitar direccionamiento DHCP para la computadora portátil doméstica

Esta actividad se centra en la oficina doméstica. Los clientes que configurará con DHCP son **Home Laptop** (Computadora portátil doméstica) y **Tablet PC**.

a. Haga clic en **Home Laptop** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

c. Ahora, **Home Laptop** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

d. Cierre la ventana IP Configuration y, a continuación, cierre la ventana **Home Laptop**.

Paso 4: Solicitar direccionamiento DHCP para la tablet PC

a. Haga clic en **Tablet** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration**.

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

Paso 5: Probar el acceso a sitios Web

a. Cierre la ventana **IP Configuration** y, a continuación, haga clic en Web Browser (Explorador Web).

b. En el cuadro de dirección URL, escriba **10.10.10.2** (para el sitio Web de **CentralServer**) o **64.100.200.1** (para el sitio web de **BranchServer**) y haga clic en **Go** (Ir). Deben aparecer ambos sitios Web.

c. Vuelva a abrir el explorador Web. Pruebe los nombres para esos mismos sitios Web mediante la introducción de **centralserver.pt.pka** y **branchserver.pt.pka**. Haga clic en **Fast Forward Time** (Adelantar el tiempo) en la barra amarilla que se encuentra debajo de la topología, a fin de acelerar el proceso.

Parte 2: Configurar los registros en el servidor DNS

Paso 1: Configurar famous.dns.pka con registros para CentralServer y BranchServer.

En general, los registros DNS se realizan ante compañías, pero en esta actividad, usted controla el servidor **famous.dns.pka** en Internet.

a. Haga clic en la nube de **Internet**. Se muestra una nueva red.

b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config** > **DNS**.

c. Agregue los siguientes registros del recurso:

Nombre de registro del recurso	Dirección
centralserver.pt.pka	10.10.10.2.
branchserver.pt.pka	64.100.200.1

d. Cierre la ventana famous.dns.pka.

e. Haga clic en **Back** (Atrás) para salir de la nube de **Internet**.

Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

Ahora que configuró los registros DNS, **Home Laptop** y **Tablet** deben ser capaces de acceder a los sitios Web mediante los nombres en lugar de las direcciones IP. Primero, compruebe que el cliente DNS funcione correctamente y, a continuación, verifique el acceso al sitio Web.

a. Haga clic en **Home Laptop** o **Tablet**.

b. Si el explorador Web está abierto, ciérrelo y seleccione **Command Prompt** (Símbolo del sistema).

c. Verifique el direccionamiento IPv4 mediante la introducción del comando **`ipconfig /all`**. Debe ver la dirección IP del servidor DNS.

d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.

Nota: es posible que los primeros dos o tres pings fallen, ya que Packet Tracer simula los distintos procesos que deben ocurrir para que la conectividad a un recurso remoto sea correcta.

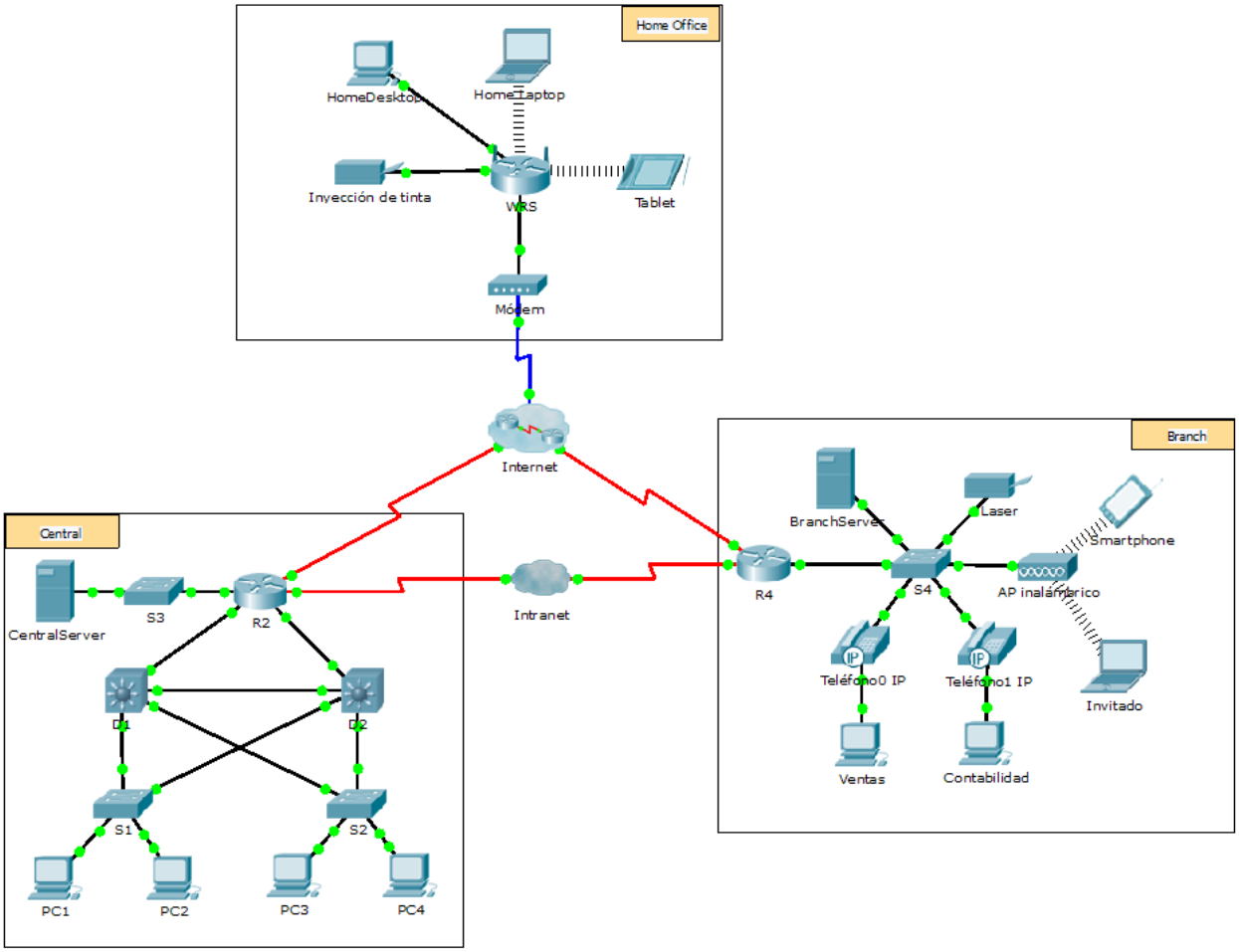
e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos **`nslookup centralserver.pt.pka`** y **`nslookup branchserver.pt.pka`**. Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.

f. Cierre la ventana Command Prompt y haga clic en **Web Browser**. Verifique que **Home Laptop** o **Tablet** puedan acceder ahora a las páginas Web de **CentralServer** y **BranchServer**.

Packet Tracer: Servidores FTP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Configurar servicios FTP en los servidores

Parte 2: Subir un archivo al servidor FTP

Parte 3: Descargar un archivo del servidor FTP

Información básica

En esta actividad, configurará servicios FTP. Luego, utilizará los servicios FTP para transferir archivos entre los clientes y el servidor.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de servidor y cliente FTP tiene sus propias instrucciones exclusivas de configuración e instalación. La primera vez que intente conectarse a una dirección Web, Packet Tracer tardará varios segundos en simular el proceso de resolución de nombres DNS.

Parte 1: Configurar servicios FTP en los servidores

Paso 1: Configurar el servicio FTP en CentralServer

a. Haga clic en **CentralServer** > ficha **Config** > **FTP**.

b. Haga clic en **On** (Activar) para habilitar el servicio FTP.

c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario. Haga clic en el botón **+** para agregar la cuenta:

Nombre de usuario	Contraseña	Permisos
anonymous	anonymous	limitado a **Read** (Lectura) y **List** (Lista)
administrator	cisco	permiso total

d. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón **-** para eliminarla. Cierre la ventana de configuración de la CentralServer.

Paso 2: Configurar el servicio FTP en BranchServer

Repita el paso 1 en **BranchServer**.

Parte 2: Subir un archivo al servidor FTP

Paso 1: Transferir el archivo README.txt de la computadora portátil doméstica a CentralServer

Como administrador de red, debe colocar un aviso en los servidores FTP. El documento se creó en la computadora portátil doméstica y se debe subir a los servidores FTP.

a. Haga clic en **Home Laptop** (Computadora portátil doméstica) y, a continuación, haga clic en la ficha **Desktop** > **Text Editor** (Escritorio > Editor de texto).

b. Abra el archivo **README.txt** y revíselo. Cierre **Text Editor** cuando haya terminado.

Nota: no modifique el archivo porque esto afecta la puntuación.

c. En la ficha **Desktop**, abra la ventana del símbolo del sistema y siga estos pasos:

1) Escriba **`ftp centralserver.pt.pka`**. Espere algunos segundos mientras se conecta el cliente.

Nota: dado que Packet Tracer es una simulación, FTP puede tardar hasta 30 segundos en conectarse la primera vez.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **administrator** (administrador).

3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo **`dir.`** Se muestra el directorio de archivos en **CentralServer**.

4) Transfiera el archivo README.txt: en la petición de entrada `ftp>`, escriba **`put README.txt`**. El archivo README.txt se transfiere de la computadora portátil doméstica a **CentralServer**.

5) Para verificar la transferencia del archivo, escriba **`dir`**. El archivo README.txt ahora figura en el directorio de archivos.

6) Cierre el cliente FTP escribiendo **`quit`**. La petición de entrada se revierte a `PC>`.

Paso 2: Transferir el archivo README.txt de la computadora portátil doméstica a BranchServer

a. Repita el paso 1c para transferir el archivo README.txt a **branchserver.pt.pka**.

b. Cierre las ventanas Command Prompt (Símbolo del sistema) y Home Laptop.

Parte 3: Descargar un archivo del servidor FTP

Paso 1: Transferir README.txt de CentralServer a la PC2

a. Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

1) Escriba **`ftp centralserver.pt.pka`**.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **anonymous** (anónimo)

3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo **`dir.`** El archivo README.txt figura en la parte superior de la lista del directorio.

4) Descargue el archivo README.txt: en la petición de entrada ftp>, escriba **`get README.txt`**. El archivo README.txt se transfiere a la **PC2**.

5) Verifique que la cuenta **anonymous** no tenga permiso para escribir archivos en **CentralServer** escribiendo **`put sampleFile.txt`**. Se muestra el siguiente mensaje de error:

```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...

%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

6) Cierre el cliente FTP escribiendo **`quit`**. La petición de entrada se revierte a `PC>`.

7) Para verificar la transferencia del archivo a la PC2, escriba **`dir`**. El archivo README.txt figura en el directorio.

8) Cierre la ventana de línea de comandos.

b. En la ficha **Desktop**, abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.

c. Cierre **Text Editor** y, luego, cierre la ventana de configuración de la PC2.

Paso 2: Transferir el archivo README.txt de BranchServer al smartphone

Repita el paso 1 para **Smart Phone**, excepto la descarga del archivo README.txt desde **branchserver.pt.pka**.

Función Multiusuario de Packet Tracer: Tutorial
(versión para el instructor)

Topología

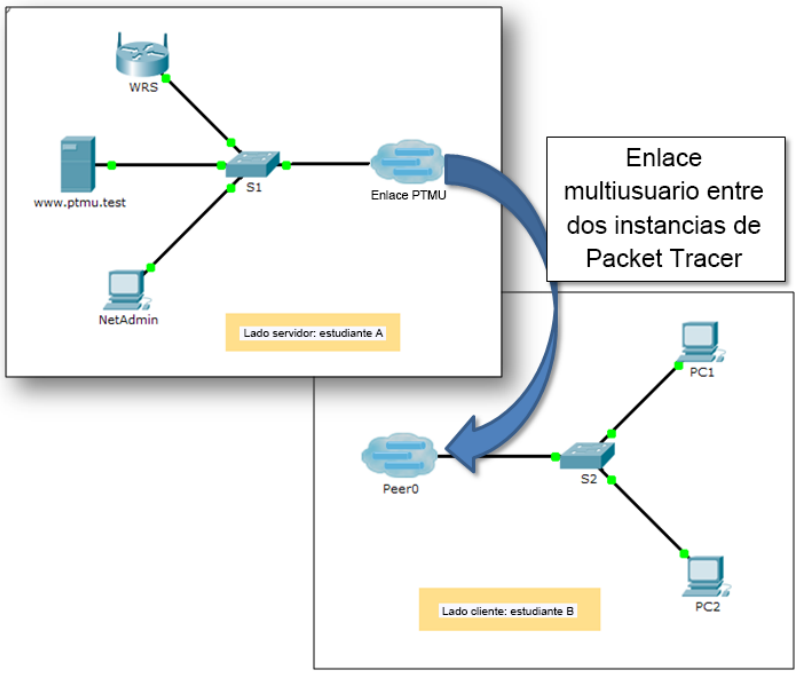


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred	Servidor DNS
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objetivos

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Información básica

La característica Multiusuario de Packet Tracer permite varias conexiones punto a punto entre diversas instancias de Packet Tracer. Esta primera actividad de la función Multiusuario de Packet Tracer (PTMU, Packet Tracer Multiuser) es un tutorial rápido que muestra los pasos para establecer y verificar una conexión multiusuario a otra instancia de Packet Tracer dentro de la misma LAN. Idealmente, esta actividad está pensada para dos estudiantes. Sin embargo, también se puede realizar como actividad individual abriendo los dos archivos independientes para crear dos instancias distintas de Packet Tracer en su máquina local.

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.

b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.

- El jugador del lado servidor abre el archivo **Packet Tracer Multiuser - Tutorial - Server Side.pka.**
- El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Tutorial - Client Side.pka.**

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Jugador del lado servidor: configurar el lado servidor del enlace PTMU

El jugador del lado cliente debe contar con la dirección IP, el número de puerto y la contraseña utilizados por el jugador del lado servidor para poder crear una conexión con el jugador del lado servidor.

a. Siga estos pasos para configurar Packet Tracer de manera de que esté preparado para recibir una conexión entrante:

1) Haga clic en el menú **Extensions** (Extensiones), después en **Multiuser** (Multiusuario) y, finalmente, en **Listen** (Escuchar).

2) Tiene dos Local Listening Addresses (Direcciones de escucha locales). Si se indican más de dos direcciones, utilice solo las primeras dos. La primera es la dirección IP real de la máquina local del jugador del lado servidor. Es la dirección IP que utiliza su PC para enviar y recibir datos. La otra dirección IP (127.0.0.1) solamente se puede utilizar para comunicaciones dentro del entorno de su propia PC.

3) El número de puerto se indica junto a las direcciones IP y en el campo Port Number (Número de puerto). Si esta es la primera instancia de Packet Tracer que abrió en la PC, el número de puerto será 38000. Sin embargo, si hay varias instancias abiertas, el número aumenta de a uno por cada instancia (38001, 38002, etcétera). El número de puerto es necesario para que el jugador del lado cliente configure la conexión multiusuario.

4) La contraseña está establecida en **cisco** de manera predeterminada. Puede cambiarla, pero no es necesario hacerlo para esta actividad.

5) Comuníquele al jugador del lado cliente su dirección IP, número de puerto y contraseña. El jugador del lado cliente necesitará estos tres datos para conectarse a su instancia de Packet Tracer en el paso 3.

6) En la sección **Existing Remote Networks** (Redes remotas existentes), debe hacer clic en el botón de opción **Always Accept** (Aceptar siempre) o **Prompt** (Preguntar) para que el jugador del lado cliente se conecte de forma correcta.

7) En la sección **New Remote Networks** (Nuevas redes remotas), confirme que el botón de opción **Always Deny** (Denegar siempre) esté habilitado. Esto evitará que el jugador del lado cliente cree un nuevo enlace no especificado en esta actividad.

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

b. Haga clic en el ícono **Multiuser Connection** (Conexión multiusuario, representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

c. Haga clic en el nombre **Peer0** y cámbielo por **Enlace PTMU** (distingue mayúsculas de minúsculas).

d. Haga clic en la nube del **Enlace PTMU** y verifique que en Connection Type (Tipo de conexión) diga **Incoming** (Entrante) y que la casilla de verificación **Use Global Multiuser Password** (Utilizar contraseña de multiusuario global) esté habilitada.

e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).

f. Haga clic en el **S1** y elija la conexión GigabitEthernet1/1. A continuación, haga clic en **Enlace PTMU** > **Create New Link** (Crear nuevo enlace).

Paso 3: Jugador del lado cliente: configurar el lado cliente del enlace PTMU

a. Registre la siguiente información que le suministró el jugador del lado servidor:

Dirección IP: _____

Número de puerto: _____

Contraseña (**cisco**, de manera predeterminada) _____

b. El jugador del lado cliente debe agregar una **red remota** a la topología mediante las siguientes instrucciones: haga clic en el ícono **Multiuser Connection** (representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

c. Haga clic en la nube de **Peer0** y cambie Connection Type por **Outgoing** (Saliente).

1) En el campo Peer Address (Dirección del punto), introduzca la dirección IP del lado servidor que registró en el paso 3a.

2) En el campo Peer Port Number (Número de puerto del punto), introduzca el número de puerto del lado servidor que registró en el paso 3a.

3) En el campo Peer Network Name (Nombre de red del punto), introduzca **Enlace PTMU**. Este campo distingue mayúsculas de minúsculas.

4) En el campo Password (Contraseña), introduzca **cisco** o la contraseña que haya configurado el jugador del lado servidor.

5) Haga clic en **Connect** (Conectar).

d. La nube de **Peer0** ahora debería ser amarilla, lo que indica que las dos instancias de Packet Tracer están conectadas.

e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).

f. Haga clic en el **S2** y elija la conexión **GigabitEthernet1/1**. A continuación, haga clic en **Peer0** > **Link 0 (S1 GigabitEthernet 1/1)**.

Tanto la nube de **Peer0** del jugador del lado cliente como la nube de **Enlace PTMU** del jugador del lado servidor ahora deben ser azules. Después de un período breve, la luz de enlace entre el switch y la nube pasa de color ámbar a verde.

El enlace de multiusuario está establecido y listo para probar.

Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Paso 1: Configurar el direccionamiento IP

a. El jugador del lado servidor configura el servidor de **www.ptmu.test** con la dirección IP **10.10.10.1**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.

b. El jugador del lado cliente configura la PC con la dirección IP **10.10.10.10**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.

Paso 2: Verificar la conectividad y acceder a una página Web desde el lado servidor

a. El jugador del lado servidor ahora debe poder hacer ping a la PC en la instancia de Packet Tracer del jugador del lado cliente.

b. El jugador del lado cliente ahora debe poder hacer ping al servidor de **www.ptmu.test**.

c. El jugador del lado cliente también debe poder abrir el explorador Web y acceder a la página Web en **www.ptmu.test.** ¿Qué se muestra en la página Web? Congratulations! You successfully verified a Packet Tracer multiuser connection (Felicidades. Verificó correctamente una conexión multiusuario de Packet Tracer).

Función Multiusuario de Packet Tracer: Implementación de servicios (versión para el instructor)

Topología

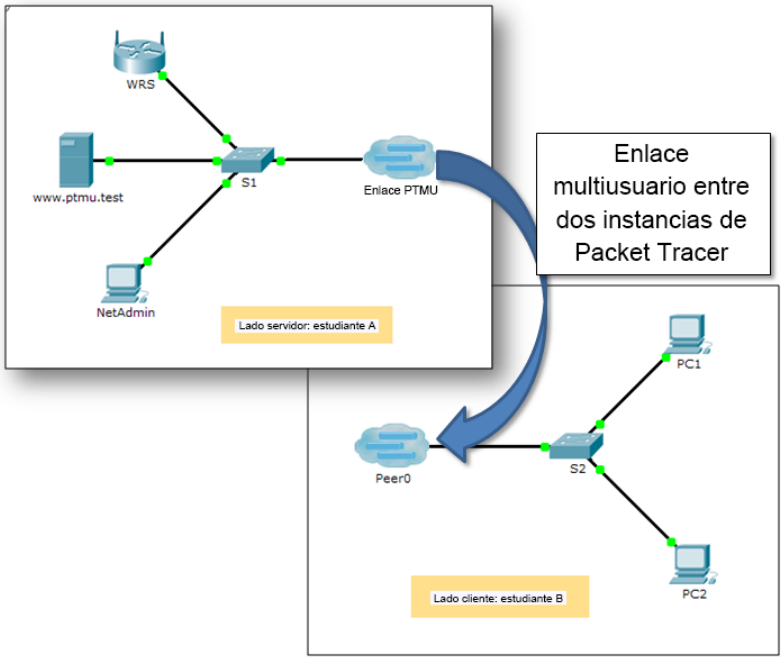


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred
Jugador del lado servidor		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP asignado	DHCP asignado
Jugador del lado cliente		
S2	172.16.1.2	255.255.255.0
PC1	DHCP asignado	DHCP asignado
PC2	DHCP asignado	DHCP asignado

Objetivos

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Información básica

Nota: completar las actividades previas de este capítulo, incluida la actividad **Función Multiusuario de Packet Tracer: Tutorial**, constituye un requisito previo.

En esta actividad para varios usuarios, dos estudiantes (jugadores) cooperan para implementar y verificar servicios, incluso DHCP, HTTP, correo electrónico, DNS y FTP. El jugador del lado servidor implementará y verificará servicios en un servidor. El jugador del lado cliente configurará dos clientes y verificará el acceso a los servicios.

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.

b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.

   - El jugador del lado servidor abre el archivo **Packet Tracer Multiuser - Implement Services - Server Side.pka.**
   - El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Implement Services - Client Side.pka.**

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los switches

Cada jugador: configure su respectivo switch con los siguientes parámetros:

- Nombre de host que utilice el nombre para mostrar (**S1** o **S2**)
- Mensaje del día (MOTD) adecuado
- Contraseñas de modo EXEC privilegiado y de línea
- Direccionamiento IP correcto, según Addressing Table

Paso 3: Jugador del lado servidor: Configurar el enlace PTMU y comunicar el direccionamiento

a. Complete los pasos necesarios para verificar que el **enlace PTMU** esté listo para recibir una conexión entrante.

b. Comunique la información de configuración necesaria al jugador del lado cliente.

Paso 4: Jugador del lado cliente: Configurar la conexión multiusuario saliente

a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor:

   Dirección IP: _____

   Número de puerto: _____

   Contraseña (**cisco**, de manera predeterminada) _____

b. Configure **Peer0** para conectarse al **enlace PTMU** del jugador del lado servidor.

c. Conecte la **GigabitEthernet1/1** de **S2** al **Link0** en **Peer0**.

Paso 5: Verificar la conectividad a través de una conexión multiusuario local

a. El jugador del lado servidor debe poder hacer ping al S2 en la instancia de Packet Tracer del jugador del lado cliente.

b. El jugador del lado cliente debe poder hacer ping al S1 en la instancia de Packet Tracer del jugador del lado servidor.

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Paso 1: Configurar WRS como servidor de DHCP

WRS proporciona servicios de DHCP. Establezca los siguientes parámetros para la configuración del servidor de DHCP:

- La dirección IP de inicio es **172.16.1.11**.
- La cantidad máxima de usuarios es **100**.
- El **DNS 1 estático** es **172.16.1.5**.
- Verifique si **NetAdmin** recibió el direccionamiento IP mediante DHCP.
- En **NetAdmin**, acceda a la página Web User Account Information (Información de cuenta de usuario) en **172.16.1.5**. Utilizará esta información para configurar las cuentas de usuario en el paso 2.

Paso 2: Configurar servicios en www.ptmu.test

El servidor **www.ptmu.test** proporciona el resto de los servicios y se debe configurar con lo siguiente:

- Un registro DNS que asocie la dirección IP del servidor **www.ptmu.test** al nombre www.ptmu.test.
- Cuentas de usuario y servicios de correo electrónico según la lista de usuarios. El nombre de dominio es **ptmu.test.**
- Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.

Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos

En **NetAdmin**, realice lo siguiente:

- Configure el cliente de correo electrónico para la cuenta de usuario de NetAdmin.
- Envíe un correo electrónico al usuario de la **PC1**.
- Suba el archivo **secret.txt** al servidor FTP. No modifique el archivo.

  Nota: la puntuación para el jugador del lado servidor será de **43/44** hasta que el jugador del lado cliente descargue correctamente el archivo **secret.txt**, lo modifique y lo suba al servidor FTP **www.ptmu.test**.

Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Paso 1: Configurar y verificar el direccionamiento de las PC

a. Configure la **PC1** y **la PC2** para obtener el direccionamiento automáticamente.

b. Las PC1 y PC2 deben poder acceder a la página Web **http://www.ptmu.test**.

Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

a. Configure las cuentas de correo electrónico según los requisitos que se indican en **www.ptmu.test/user.html**.

b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta.

c. Envíe un correo electrónico de la PC1 a la PC2. **Nota:** la puntuación no cambiará.

d. Verifique si la PC2 recibió un correo electrónico de la PC1.

Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

a. En la PC2, acceda al servidor FTP y descargue el archivo **secret.txt**.

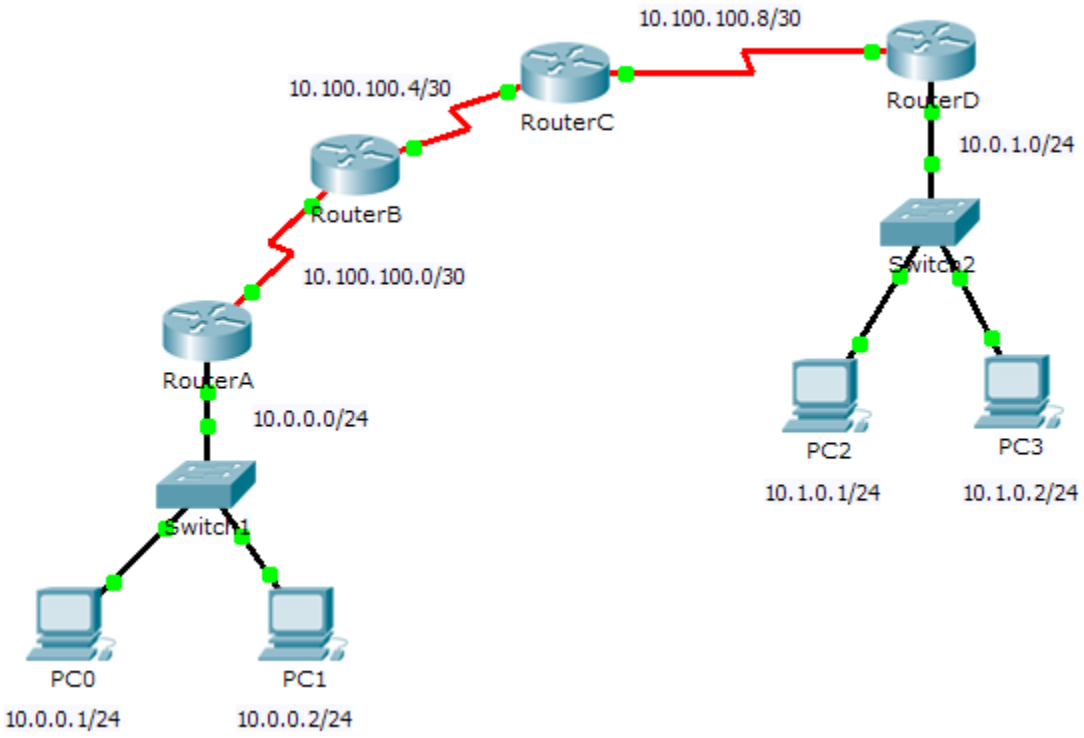
b. Abra el archivo **secret.txt**, solo cambie la palabra secreta por **apple** y suba el archivo.

c. La puntuación del jugador del lado servidor debería ser **44/44** y la del jugador del lado cliente debería ser **33/33**.

Packet Tracer: Prueba de la conectividad con traceroute (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Parte 2: Comparar con el comando traceroute en un router

Información básica

Esta actividad está diseñada para ayudarlo a llevar a cabo la resolución de problemas de conectividad de red utilizando comandos para rastrear la ruta de origen a destino. Debe examinar el resultado de **tracert** (el comando de Windows) y **traceroute** (el comando de IOS) mientras los paquetes atraviesan la red y determinar la causa de un problema de red. Una vez que se corrija el problema, utilice los comandos **tracert** y **traceroute** para verificar la finalización.

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Paso 1: Enviar un ping de un extremo al otro de la red

Haga clic en **PC1** y abra el **símbolo del sistema**. Haga ping a **PC3** en **10.1.0.2**. ¿Qué mensaje se muestra como resultado del ping? Host de destino inalcanzable.

Paso 2: Rastrear la ruta de PC1 para determinar dónde falla la conectividad

a. En el **símbolo del sistema** de la **PC1**, introduzca el comando **tracert 10.1.0.2**.

b. Cuando reciba el mensaje **Request timed out** (Tiempo de espera agotado), presione **Ctrl**+**C**. ¿Cuál fue la primera dirección IP indicada en el resultado del comando **tracert**? 10.0.0.254, la dirección de gateway de la PC.

c. Observe los resultados del comando **tracert**. ¿Cuál es la última dirección que se alcanzó con el comando **tracert**? 10.100.100.6

Paso 3: Corregir el problema de red

a. Compare la última dirección que se alcanzó con el comando **tracert** con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de falla. ¿Qué dispositivos tienen direcciones configuradas para la red donde ocurrió la falla? El RouterB y el RouterC.

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

c. ¿Cuál es el estado de las interfaces? Parecen estar activas.

d. Compare las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo común? La interfaz serial 0/0/0 tiene una dirección IP incorrecta según la topología.

e. Realice los cambios necesarios para restaurar la conectividad, pero no modifique las subredes. ¿Cuál es la solución? Cambiar la dirección IP de la S0/0/0 a 10.100.100.9/30.

Paso 4: Verificar que la conectividad de extremo a extremo esté establecida

a. En el **símbolo del sistema de la PC1**, introduzca el comando **tracert 10.1.0.2**.

b. Observe el resultado del comando **tracert**. ¿El comando funcionó correctamente? Sí

Parte 2: Comparar con el comando traceroute en un router

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

b. Introduzca el comando **traceroute 10.1.0.2**. ¿El comando se completó correctamente? Sí

c. Compare el resultado del comando **traceroute** del router con el del comando **tracert** de la PC. ¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió? El router tiene una dirección IP menos, porque el próximo dispositivo que utilizará en la ruta será el RouterB.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Probar la conectividad de extremo a extremo con el comando **tracert**	Paso 1	10	
	Paso 2b	10	
	Paso 2c	10	
	Paso 3a	10	
	Paso 3c	10	
	Paso 3d	10	
	Paso 3e	10	
	Paso 4b	10	
Total de la parte 1		**80**	
Parte 2: Comparar con el comando **traceroute** en un router	a	10	
	b	10	
Total de la parte 2		**20**	
Puntuación total		**100**	

Packet Tracer: Uso de los comandos show (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Analizar el resultado del comando show

Parte 2: Preguntas de reflexión

Información básica

Esta actividad está diseñada para reforzar el uso de los comandos **show** del router. No debe realizar configuraciones, sino examinar el resultado de diversos comandos **show**.

Parte 1: Analizar el resultado del comando show

Paso 1: Conectarse a ISPRouter

a. Haga clic en **PC ISP** y, a continuación, en la ficha **Desktop** (Escritorio), seguida de **Terminal**.

b. Ingrese al modo EXEC privilegiado.

c. Use los siguientes comandos **show** para contestar las preguntas de reflexión en la parte 2:

```
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version
```

Parte 2: Preguntas de reflexión

1. ¿Qué comandos proporcionarían la dirección IP, el prefijo de red y la interfaz? show ip route, show interfaces, show protocols (antes de IOS 15, el comando show ip route no mostraba la dirección IP de las interfaces).
2. ¿Qué comandos proporcionan la dirección IP y la asignación de interfaces, pero no el prefijo de red? show ip interface brief
3. ¿Qué comandos proporcionan el estado de las interfaces? show interfaces, show ip interface brief.
4. ¿Qué comandos proporcionan información sobre el IOS que se encuentra cargado en el router? show flash, show version.
5. ¿Qué comandos proporcionan información sobre las direcciones de las interfaces del router? show arp, show interfaces
6. ¿Qué comandos proporcionan información sobre la cantidad de memoria flash disponible? show version
7. ¿Qué comandos proporcionan información sobre las líneas que se utilizan para propósitos de control de dispositivos o de configuración? show users
8. ¿Qué comandos proporcionan estadísticas de tráfico de las interfaces del router? show interfaces

9. ¿Qué comandos proporcionan información sobre las rutas disponibles para el tráfico de la red? show ip route
10. ¿Qué interfaces están activas actualmente en el router? GigabitEthernet 0/0, Serial 0/0/1.

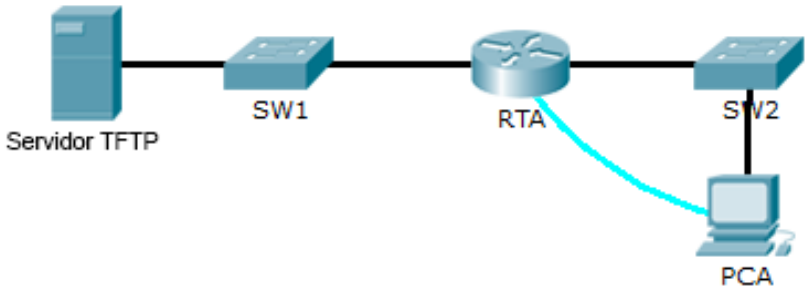
Tabla de calificación sugerida

Cada pregunta vale 10 puntos, para obtener una puntuación total de 100.

Packet Tracer: Realización de copias de seguridad de archivos de configuración (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Establecer la conectividad al servidor TFTP

Parte 2: Transferir la configuración del servidor TFTP

Parte 3: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP

Información básica/Situación

Esta actividad está diseñada para mostrar cómo restaurar una configuración a partir de una copia de seguridad y, luego, realizar una nueva copia de seguridad. Debido a una falla del equipo, se colocó un router nuevo. Afortunadamente, los archivos de configuración de respaldo se guardaron en un servidor de protocolo TFTP (Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos). Debe restaurar los archivos del servidor TFTP para que el router vuelva a estar en línea con el menor tiempo de inactividad posible.

Parte 1: Establecer la conectividad al servidor TFTP

Nota: debido a que es un router nuevo, la configuración inicial se realizará mediante una conexión de consola al router.

a. Haga clic en **PCA**, después en la ficha **Desktop** (Escritorio) y, a continuación, en **Terminal** para acceder a la línea de comandos **RTA**.

b. Configure y active la interfaz **Gigabit Ethernet 0/0**. La dirección IP debe coincidir con el gateway predeterminado para el **servidor TFTP**.

c. Pruebe la conectividad al **servidor TFTP**. Si es necesario, lleve a cabo la resolución de problemas.

Parte 2: Transferir la configuración del servidor TFTP

a. Emita el siguiente comando desde el modo EXEC privilegiado:

```
Router# copy tftp running-config
Address or name of remote host []? 172.16.1.2
```

```
Source filename []? RTA-confg
Destination filename [running-config]? <cr>
```

El router debe devolver lo siguiente:

```
Accessing tftp://172.16.1.2/RTA-confg...
Loading RTA-confg from 172.16.1.2: !
[OK - 785 bytes]
785 bytes copied in 0 secs
RTA#
%SYS-5-CONFIG_I: Configured from console by console
RTA#
```

b. Emita el comando para visualizar la configuración actual. ¿Qué cambios se realizaron? La configuración almacenada en el servidor TFTP se cargó en el router.

c. Emita el comando **show** adecuado para mostrar el estado de la interfaz. ¿Todas las interfaces están activas? No, la interfaz Gi0/1 está inactiva administrativamente. Todas las interfaces del router están desactivadas de manera predeterminada.

d. Corrija cualquier problema relacionado con las interfaces y pruebe la conectividad.

Parte 3: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP

a. Cambie el nombre de host **RTA** a **RTA-1**.

b. Guarde la configuración en la NVRAM.

c. Copie la configuración al **servidor TFTP** con el comando **copy**:

```
RTA-1# copy running-config tftp:
Address or name of remote host []? 172.16.1.2
Destination filename [RTA-1-confg]? <cr>
```

d. Emita el comando para mostrar los archivos ubicados en la memoria flash.

e. Copie el IOS que está en la memoria flash al **servidor TFTP** con el siguiente comando:

```
RTA-1# copy flash tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? <cr>
```

Packet Tracer: Configuración de un router Linksys

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Objetivos

Parte 1: Conectar al router Linksys

Parte 2: Habilitar conectividad inalámbrica

Parte 3: Configurar y verificar el acceso al cliente inalámbrico

Información básica

En esta actividad, configurará un router inalámbrico Linksys, lo que permite el acceso remoto a los clientes inalámbricos así como conectividad con seguridad WPA.

Parte 1: Conectar al router Linksys

Paso 1: Establecer y verificar la conectividad al router Linksys

a. Conecte el cable adecuado del **Host-A** al puerto Ethernet 1 en **Linksys**.

b. Espere a que la luz de enlace se vuelva de color verde. A continuación, abra el símbolo del sistema para el **Host-A**. Utilice el comando **ipconfig** para verificar la información de direccionamiento IP del **Host recibido**.

c. Introduzca el comando **ping 192.168.0.1** para verificar que el **Host-A** pueda acceder al gateway predeterminado.

Paso 2: Acceda a la interfaz gráfica de usuario (GUI) de Linksys mediante un explorador Web.

a. Para configurar el router **Linksys** con la GUI, debe acceder a este mediante el explorador Web del **Host-A**. Abra el explorador Web y escriba la dirección de gateway predeterminado en el campo de dirección URL para acceder a **Linksys**.

b. Introduzca **admin** como nombre de usuario y contraseña predeterminados para acceder al router **Linksys**.

Nota: no podrá ver el cambio en la puntuación al configurar el router **Linksys** hasta que haya hecho clic en **Save Settings** (Guardar configuración).

Parte 2: Habilitar conectividad inalámbrica

Paso 1: Configure el router Linksys para que tenga conectividad a Internet.

En esta situación no hay conectividad a Internet, pero de todas formas configurará los parámetros para la interfaz con conexión a Internet. Para **Internet Connection Type** (Tipo de conexión a Internet), elija **Static IP** (IP estática) en la lista desplegable. A continuación, introduzca la siguiente información de IP estática:

- Dirección IP de Internet: **198.133.219.1**
- Máscara de subred: **255.255.255.0**
- Gateway predeterminado: **198.133.219.254**
- DNS 1: **198.133.219.10**

Paso 2: Configure los parámetros de red internos.

Desplácese hasta la sección **Network Setup** (Configuración de red) y configure la siguiente información:

- Dirección IP: **172.31.1.1**
- Máscara de subred: **255.255.255.224**
- Dirección IP de inicio: introduzca **5** para el último octeto.
- Cantidad máxima de usuarios: **25**

Nota: el rango de direcciones IP del pool de DHCP solo refleja los cambios una vez que hace clic en **Save Settings**.

Paso 3: Guardar la configuración y volver a conectarse al router Linksys

a. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**. Si pasa de una ficha a otra sin guardar la configuración, esta se perderá.

b. Cuando hace clic en **Save Settings**, se pierde la conexión. Esto ocurre porque cambió la dirección IP del router.

c. Regrese al símbolo del sistema del **Host-A**. Introduzca el comando **ipconfig /renew** para renovar la dirección IP.

d. Utilice el explorador Web del **Host-A** para volver a conectarse al router **Linksys**. Deberá utilizar la nueva dirección de gateway predeterminado. Verifique la configuración de **Internet Connection** (Conexión a Internet) en la ficha **Status** (Estado). La configuración debe coincidir con los valores que configuró en el paso 1 de la parte 2. Si no coinciden, repita los pasos 1 y 2 de la parte 2.

Paso 4: Configurar la conectividad inalámbrica de los dispositivos inalámbricos

a. Haga clic en la ficha **Wireless** (Conexión inalámbrica) e investigue las opciones de la lista desplegable de **Network Mode** (Modo de red).

¿En qué caso elegiría la opción **Disable** (Deshabilitar)? Cuando no hay dispositivos inalámbricos.

¿En qué caso elegiría la opción **Mixed** (Combinada)? Cuando hay dispositivos inalámbricos que constan de B, G o N.

b. Configure el modo de red en **Wireless-N Only** (Solo Wireless-N).

c. Cambie el SSID a **MiRedDoméstica.**

¿Cuáles son dos características de un SSID? Distingue mayúsculas de minúsculas y el nombre no puede exceder los 32 caracteres.

d. Cuando un cliente inalámbrico busca redes inalámbricas en el área, este detecta cualquier transmisión del SSID. Las transmisiones del SSID están habilitadas de manera predeterminada.

Si no se transmite el SSID de un punto de acceso, ¿cómo se conectan los dispositivos a este? El cliente debe estar configurado con el nombre, el cual debe estar bien escrito para que se lleve a cabo la conexión.

e. Para obtener el mejor rendimiento de una red que utiliza Wireless-N, configure la banda de radio en **Wide-40MHz** (40 MHz de ancho).

f. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 5: Configure la seguridad inalámbrica de modo que los clientes deban autenticarse para poder conectarse a la red inalámbrica.

a. Haga clic en la opción **Wireless Security** (Seguridad inalámbrica) en la ficha **Wireless**.

b. Configure el **Security Mode** (Modo de seguridad) en **WPA2 Personal**.

¿Cuál es la diferencia entre la opción Personal y la opción Enterprise (Empresa)? La opción Enterprise utiliza un servidor Radius para autenticar a los usuarios, mientras que el modo Personal utiliza el router Linksys para autenticar usuarios.

c. Deje el modo de encriptación en AES y establezca la frase de contraseña **itsasecret**.

d. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 6: Cambie la contraseña predeterminada para acceder a la configuración del router Linksys.

a. Siempre debe cambiar la contraseña predeterminada. Haga clic en la ficha **Administration** (Administración) y cambie la contraseña de **Router Access** (Acceso al router) por **letmein**.

b. Haga clic en **Save Settings**. Introduzca el nombre de usuario **admin** y la nueva contraseña.

Parte 3: Configurar y verificar el acceso al cliente inalámbrico

Paso 1: Configurar la computadora portátil para acceder a la red inalámbrica

a. Haga clic en **Laptop** (Computadora portátil) y después en **Desktop** > **PC Wireless** (PC inalámbrica). La ventana que se abre es la GUI de Linksys del cliente.

b. Haga clic en la ficha **Connect** (Conectar) y después en **Refresh** (Actualizar), si es necesario. Debería ver la red **MiRedDoméstica** indicada en Wireless Network Name (Nombre de red inalámbrica).

c. Haga clic en **MiRedDoméstica** y después en **Connect**.

d. Ahora debería ver la red **MiRedDoméstica**. Haga clic en esta y después en **Connect**.

e. La **Pre-shared Key** (Clave previamente compartida) es la contraseña que configuró en el paso 5c de la parte 2. Introduzca la contraseña y haga clic en **Connect**.

f. Cierre la GUI de Linksys y haga clic en **Command Prompt** (Símbolo del sistema). Introduzca el comando **ipconfig** para verificar si **Laptop** recibió el direccionamiento IP.

Paso 2: Verificar la conectividad entre la computadora portátil y el Host-A

a. Haga ping al router **Linksys** desde la **computadora portátil**.

b. Haga ping desde el **Host-A** a la **computadora portátil.**

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Habilitar conectividad inalámbrica	Paso 4	4	
	Paso 5	1	
Total de la parte 2		**5**	
Puntuación de Packet Tracer		**95**	
Puntuación total		**100**	

Packet Tracer: Reto de habilidades de integración

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

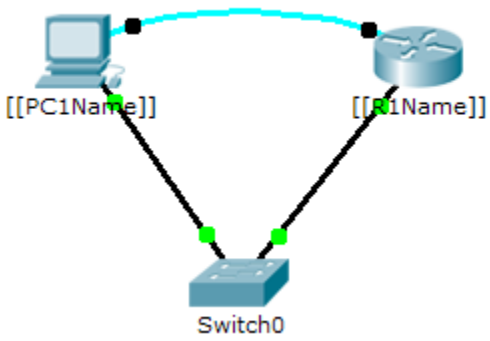


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
[[R1Name]]	G0/0	[[R1Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0

Situación

El administrador de red le solicitó que prepare un router para la implementación. Antes de que pueda conectarse a la red, se deben habilitar las medidas de seguridad. En esta actividad, encriptará y configurará contraseñas seguras. A continuación, configurará SSH para obtener acceso remoto y demostrará que puede acceder al router desde una PC.

Requisitos

- Configure el direccionamiento IP en **[[PC1Name]]** y **[[R1Name]]**.
- Configure el nombre de host como **[[R1Name]]** y encripte todas las contraseñas de texto no cifrado.
- Establezca la contraseña secreta segura que desee.
- Establezca el nombre de dominio en **[[R1Name]]** (distinguir mayúsculas de minúsculas).

```
[[R1Name]](config)# ip domain-name [[R1Name]]
```

- Cree un usuario de su elección con una contraseña segura.

```
[[R1Name]](config)# user any_user password any_password
```

- Genere claves RSA de 1024 bits.

  Nota: en Packet Tracer, introduzca el comando **crypto key generate rsa** y presione tecla **Entrar** para continuar.

```
[[R1Name]](config)# crypto key generate rsa
```

```
The name for the keys will be: [[R1Name]].[[R1Name]]
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

- Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

```
[[R1Name]](config)# login block-for 180 attempts 4 within 120
```

- Configure las líneas vty para el acceso por SSH y solicite los perfiles de usuarios locales.

```
[[R1Name]](config-line)# transport input ssh
[[R1Name]](config-line)# login local
```

- Guardar la configuración en la NVRAM.
- Esté preparado para demostrar al instructor que estableció el acceso por SSH de **[[PC1Name]]** a **[[R1Name]]**.

ID: [[indexAdds] [[indexNames]]]