Cisco | Networking Academy®
Mind Wide Open™

Switching y routing CCNA: Conexión de redes

Manual de prácticas de laboratorio para el instructor

Jerarquía de diseño (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.

Objetivo

Identificar las tres capas de una red jerárquica y cómo se utilizan en el diseño de red.

(Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños).

Situación

A un administrador de red se le asigna la tarea de diseñar una red ampliada para la empresa.

Después de hablar con los administradores de red de otras sucursales de la empresa, se decidió utilizar el modelo de diseño de red jerárquico de tres capas de Cisco para orientar la expansión. Este modelo se eligió debido a su influencia simple en la planificación de la red.

Las tres capas del diseño de la red ampliada incluyen lo siguiente:

- Acceso
- Distribución
- Núcleo

Recursos

- Acceso a la World Wide Web
- Software de presentación

Paso 1: Utilizar Internet para investigar el modelo de diseño de tres capas de Cisco solo con imágenes.

a. Busque dos imágenes que muestren el modelo de diseño jerárquico de tres capas.

b. Anote la dirección web de la imagen en línea.

Paso 2: Analizar las dos imágenes que seleccionó en el paso 1.

a. Observe los tipos de equipos en cada capa de los diseños que eligió.

b. Diferencie por qué se supone que los tipos de equipos que se muestran en las imágenes se encuentran en determinado lugar del diseño.

c. Observe cualquier otra diferencia entre las imágenes seleccionadas.

   1) Cantidad de dispositivos que se utilizan dentro de las capas

   2) Redundancia, si la hubiera

Paso 3: Crear una presentación de tres diapositivas que incluya lo siguiente:

a. Los dos diseños que se eligieron con hipervínculos a las ubicaciones del sitio de Internet.

b. Una explicación en cada diapositiva sobre por qué se eligió la imagen.

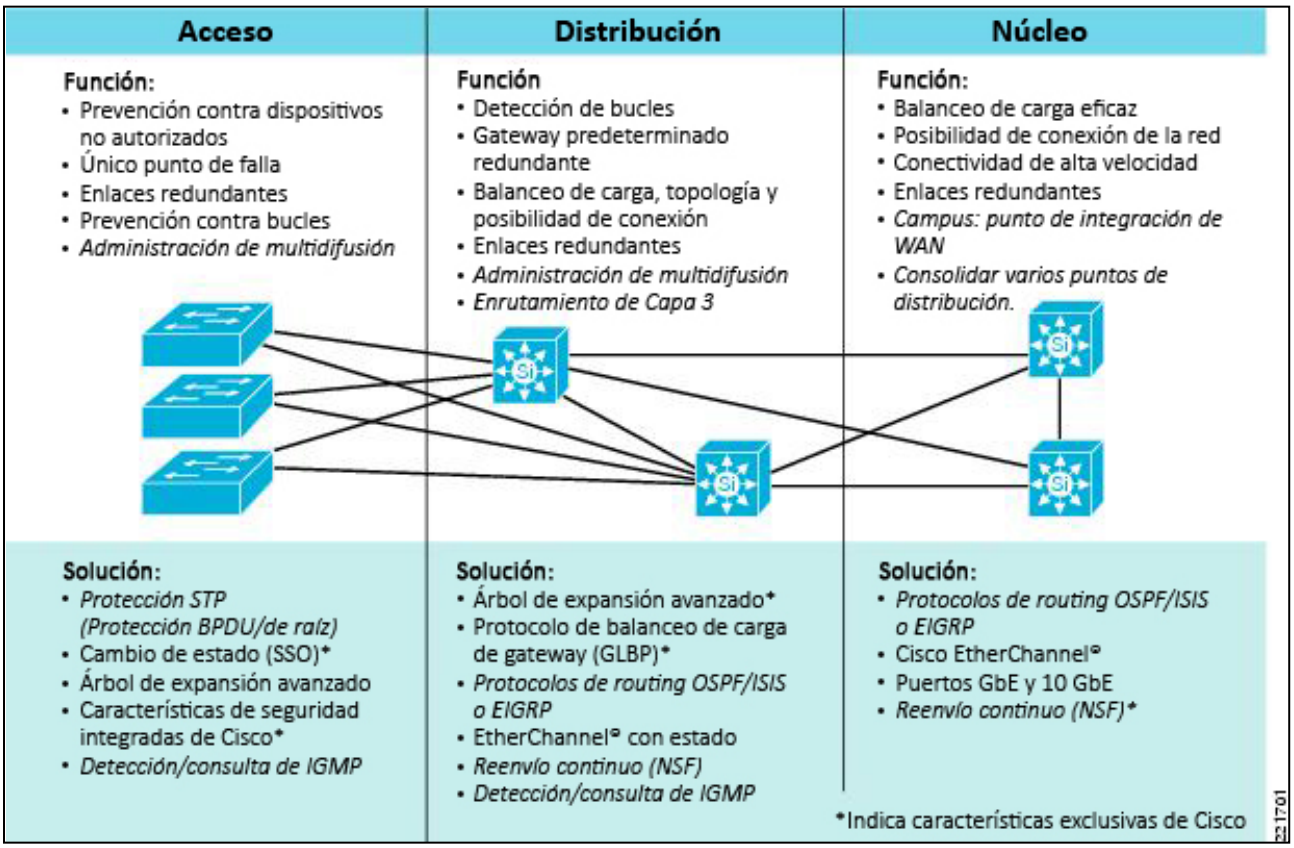
c. Comparaciones con respecto a las diferencias entre las dos imágenes, pero con una explicación de por qué se clasifican como diseños jerárquicos de tres niveles.

Paso 4: Presentar las diapositivas a un compañero, a otro grupo o a la clase para su análisis.

Ejemplo sugerido para la actividad (no se proporcionan números de modelo, ya que el énfasis está en las funciones jerárquicas de los dispositivos de red que se muestran):

Diapositiva 1:

Gráfico 1

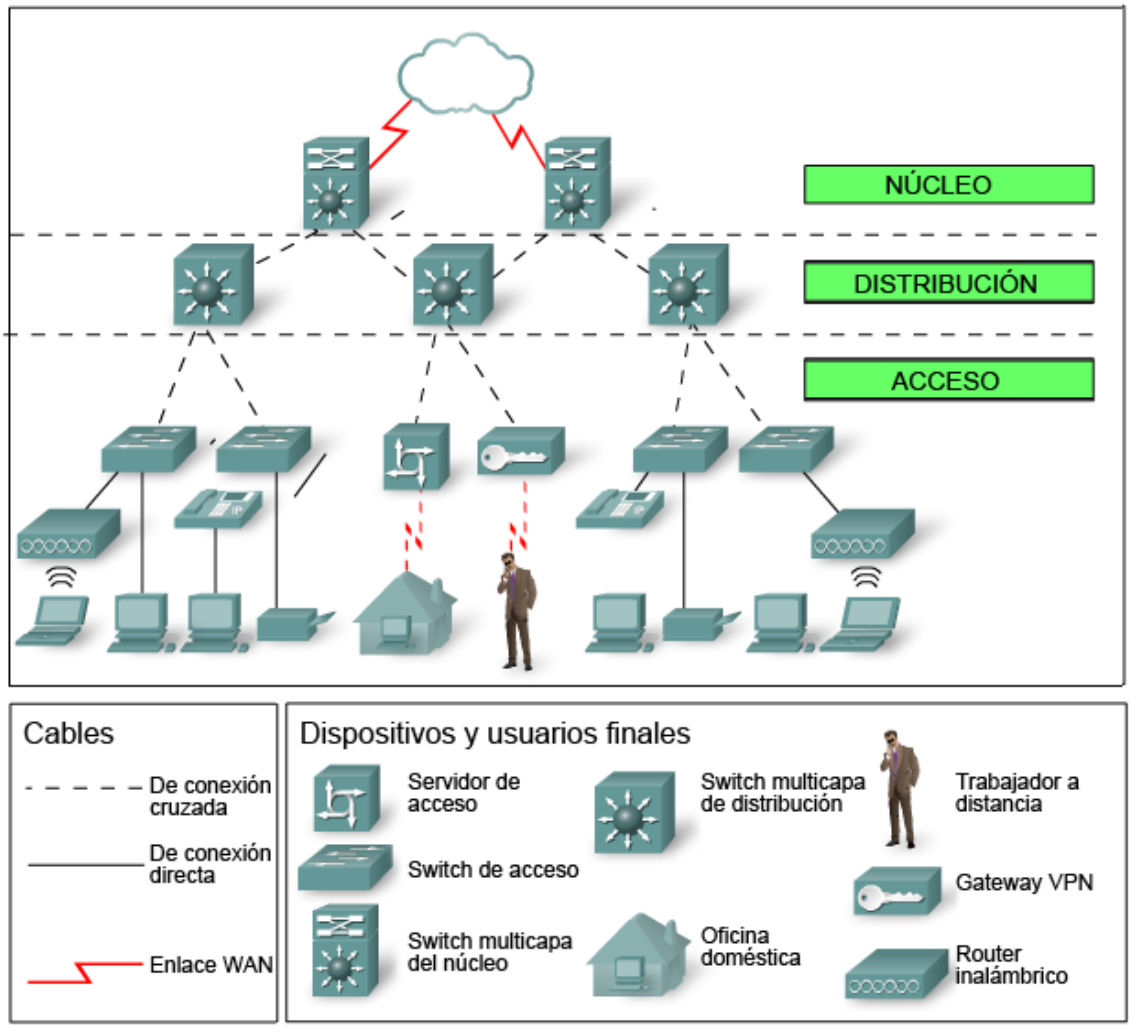


Notas del estudiante o del grupo acerca de por qué se eligió este gráfico:

- En la capa de acceso, se muestran los switches básicos, las opciones del árbol de expansión, la redundancia a la capa de distribución y las consideraciones de seguridad.
- En la capa de distribución, se muestra la redundancia, el balanceo de carga y los protocolos de routing vinculados a la capa de núcleo.
- En la capa de núcleo, se muestra el balanceo de carga, la redundancia, los protocolos de routing y la agregación de puertos.

Diapositiva 2:

Gráfico 2



Notas del estudiante o del grupo acerca de por qué se eligió este gráfico:

- En la capa de acceso, se muestran las computadoras, los switches de acceso, los gateways VPN, las impresoras, el trabajador a distancia, la oficina doméstica y el router inalámbrico. En esta capa, también se muestran los enlaces redundantes a la capa de distribución.
- En la capa de distribución, se muestran varios switches multicapa y conexiones de enlace a la capa de núcleo.
- En la capa de núcleo, se muestran los switches multicapa y las conexiones a la capa de distribución y a la nube.

Diapositiva 3:

- Los tipos de equipos básicos se ubican en la capa de acceso, más cerca del usuario, y funcionan con la capa de distribución que está por encima de la capa de acceso. La mayoría de los dispositivos de red se ubican en este nivel en ambas imágenes.

- El equipo de la capa de distribución interactúa con las capas de núcleo y de acceso en ambas imágenes. Este nivel jerárquico parece contener el equipo más sofisticado y con más funciones. La redundancia es claramente evidente para las capas de núcleo y de acceso, como se muestra en el primer modelo. Parece que los switches multifunción de gran potencia se ubican en este nivel de los dos gráficos. La cantidad de dispositivos de red que se muestran en ambos gráficos en este nivel es más pequeña que la de la capa de acceso, pero más grande que la de la capa de núcleo.
- Como se muestra en los dos gráficos anteriores, la capa de núcleo tiene el equipo más sofisticado. Hay menos dispositivos de red en esta capa, lo que parece indicar que los dispositivos tienen una alta funcionalidad como procesadores de tráfico rápidos.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Niveles del modelo de diseño jerárquico de Cisco
  - Acceso
  - Distribución
  - Núcleo
- Funciones del modelo de diseño jerárquico de Cisco
- Tipos de equipos ubicados en las capas de la jerarquía
- Cantidad de equipos ubicados en las capas de la jerarquía

Innovaciones sin fronteras: en todas partes (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.

Objetivo

Describir los componentes de las redes sin fronteras.

Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños o grandes.

Situación

Usted es el administrador de red de su pequeña o mediana empresa. Se interesa por los servicios de red sin fronteras mientras hace planes para el futuro de la red.

Mientras planifica las políticas y los servicios de red, se da cuenta de que las redes cableadas e inalámbricas requieren capacidad de administración y un diseño de implementación.

Por consiguiente, esto lo lleva a considerar los siguientes servicios sin fronteras de Cisco como opciones posibles para su empresa:

- Seguridad: ***TrustSec***
- Movilidad: ***Motion***
- Rendimiento de las aplicaciones: ***App Velocity***
- Rendimiento multimedia: ***Medianet***
- Administración de la energía: ***EnergyWise***

Recursos

- Acceso a la World Wide Web
- Software de presentación o de procesamiento de texto

Instrucciones

Paso 1: Seleccione tres servicios de red sin fronteras de Cisco que le interesen de la siguiente lista:

- Seguridad: ***TrustSec***
- Movilidad: ***Motion***
- Rendimiento de las aplicaciones: ***App Velocity***
- Rendimiento multimedia: ***Medianet***
- Administración de la energía: ***EnergyWise***

Paso 2: Investigue las tres selecciones mediante el uso de Internet. Busque presentaciones cortas de video y diversos sitios web de los tres servicios de red sin fronteras que seleccionó. Tome notas durante la investigación:

a. Sobre la base de la investigación realizada, cree una definición básica de cada servicio de red sin fronteras.

b. Indique, por lo menos, tres áreas de asistencia que ofrece cada servicio de red sin fronteras a los administradores de red.

Paso 3: Prepare una matriz informativa que indique los tres servicios de red sin fronteras que seleccionó. Incluya las notas sobre los videos que completó en los pasos 2a y b.

Paso 4: Comparta su matriz con otro estudiante, con el grupo o con toda la clase.

Nota: mientras los estudiantes escuchan las presentaciones grupales, pueden tomar notas y entregarlas al instructor.

Ejemplo sugerido de la actividad (los diseños de los estudiantes varían):

Servicio de red sin fronteras	Definición básica	Servicios de red sin fronteras ofrecidos
Seguridad: ***TrustSec*** The Power of Cisco ISE	Un servicio red sin fronteras integral que se centra en la seguridad para redes cableadas e inalámbricas.	Administración de seguridad centralizada. Opciones para la implementación de políticas de administración de seguridad. Proporciona un registro de infracciones de seguridad, tanto actuales como antiguas. Es transparente para los usuarios. Cisco Identity Services Engine
Movilidad: ***Motion*** Cisco Data In Motion	Un servicio de red sin fronteras que permite que los administradores de red recopilen datos de sensores, dispositivos móviles y cámaras de video para ayudarlos a tomar decisiones y a comunicarse en tiempo real.	Conecta los datos sin fronteras de IoE desde plantas de fabricación, redes de energía, instalaciones para la salud y sistemas de transporte. Consolida los datos para ayudar a los clientes a mejorar las operaciones de datos y, al mismo tiempo, ahorrar tiempo y dinero valiosos. Ayuda a las empresas a compartir datos y a fundamentar una propuesta empresarial de cambio. Datos en movimiento
Rendimiento de las aplicaciones: ***App Velocity*** Application Velocity	Un servicio de red sin fronteras que utiliza sistemas de distribución basados en aplicaciones para mejorar las comunicaciones entre las empresas y los clientes.	Proporciona servicios de traducción de idiomas en tiempo real. Permite que las empresas utilicen aplicaciones de red para compartir investigaciones y comunicarse nuevas ideas.

		Centraliza las aplicaciones de red para simplificar la entrega y la administración, lo que reduce los costos operativos. Application Performance Management Service
Rendimiento multimedia: ***Medianet*** Video-ready Network with Cisco MediaNet	Un servicio de red sin fronteras que facilita la configuración por cable e inalámbrica, el control de los medios y las operaciones multimedia de bajo costo.	Realiza un seguimiento del tráfico multimedia que fluye en la red. Ayuda a reducir los costos operativos mediante la rápida resolución de problemas de los servicios de video, de voz y de datos. Permite la evaluación precisa del impacto que tienen los servicios de video, de voz y de datos en la red. Arquitectura Medianet
Administración de la energía: ***EnergyWise*** Lights Out - Cisco EnergyWise	Un servicio de red sin fronteras que reduce los costos de energía mediante dispositivos conectados por cable e inalámbricos.	Permite las comunicaciones en tiempo real en todo el mundo mediante sistemas de distribución con dispositivos conectados por cable e inalámbricos. Ahorra costos de energía al entregar información de forma rápida y eficaz. Ahorra energía y tiempo al implementar servicios de red en lugar de recurrir a esfuerzos colectivos de recursos humanos. Video de Borderless Networks

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Servicios de red sin fronteras
  - Seguridad: TrustSec
  - Movilidad: Motion
  - Rendimiento de las aplicaciones: App Velocity
  - Rendimiento multimedia: Medianet
  - Administración de la energía: EnergyWise
- Planificación de estrategias de políticas para los servicios de red sin fronteras

Sucursales (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.

Objetivo

Describir las tecnologías de acceso WAN disponibles para las redes de pequeñas o medianas empresas.

Nota para el instructor:

- Esta actividad se puede completar de manera individual o en grupos pequeños; luego, se puede compartir y analizar con otro grupo de estudiantes, con toda la clase o con el instructor.
- En este punto del currículo, los estudiantes deben aprender que existen diferentes tipos de equipos de red más adecuados a los distintos tamaños de las redes, y no qué modelos específicos de equipos se deben considerar para la compra.

Situación

Su empresa mediana abre una nueva sucursal para prestar servicios a una red basada en el cliente más amplia. Esta sucursal se centra en operaciones de red cotidianas comunes, pero también proporcionará TelePresence, conferencias web, telefonía IP, video a petición y servicios inalámbricos.

Aunque sabe que un ISP puede proporcionar los routers y switches WAN para admitir la conectividad a la red para la sucursal, prefiere utilizar su propio equipo local del cliente (CPE). Para garantizar la interoperabilidad, se utilizaron dispositivos de Cisco en las demás WAN de sucursales.

Como administrador de red de la sucursal, tiene la responsabilidad de investigar los posibles dispositivos de red que se pueden comprar y utilizar para la WAN.

Recursos

- World Wide Web
- Software de procesamiento de texto

Instrucciones

Paso 1: Visite el sitio Cisco Branch-WAN Business Calculator (Calculadora empresarial de WAN para sucursales). Acepte el acuerdo para usar la calculadora.

Paso 2: Introduzca datos para ayudar a la calculadora a determinar qué router u opción de ISR se recomienda para la sucursal y la WAN (ambas).

Nota: hay una herramienta de barra deslizable dentro de la ventana de la calculadora que permite elegir más opciones de servicio para la sucursal y la WAN.

Paso 3: La calculadora sugerirá una solución de router o de dispositivo ISR posible para la sucursal y la WAN. Para ver el resultado, use las fichas en la parte superior de la ventana de la calculadora.

Paso 4: Cree una matriz con tres encabezados de columnas e incluya parte de la información proporcionada por el resultado en cada categoría:

- Rendimiento de la inversión (ROI)
- Costo total de propiedad (TCO)

- Ahorro de energía

Paso 5: Analice la investigación con un compañero, un grupo, la clase o el instructor. En el análisis, incluya lo siguiente:

- Datos específicos sobre los requisitos de la red que se usó como datos de entrada para la calculadora
- Datos de resultados de la matriz
- Factores adicionales que consideraría antes de comprar un router o un ISR para una nueva sucursal

Solución de ejemplo sugerida para la actividad:

Notas para el instructor: (la información variará para cada grupo, según la información especificada de la calculadora)

Routers o ISR sugeridos para la sucursal y la oficina de la WAN: _____

Rendimiento de la inversión	Total Cost of Ownership, costo total de propiedad	Ahorro de energía
(las notas de los resultados variarán por grupo, según las consideraciones y los servicios WAN especificados)		

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Ubicaciones y tamaños de WAN
- Dispositivos usados en la WAN
- Costo de propiedad para dispositivos CPE de la WAN
- Ahorro de energía de WAN (tecnología ecológica)

Práctica de laboratorio: Investigación de las tecnologías WAN (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: Investigar las tecnologías WAN dedicadas y sus proveedores

Parte 2: Investigar un proveedor de servicios de línea arrendada dedicada en su área

Información básica/situación

Los servicios de Internet de banda ancha actuales son rápidos, accesibles y seguros mediante las tecnologías VPN. Sin embargo, muchas empresas aún necesitan una conexión dedicada a Internet las 24 horas o una conexión dedicada punto a punto de una oficina a otra. En esta práctica de laboratorio, investigará el costo y la disponibilidad para la compra de una conexión dedicada a Internet T1 para su hogar o empresa.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Investigar las tecnologías WAN dedicadas y sus proveedores

En la parte 1, investigará las características básicas de las tecnologías WAN dedicadas y, en el paso 2, descubrirá los proveedores que ofrecen servicios WAN dedicados.

Paso 1: Investigar las características de la tecnología WAN.

Use los motores de búsqueda y los sitios web para investigar las siguientes tecnologías WAN y completar la tabla que se incluye a continuación.

Tecnología WAN	Conexión dedicada (sí/no)	Medios de última milla			Velocidad/alcance
		Cobre (sí/no)	Fibra (sí/no)	Tecnología inalámbrica (sí/no)	
T1/DS1	sí	sí	sí	sí	1.544 Mbps
T3/DS3	sí	sí	sí	sí	44.736 Mbps
OC3 (SONET)	sí	no	sí	no	155.52 Mb/s
Frame Relay	sí	sí	sí	sí	56 Kb/s a 1,544 Mb/s
ATM	sí	sí	sí	sí	155 Mb/s a 622 Mb/s
MPLS	sí	sí	sí	sí	Hasta 10 Gb/s
EPL (línea privada de Ethernet)	sí	sí	sí	no	Hasta 10 Gb/s

Paso 2: Descubrir proveedores de servicios de tecnología WAN dedicada.

Navegue hasta http://www.telarus.com/carriers.html. En esta página web, se incluyen los proveedores de servicios de Internet (también conocidos como prestadoras de servicios) que se asocian a Telarus para proporcionar información de precios automatizada de telecomunicaciones en tiempo real. Haga clic en los enlaces a las diversas prestadoras de servicios asociadas y busque las tecnologías WAN dedicadas que proporcionan. Complete la tabla que se incluye a continuación a medida que identifique los servicios WAN dedicados de cada proveedor de servicios, con la información proporcionada en el sitio web. Use las líneas adicionales proporcionadas en la tabla para registrar otros proveedores de servicios.

Proveedor de servicios de Internet (Internet Service Provider)	**T1/DS1/PRI**	**T3/DS3**	**OC3 (SONET)**	**Frame Relay**	**ATM**	**MPLS**	**EPL Línea privada de Ethernet**
Comcast							x
Integra	x	x	x			x	x
tw telecom		x	x			x	
AT&T							
Cbeyond							
Earthlink							
Level 3 Communications							
XO Communications							
Verizon							

Parte 2: Investigar un proveedor de servicios de línea arrendada dedicada en su área

En la parte 2, investigará a un proveedor de servicios local que ofrezca líneas arrendadas dedicadas T1 en el área geográfica especificada. Antes de poder realizar la búsqueda, esta aplicación requiere un nombre, una dirección y un número de teléfono. Quizá desee usar sus datos actuales o investigar una dirección local donde una empresa podría estar buscando una conexión WAN.

Paso 1: Navegar hasta http://www.telarus.com/geoquote.html para probar GeoQuote.

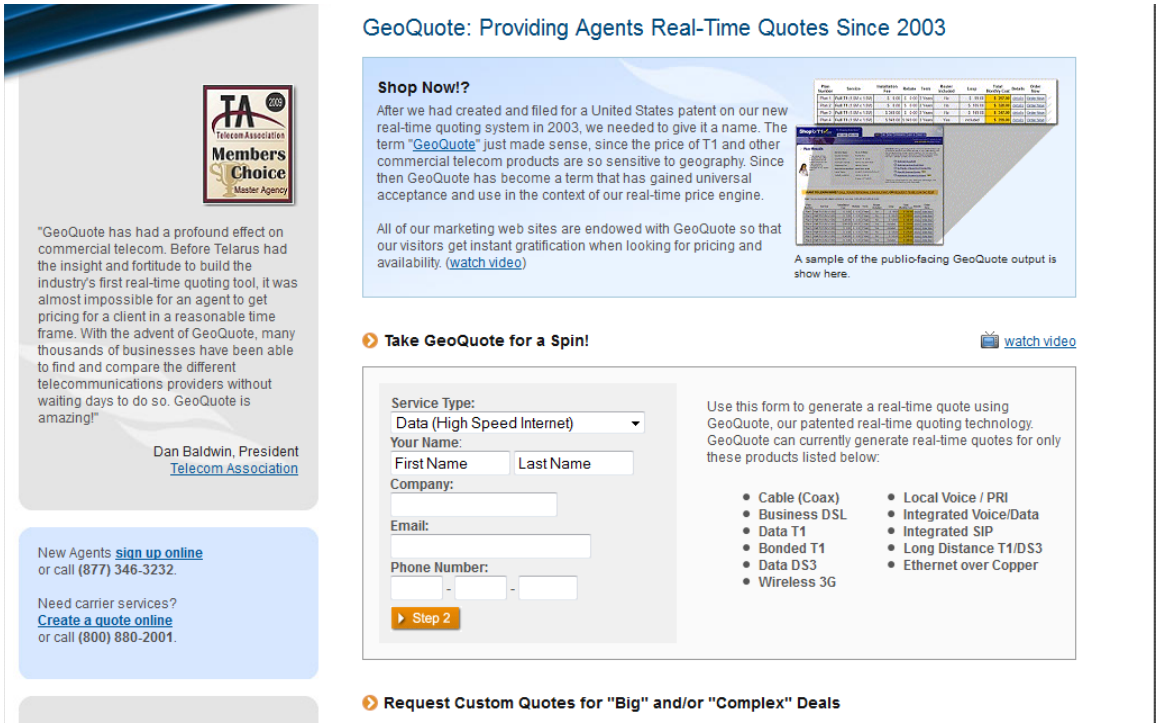
GeoQuote es una aplicación web que automatiza la búsqueda de proveedores de servicios de tecnología WAN y proporciona cotizaciones de precios en tiempo real. Rellene los campos requeridos.

a. Haga clic en la lista desplegable **Service Type** (Tipo de servicio) y seleccione **Data (High Speed Internet)** (Datos [Internet de alta velocidad]).

b. Rellene los campos **First Name** (Nombre) y **Last Name** (Apellido), **Company** (Empresa) con un nombre de ejemplo e **Email** (Correo electrónico).

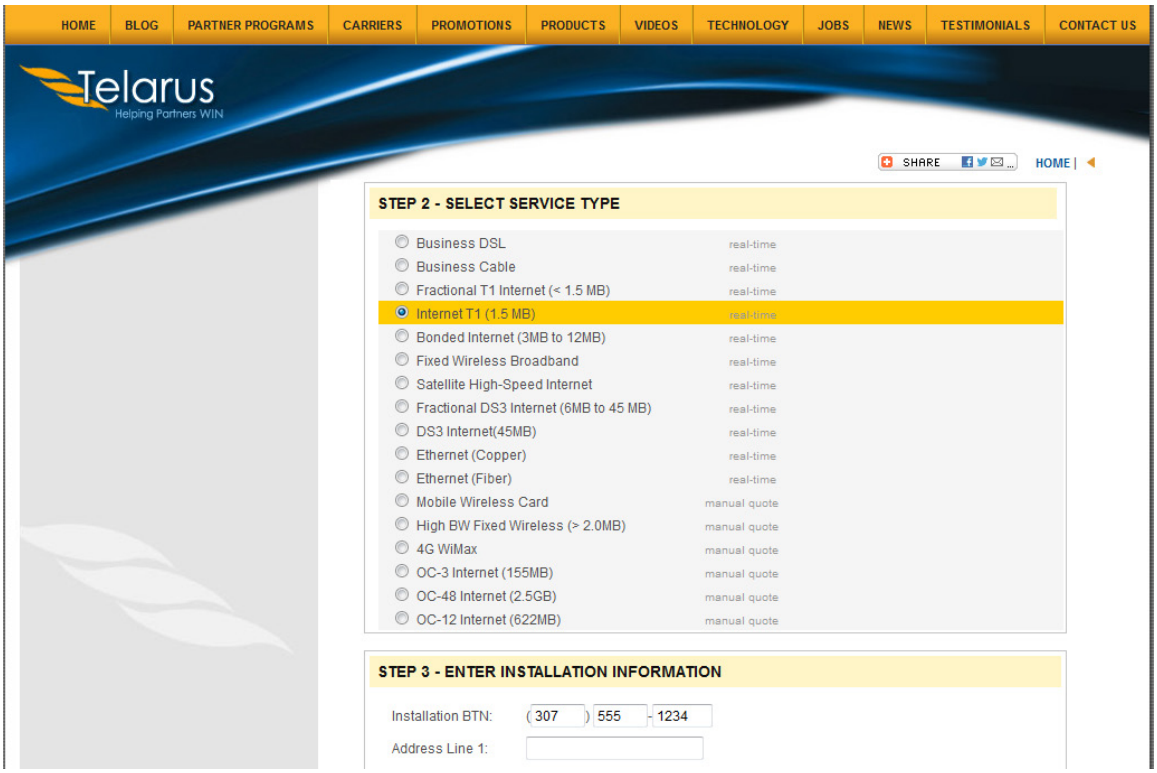
c. Complete el campo **Phone Number** (Número de teléfono) con el número utilizado para conectarse a la WAN. Debe ser un número de teléfono fijo.

d. Haga clic en el botón con el rótulo **Step 2** (Paso 2).



Paso 2: Seleccionar el tipo de servicio.

Elija **Internet T1 (1.5 MB)** y desplácese hacia abajo, hasta **Step 3** (Paso 3) en la página web.



Paso 3: Introducir la información de instalación.

a. En el campo **Installation BTN** (BTN de instalación), introduzca su número de teléfono comercial (BTN) de ejemplo. Debe ser un número de teléfono fijo.

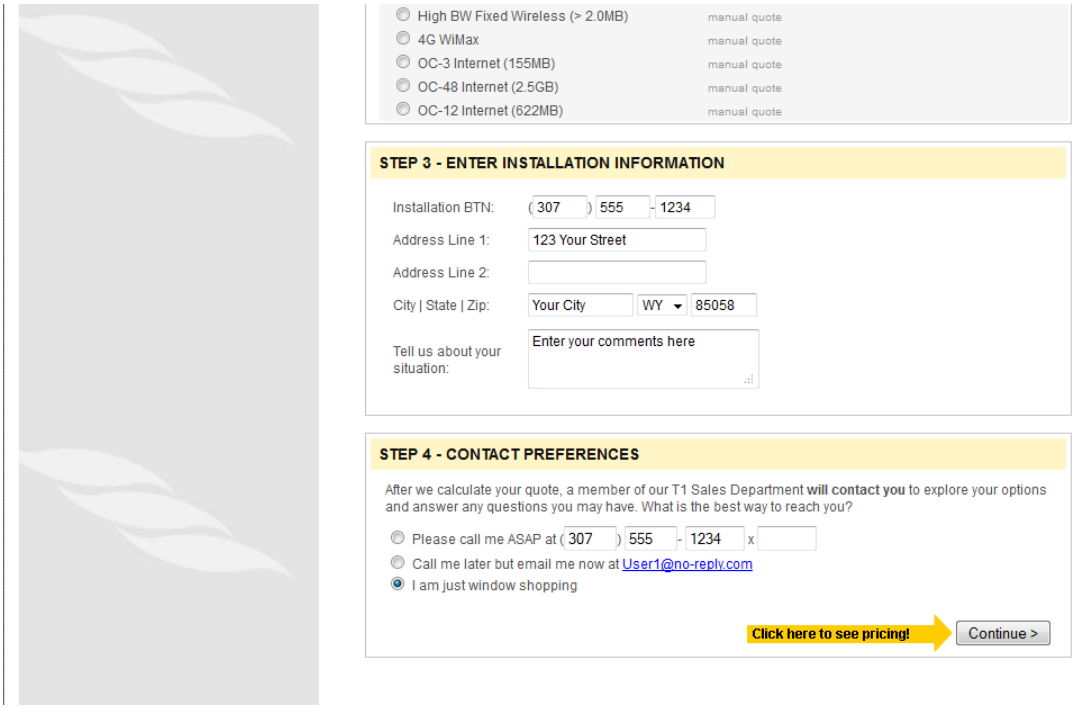
b. Introduzca su dirección, ciudad, estado y código postal.

Paso 4: Introducir las preferencias de contacto.

a. No haga clic en el primer botón de opción (**Please call me ASAP at** [Llámenme lo antes posible al]), pero proporcione su número de teléfono de contacto.

b. Haga clic en el botón de opción **I am just window shopping** (Solo estoy mirando).

c. Haga clic en **Continue**.



Paso 5: Examinar los resultados.

Debería ver una lista de cotizaciones que indiquen los precios disponibles de una conexión T1 a la ubicación que especificó. ¿El precio en el área que eligió es comparable a los que se muestran a continuación?

_____

_____

Las respuestas varían según la ubicación y la disponibilidad del servicio.

¿Cuál fue el intervalo de precios de sus resultados?

_____

_____

Las respuestas varían según la ubicación y la disponibilidad del servicio.

Plan	Service Type	Bandwidth	Install	Rebate	Term	Router	Loop	Monthly Cost ↓	Order
1	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	No	$35.33	$210.33	Order Now
2	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	No	$128.51	$229.91	Order Now
3	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	2 Year	No	$46.67	$231.67	Order Now
4	Internet T1 (1.5 MB)	1.5M x 1.5M	$345.87	$0.00	5 Year	No	$117.13	$246.73	Order Now
5	Internet T1 (1.5 MB)	1.5M x 1.5M	$345.87	$0.00	3 Year	No	$117.13	$254.83	Order Now
6	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	No	$202.02	$256.62	Order Now
7	Internet T1 (1.5 MB)	1.5M x 1.5M	$345.87	$0.00	2 Year	No	$117.13	$262.93	Order Now
8	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	1 Year	No	$58.01	$268.01	Order Now
9	Internet T1 (1.5 MB)	1.5M x 1.5M	$345.87	$0.00	1 Year	No	$117.13	$279.13	Order Now
10	Internet T1 (1.5 MB)	1.5M x 1.5M	$50.00	$0.00	3 Year	Yes	$70.33	$280.33	Order Now
11	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	$202.02	$285.62	Order Now
12	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	included	$288.00	Order Now
13	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	No	included	$299.00	Order Now
14	Internet T1 (1.5 MB)	1.5M x 1.5M	$50.00	$0.00	2 Year	Yes	$81.67	$301.67	Order Now
15	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	$146.00	$306.00	Order Now
16	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	included	$318.00	Order Now

Reflexión<X1/>

1. ¿Cuáles son las desventajas de usar una línea arrendada T1 para uso doméstico personal? ¿Cuál sería una mejor solución?

   Para uso doméstico, un servicio simétrico como T1 sería más costoso e innecesario. Los usuarios domésticos en general descargan mucho más de lo que suben, y un servicio asimétrico como DSL o cable podría proporcionar descargas más rápidas a un precio más accesible.

2. ¿Cuándo podría ser una buena solución de conectividad para una empresa el uso de una conexión WAN dedicada, de cualquier tipo?

   Las respuestas varían. Una empresa, que requiere velocidades de Internet rápidas de subida y descarga, y una conexión ininterrumpida, se beneficiaría con una conexión dedicada.

3. Describa otras tecnologías WAN que proporcionen opciones de alta velocidad económicas que podrían ser una solución alternativa a una conexión T1.

   Frame Relay, MPLS y Ethernet metropolitana o una línea privada de Ethernet (EPL) son tecnologías que podría valer la pena investigar.

Módulos de dispositivos WAN (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.

Objetivo

Seleccionar tecnologías de acceso WAN que satisfagan los requisitos comerciales de una red de una pequeña o mediana empresa.

Nota para el instructor: esta actividad se puede completar de manera individual o en grupos pequeños; luego, se puede compartir y analizar con otro grupo de estudiantes, con toda la clase o con el instructor.

Situación

En su empresa mediana, están actualizando la red. Para aprovechar al máximo el equipo que se usa actualmente, decide adquirir módulos WAN en lugar de equipos nuevos.

En todas las sucursales se utilizan ISR Cisco de las series 1900 o 2911. Actualizará estos routers en varias ubicaciones. Cada sucursal tiene sus propios requisitos de ISP para tener en cuenta.

Para actualizar los dispositivos, enfóquese en los siguientes tipos de acceso de los módulos WAN:

- Ethernet
- Banda ancha
- T1/E1 e ISDN PRI
- BRI
- Serial
- Voz y WAN de enlaces troncales T1 y E1
- LAN y WAN inalámbricas

Recursos

- World Wide Web
- Software de procesamiento de texto

Instrucciones

Paso 1: Visite Interfaces and Modules (Interfaces y módulos). En esta página, verá muchas opciones de módulos de interfaz de ISR. Recuerde que actualmente es propietario de routers Cisco de las series 1900 y 2900, y estos son los únicos que utiliza.

Nota: si el enlace anterior ya no es válido, busque "Interfaces and Modules" en el sitio de Cisco.

Paso 2: Cree una matriz de comparación en la que se indiquen los siguientes tipos de acceso WAN para las redes de las sucursales:

- Ethernet
- Banda ancha
- T1/E1 e ISDN PRI
- BRI

- Serie WAN
- Voz y WAN de enlaces troncales T1 y E1
- LAN y WAN inalámbricas

Paso 3: En la matriz, registre el tipo de módulo de interfaz que necesite comprar para la actualización de los ISR.

Paso 4: Utilice Internet para investigar imágenes de los módulos. Proporcione una captura de pantalla del módulo o un hipervínculo a una imagen de cada módulo.

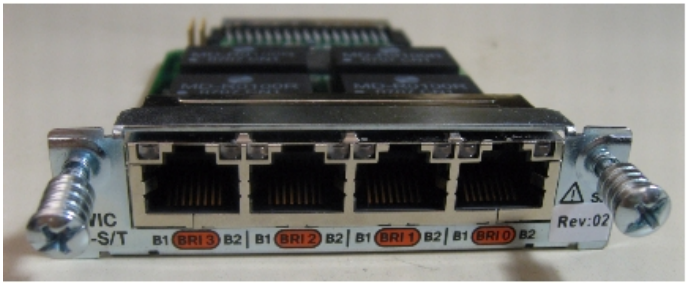
Paso 5: Comparta la matriz con un compañero, un grupo, la clase o el instructor.

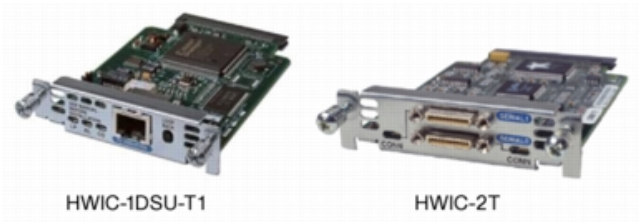
Solución de ejemplo sugerida para la actividad:

Notas para el instructor:

- Este es un buen momento para que los estudiantes analicen la terminología. Por ejemplo, WIC2T = tarjeta de interfaz WAN con 2 puertos serie.
- Los estudiantes pueden agregar varias tarjetas a los routers en PT y usar comandos como **show ip interface brief** para ver los cambios.
- Aliente a los estudiantes a leer la información de la hoja de datos que se presenta en los sitios de gráficos de las tarjetas modulares: al hacerlo, se familiarizarán con los diferentes tipos de interfaz.
- Como se verá en la matriz final de los estudiantes, todos los gráficos variarán: los gráficos que se muestran en esta solución de ejemplo para la actividad tienen carácter representativo y se copiaron de sitios de productos de Cisco. Cada gráfico tiene un hipervínculo al origen, que estaba disponible en el momento en que se creó esta actividad.

Módulos de dispositivos WAN

Tipo de acceso WAN	Disponibilidad de módulos en las series 2900 y 1900	Ejemplo de módulo (tarjeta de interfaz) (* en la columna 2 indica el gráfico que se muestra)
Ethernet	• EHWIC, 1 puerto, modo doble, con SFP(100M/1G) o GE(10M/100M/1G)* • HWIC, 2 puertos, puerto enrutado 10/100	
Banda ancha	• EHWIC VDSL2/ADSL/2/2+ multimodo con anexo (variaciones A, B y M)* • EHWIC EFM/ATM SHDSL multimodo • HWIC G.SHDSL de 4 pares con soporte de 2, 4 y 8 hilos o HWIC G.SHDSL de 2 pares con soporte de 2 y 4 hilos	
T1/E1 e ISDN PRI	(para utilizar solo con serie 2900) • HWIC E1/T1/PRI ISDN, 2 puertos, canalizado* • HWIC E1/T1/PRI ISDN, 1 puerto, canalizado	
BRI	(para utilizar solo con serie 2900) • Tarjeta VIC, 2 puertos, BRI (NT y TE) (para utilizar con series 2900 y 1900) • Tarjeta de interfaz WAN de alta velocidad BRI ISDN, 4 puertos* • Tarjeta de interfaz WAN de alta velocidad BRI ISDN, 1 puerto U • Tarjeta de interfaz WAN ISDN, 1 puerto (dial y línea arrendada)	

Serial	(para utilizar solo con serie 2900) • Módulo de servicio T3/E3, canal despejado de un puerto • HWIC T1/E1, canal despejado de 4 puertos • HWI, 4 puertos, serial (para utilizar con series 2900 y 1900) • Tarjeta de interfaz WAN CSU/DSU, 1 puerto, 4 hilos, 56/64 Kpbs • Tarjeta de interfaz WAN de alta velocidad T1/T1 fraccionada DSU/CSU, 1 puerto* • Tarjeta de interfaz WAN de alta velocidad, 1 puerto, serial • Tarjeta de interfaz WAN de alta velocidad, 2 puertos, serial	 HWIC-1DSU-T1 HWIC-2T
Voz y WAN de enlaces troncales T1 y E1	• Voz/WAN T1/E1 con D&I sin estructurar E1 (G703), 1 puerto[1] • Voz/WAN T1/E1 con opciones soltar e insertar (D&I), 2 puertos • Voz/WAN T1/E1 con opciones soltar e insertar, 1 puerto[2] • Voz/WAN T1/E1 con D&I y E1 sin estructurar (G703), 2 puertos • Voz/WAN T1/E1 con D&I y E1 sin estructurar (G703), 1 puerto	1  2 
LAN y WAN inalámbricas	• EHWIC LTE 4G dedicada para red inalámbrica Verizon, EE.UU. (SKU de Verizon), funciona en LTE en la banda 13 de 700 Mhz con GPS • EHWIC LTE 4G AT&T, banda 17 de 700 MHz, UMTS/HSPA de 850/1900/2100 MHz • EHWIC LTE 4G para	

	Europa, LTE en 800/900/1800/2100/2600 MHz, bandas UMTS/HSPA de 900/1900/2100 MHz • (fuera de EE.UU.) EHWIC HSPA+ versión 7 3.7G con SMS/GPS (MC8705) • EHWIC HSPA+ versión 7 AT&T con SMS/GPS basado en MC8705 • (fuera de EE.UU.) EHWIC HSPA/UMTS 3.5G de 850/900/1900/2100 MHz con SMS/GPS • EHWIC 3G Verizon EV-DO Rev A/0/1xRTT de 800/1900 MHz con SMS/GPS • EHWIC 3G Sprint EV-DO Rev A/0/1xRTT de 800/1900 MHz con SMS/GPS • EHWIC 3G BSLN EV-DO Rev A/0/1xRTT de 800/1900 MHz con SMS/GPS • (solo para India) HWIC 3G TATA EV-DO Rev A/0/1xRTT 800/1900 MHz	

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Interfaces modulares WAN
- Tipos de interfaces de la tarjeta de red
- Disponibilidad de módulo ISR por tipo de modelo

Persuasión para el uso de PPP (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

Describir los beneficios de usar PPP a través de HDLC en una WAN.

Esta actividad se puede completar en forma individual o en pequeños grupos de 2 a 3 estudiantes por grupo.

Situación

Su supervisor de ingeniería de red asistió recientemente a una conferencia sobre tecnología de redes en la que se abordaron los protocolos de capa 2. Él sabe que usted cuenta con equipos de Cisco en las instalaciones, pero también quiere ofrecerle seguridad y opciones y controles avanzados de TCP/IP en esos mismos equipos mediante el protocolo punto a punto (PPP).

Después de investigar el protocolo PPP, descubre que este ofrece algunas ventajas que el protocolo HDLC, que se utiliza actualmente en la red, no ofrece.

Cree una matriz donde se incluyan las ventajas y desventajas de utilizar el protocolo HDLC en comparación con el protocolo PPP. Cuando compare los dos protocolos, incluya lo siguiente:

- Facilidad de configuración
- Adaptabilidad a equipos de red no exclusivos
- Opciones de seguridad
- Uso y compresión del ancho de banda
- Consolidación del ancho de banda

Comparta el gráfico con otro estudiante o con la clase. Explique si sugeriría, o no, mostrarle la matriz al supervisor de ingeniería de red para justificar la implementación de un cambio de HDLC a PPP para la conectividad de red de capa 2.

Recursos

- Acceso a Internet para conectarse a la World Wide Web
- Software de procesamiento de texto o de hoja de cálculo

Recursos y ejemplo de modelo sugeridos para el instructor

Recursos/sitios de Internet

- 3 WAN Protocols You Should Know
- RFC 1661

Gráfico de comparación entre HDLC y PPP

Criterios	HDLC	PPP
Facilidad de configuración	Estándar o predeterminado en todos los equipos de Cisco	Puede ser simple o más complicado, según las opciones de PPP que se eligieron para implementar.
Adaptabilidad a equipos de red no exclusivos	No adaptable a otros dispositivos que no son de Cisco.	Adaptable a otros dispositivos que no son exclusivos.
Opciones de seguridad	No se ofrecen.	CHAP (contraseñas de enlace seguras y cifradas) o PAP (contraseñas de enlace no cifradas).
Uso y compresión del ancho de banda	TDM estándar y sin compresión.	Compresión disponible.
Consolidación del ancho de banda	Se utiliza ancho de banda serial estándar en una conexión.	Se pueden agrupar distintas conexiones para ofrecer mayor ancho de banda y rendimiento de tráfico.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- PPP
- HDLC
- CHAP
- PAP
- TDM
- STDM
- Compresión del ancho de banda
- Consolidación del ancho de banda

Práctica de laboratorio: Configuración de PPP básico con autenticación (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

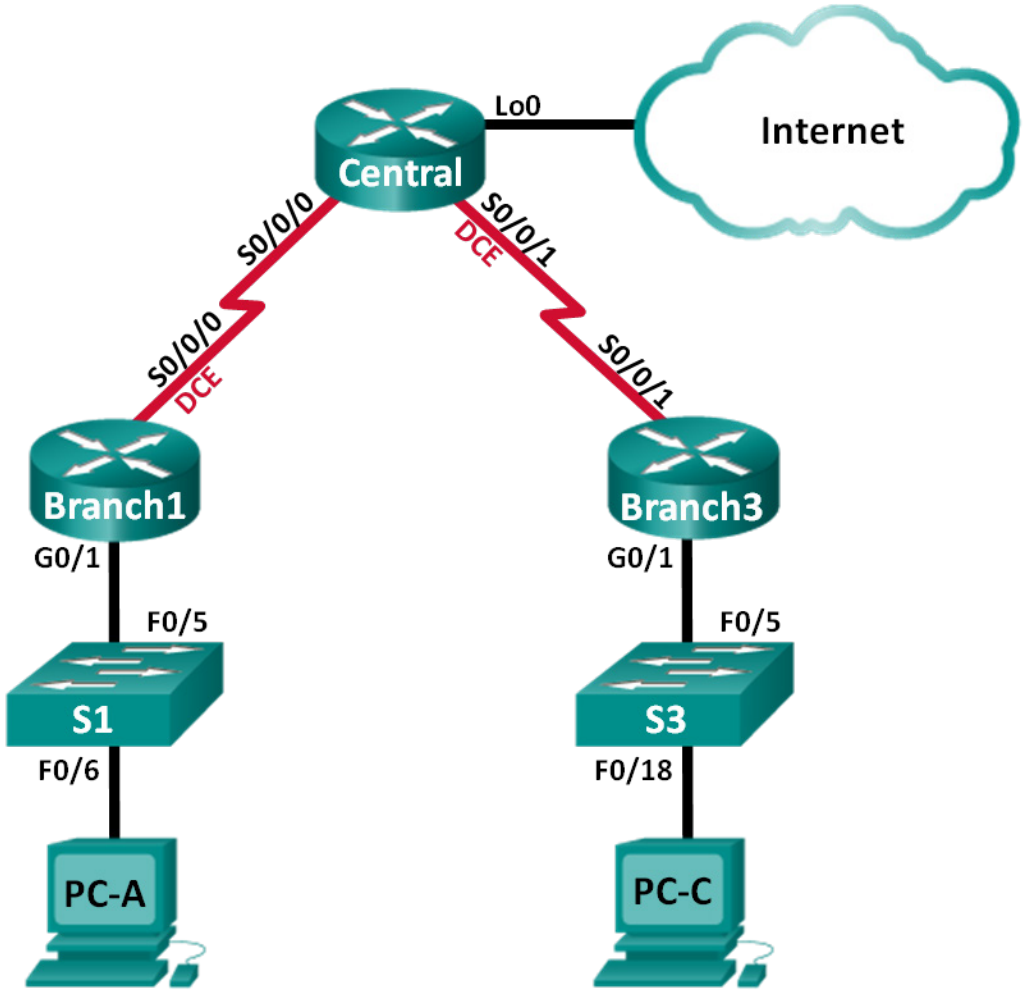


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Branch1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
Central	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
Branch3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: Configurar los parámetros básicos de los dispositivos

Parte 2: Configurar la encapsulación PPP

Parte 3: Configurar la autenticación CHAP de PPP

Información básica/situación

El protocolo punto a punto (PPP) es un protocolo WAN de capa 2 muy común. PPP se puede utilizar para conectarse de las LAN las WAN de los proveedores de servicios y para la conexión de segmentos LAN dentro de una red empresarial.

En esta práctica de laboratorio, configurará la encapsulación PPP en los enlaces seriales dedicados entre los routers de sucursal y un router central. Configurará el protocolo de autenticación por desafío mutuo (CHAP) de PPP en los enlaces seriales PPP. También examinará los efectos de los cambios de la encapsulación y la autenticación en el estado del enlace serial.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

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

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos del router, como las direcciones IP de las interfaces, el routing, el acceso a los dispositivos y las contraseñas.

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

Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.

Paso 2: Inicializar y volver a cargar los routers y los switches.

Paso 3: Configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un aviso de mensaje del día (MOTD) que advierta a los usuarios que se prohíbe el acceso no autorizado.

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

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

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Aplique las direcciones IP a las interfaces Serial y Gigabit Ethernet según la tabla de direccionamiento y active las interfaces físicas.

i. Establezca la frecuencia de reloj en **128000** para las interfaces seriales DCE.

j. Cree **Loopback0** en el router Central para simular el acceso a Internet y asigne una dirección IP según la tabla de direccionamiento.

Paso 4: Configurar el routing.

a. Habilite OSPF de área única en los routers y utilice la ID de proceso 1. Agregue todas las redes, excepto 209.165.200.224/27, al proceso OSPF.

b. Configure una ruta predeterminada hacia la simulación de Internet en el router Central con Lo0 como interfaz de salida y vuelva a distribuir esta ruta al proceso OSPF.

c. Emita los comandos **show ip route ospf**, **show ip ospf interface brief** y **show ip ospf neighbor** en todos los routers para verificar que OSPF se haya configurado correctamente. Tome nota de la ID del router para cada router.

Branch1:

```
Branch1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```



```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.1.1.2, 00:04:10, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:04:20, Serial0/0/0
O     192.168.3.0/24 [110/129] via 10.1.1.2, 00:03:21, Serial0/0/0

Branch1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/0      1     0               10.1.1.1/30        64    P2P   1/1
Gi0/1        1     0               192.168.1.1/24     1     DR    0/0

Branch1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
209.165.200.225   0   FULL/  -        00:00:33    10.1.1.2        Serial0/0/0
```

Central:

```
Central# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

O     192.168.1.0/24 [110/65] via 10.1.1.1, 00:07:43, Serial0/0/0
O     192.168.3.0/24 [110/65] via 10.2.2.1, 00:06:38, Serial0/0/1

Central# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               10.2.2.2/30        64    P2P   1/1
Se0/0/0      1     0               10.1.1.2/30        64    P2P   1/1

Central# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       0   FULL/  -        00:00:33    10.2.2.1        Serial0/0/1
192.168.1.1       0   FULL/  -        00:00:36    10.1.1.1        Serial0/0/0
```

Branch3

```
Branch3# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.2.2.2, 00:08:14, Serial0/0/1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/128] via 10.2.2.2, 00:08:14, Serial0/0/1
O     192.168.1.0/24 [110/129] via 10.2.2.2, 00:08:14, Serial0/0/1

Branch3# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               10.2.2.1/30        64    P2P   1/1
Gi0/1        1     0               192.168.3.1/24     1     DR    0/0

Branch3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
209.165.200.225   0   FULL/  -        00:00:37    10.2.2.2        Serial0/0/1
```

Paso 5: Configurar las PC.

Asigne direcciones IP y gateways predeterminados a las computadoras según la tabla de direccionamiento.

Paso 6: Verificar la conectividad de extremo a extremo.

Todos los dispositivos deben poder hacer ping a los otros dispositivos en la topología. De lo contrario, lleve a cabo la resolución de problemas hasta que pueda establecer la conectividad de extremo a extremo.

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

Paso 7: Guarde las configuraciones.

Parte 2: Configurar la encapsulación de PPP

Paso 1: Mostrar la encapsulación serial predeterminada.

En los routers, emita el comando **show interfaces serial** *id-interfaz* para mostrar la encapsulación serial actual.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
```



```
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   1003 packets input, 78348 bytes, 0 no buffer
   Received 527 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   1090 packets output, 80262 bytes, 0 underruns
   0 output errors, 0 collisions, 3 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
   2 carrier transitions
   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

¿Cuál es la encapsulación serial predeterminada en un router Cisco?

_____ HDLC

Paso 2: Cambiar la encapsulación serial a PPP.

a. Emita el comando **encapsulation ppp** en la interfaz S0/0/0 para que el router Branch1 cambie la encapsulación de HDLC a PPP.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
Branch1(config-if)#
Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Branch1(config-if)#
Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
```

b. Emita el comando para mostrar el estado de línea y el protocolo de línea para la interfaz S0/0/0 en el router Branch1. Registre el comando emitido. ¿Cuál es el estado actual de la interfaz S0/0/0?

_____

```
Branch1# show ip interface brief
```

El estado de línea es up (activo) y el protocolo figura como down (inactivo).

```
Branch1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    down
Serial0/0/1                unassigned      YES unset  administratively down down
```


c. Emita el comando **encapsulation ppp** en la interfaz S0/0/0 para que el router Central corrija la incompatibilidad en la encapsulación serial.

```
Central(config)# interface s0/0/0
Central(config-if)# encapsulation ppp
Central(config-if)#
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

d. Verifique que la interfaz S0/0/0 en los routers Branch1 y Central esté up/up, y se haya configurado con la encapsulación PPP.

¿Cuál es el estado del protocolo de control de enlace (LCP) PPP? _____ Open

¿Qué protocolos de control de red (NCP) se negociaron?

_____

El protocolo de control del protocolo de Internet (IPCP) y el protocolo de control Cisco Discovery Protocol (CDPCP)

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:03:58
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     77 packets input, 4636 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     117 packets output, 5800 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
     22 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     18 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Central# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
```



```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
Last clearing of "show interface" counters 00:01:20
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   41 packets input, 2811 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   40 packets output, 2739 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Paso 3: Interrumpir intencionalmente la conexión serial.

a. Emita los comandos **debug ppp** para observar los efectos de los cambios en la configuración PPP en el router Branch1 y el router Central.

```
Branch1# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch1# debug ppp packet
PPP packet display debugging is on

Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central# debug ppp packet
PPP packet display debugging is on
```

b. Observe los mensajes de depuración de PPP cuando fluye el tráfico en el enlace serial entre los routers Branch1 y Central.

```
Branch1#
Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#
```



```
Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
```

c. Interrumpa la conexión serial devolviendo la encapsulación serial a HDLC para la interfaz S0/0/0 en el router Branch1. Registre el comando que se utilizó para cambiar la encapsulación a HDLC.

_____

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation hdlc
```

d. Observe los mensajes de depuración de PPP en el router Branch1. La conexión serial se terminó, y el protocolo de línea está inactivo. La ruta a 10.1.1.2 (Central) se eliminó de la tabla de routing.

```
Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.295: PPP: NET STOP send to AAA.
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.29
Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN
Branch1(config-if)#
Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
```

e. Observe los mensajes de depuración de PPP en el router Central. El router Central continúa intentando establecer una conexión con Branch1, según lo que indican los mensajes de depuración. Cuando las interfaces no pueden establecer una conexión, se vuelven a desactivar. Además, OSPF no puede establecer una adyacencia con su vecino debido a la incompatibilidad en la encapsulación serial.

```
Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
```



```
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN
Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification
.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message
.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]
.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING
.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:29:52.296: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
.Jun 20 02:29:54.308: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<resultado omitido>
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:10.436: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<resultado omitido>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
```



```
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING
.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]
.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
```

¿Qué sucede cuando un extremo del enlace serial se encapsula con PPP y el otro extremo del enlace se encapsula con HDLC?

_____

_____

_____

El enlace deja de funcionar, y se interrumpe la adyacencia OSPF. PPP sigue intentando establecer una conexión con el extremo opuesto del enlace, según lo que indica el mensaje “Phase is ESTABLISHING”. Sin embargo, dado que continúa recibiendo un paquete que no es NCP, LCP no puede negociar y el enlace permanece inactivo.

f. Emita el comando **encapsulation ppp** en la interfaz S0/0/0 para que el router Branch1 corrija la incompatibilidad en la encapsulación.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
```

g. Observe los mensajes de depuración de PPP del router Branch1 a medida que este establece una conexión con el router Central.

```
Branch1(config-if)#
Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message
Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]
Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line
Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.399: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
```



```
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP:    Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
<resultado omitido>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from
LOADING to FULL, Loading Done
Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]
```

h. Observe los mensajes de depuración de PPP del router Central a medida que este establece una conexión con el router Branch1.

```
Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10
Jun 20 03:01:59.393: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating
Jun 20 03:01:59.393: PPP: NET STOP send to AAA.
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
```



```
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated
.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.1
.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<resultado omitido>
.Jun 20 03:01:59.401: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 03:01:59.433: Se0/0/0 IPCP:    Address 10.1.1.2 (0x03060A010102)
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]
<resultado omitido>
.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open
.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
```



```
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
```

Sobre la base del mensaje de depuración, ¿qué fases atraviesa PPP cuando el otro extremo del enlace serial en el router Central se configura con la encapsulación PPP?

_____

_____

PPP atraviesa las siguientes fases: DOWN, ESTABLISHING y UP.

¿Qué sucede cuando la encapsulación PPP se configura en cada extremo del enlace serial?

_____

El enlace se activa, y se restaura la adyacencia OSPF.

i. Emita el comando **undebug all** (o **u all**) en los routers Branch1 y Central para desactivar toda la depuración en ambos routers.

j. Emita el comando **show ip interface brief** en los routers Branch1 y Central una vez que converja la red. ¿Cuál es el estado para la interfaz S0/0/0 en ambos routers?

_____

El estado de serial 0/0/0 es up, y el protocolo figura como up.

```
Branch1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down

Central# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                10.1.1.2        YES manual up                    up
Serial0/0/1                10.2.2.2        YES manual up                    up
```



```
Loopback0                  209.165.200.225 YES manual up                    up
```

k. Verifique que la interfaz S0/0/0 en los routers Branch1 y Central se haya configurado para la encapsulación PPP.

En el espacio proporcionado a continuación, registre el comando para verificar la encapsulación PPP.

_____

_____

```
Branch1# show interfaces s0/0/0
Central# show interfaces s0/0/0
```

l. Cambie la encapsulación serial para el enlace entre los routers Central y Branch3 a la encapsulación PPP.

```
Central(config)# interface s0/0/1
Central(config-if)# encapsulation ppp
Central(config-if)#
Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
LOADING to FULL, Loading Done

Branch3(config)# interface s0/0/1
Branch3(config-if)# encapsulation ppp
Branch3(config-if)#
Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from LOADING to FULL, Loading Done
```

m. Verifique que se haya restaurado la conectividad de extremo a extremo antes de continuar con la parte 3.

Parte 3: Configurar la autenticación PPP CHAP

Paso 1: Verificar que se haya configurado la encapsulación PPP en todas las interfaces seriales.

Registre el comando que se utilizó para verificar que se haya configurado la encapsulación PPP.

_____

show running-config con modificadores de resultado o **show interfaces** *id-interfaz*

Paso 2: Configurar la autenticación CHAP de PPP para el enlace entre el router Central y el router Branch3.

a. Configure un nombre de usuario para la autenticación CHAP.

```
Central(config)# username Branch3 password cisco
Branch3(config)# username Central password cisco
```

b. Emita los comandos **debug ppp** en el router Branch3 para observar el proceso asociado a la autenticación.

```
Branch3# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch3# debug ppp packet
PPP packet display debugging is on
```

c. Configure la interfaz S0/0/1 en Branch3 para la autenticación CHAP.

```
Branch3(config)# interface s0/0/1
Branch3(config-if)# ppp authentication chap
```

d. Examine los mensajes de depuración de PPP en el router Branch3 durante la negociación con el router Central.

```
Branch3(config-if)#
Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed
Jun 20 04:25:02.079: PPP: NET STOP send to AAA.
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated
.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN
.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address
10.2.2.2
.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2
.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]
.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING
.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction
.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]
<resultado omitido>
.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]
.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 04:25:02.091: Se0/0/1 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 04:25:02.091: Se0/0/1 LCP:    MagicNumber 0xF7B20F10 (0x0506F7B20F10)
.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"
```



```
.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open
.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]
.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User
.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User
.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10
<resultado omitido>
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address
10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from LOADING to FULL, Loading Done
.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]
.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
```

Sobre la base de los mensajes de depuración de PPP, ¿qué fases atraviesa el router Branch3 antes de que el enlace con el router Central esté activo?

_____

_____

PPP atraviesa las siguientes fases: DOWN, ESTABLISHING, AUTHENTICATING y UP.

e. Emita el comando **debug ppp authentication** para observar los mensajes de la autenticación CHAP en el router Central.

```
Central# debug ppp authentication
PPP authentication debugging is on
```

f. Configure la autenticación CHAP en S0/0/1 en el router Central.

```
Central(config)# interface s0/0/1
Central(config-if)# ppp authentication chap
```

g. Observe los mensajes de depuración de PPP relacionados con la autenticación CHAP en el router Central.

```
Central(config-if)#
.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction
.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]
.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA
.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"
.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4
.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
```

h. Emita el comando **undebug all** (o **u all**) en los routers Central y Branch3 para desactivar toda la depuración.

```
Central# undebug all
All possible debugging has been turned off
```

Paso 3: Interrumpir intencionalmente el enlace serial configurado con la autenticación.

a. En el router Central, configure un nombre de usuario para utilizar con Branch1. Asigne **cisco** como la contraseña.

```
Central(config)# username Branch1 password cisco
```

b. En los routers Central y Branch1, configure la autenticación CHAP en la interfaz S0/0/0. ¿Qué sucede con la interfaz?

_____

La interfaz S0/0/0 se activa y se desactiva.

Nota: para acelerar el proceso, desactive la interfaz y vuelva a habilitarla.

```
.Jun 20 05:23:55.032: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
Central(config-if)#
.Jun 20 05:23:57.064: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
.Jun 20 05:23:57.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Central(config-if)#
.Jun 20 05:24:03.144: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
.Jun 20 05:24:03.156: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Central(config-if)#
```

c. Utilice un comando **debug ppp negotiation** para examinar lo que sucede.

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central(config-if)#
.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP
.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message
.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]
.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING
.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction
.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15
.Jun 20 05:25:26.229: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 05:25:26.233: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.233: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message
```

```
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN
```

Explique cuál es la causa de que se termine el enlace. Corrija el problema y, en el espacio proporcionado a continuación, registre el comando emitido para hacerlo.

_____

_____

_____

El enlace se termina porque no se puede completar el enlace CHAP sin la credencial de usuario correcta en Branch1.

```
Branch1(config)# username Central password cisco
```

d. Emita el comando **undebug all** en todos los routers para desactivar la depuración.

e. Verificar la conectividad de extremo a extremo.

Reflexión

1. ¿Cuáles son los indicadores de que puede tener una incompatibilidad en la encapsulación serial en un enlace serial?

_____

Algunos de los indicadores son los siguientes: la red ya no converge porque se eliminaron algunas rutas y el protocolo de línea para el enlace está inactivo.

2. ¿Cuáles son los indicadores de que puede tener una incompatibilidad de autenticación en un enlace serial?

_____

Algunos de los indicadores son los siguientes: se eliminó la ruta de la tabla de routing y el protocolo de línea se activa y se desactiva.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Branch1

```
Branch1# show run
Building configuration...

Current configuration : 1832 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
```



```
ip cef
!
!
!
!
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
username Central password 7 1511021F0725
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
```



```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 094F471A1A0A
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 121A0C041104
 login
 transport input all
line vty 5 15
 password 7 110A1016141D
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Central

```
Central#show run
Building configuration...

Current configuration : 1964 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```



```
!
hostname Central
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username Branch3 password 7 1511021F0725
username Branch1 password 7 05080F1C2243
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface Embedded-Service-Engine0/0
```



```
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 00071A150754
```



```
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 060506324F41
 login
 transport input all
line vty 5 15
 password 7 14141B180F0B
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Branch3

```
Branch3# show run
Building configuration...

Current configuration : 1929 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Branch3
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
```



```
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username Central password 7 0822455D0A16
!
redundancy
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
```



```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
   Unauthorized Access Prohibited.^C
!
line con 0
 password 7 13061E010803
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 045802150C2E
 login
 transport input all
line vty 5 15
 password 7 13061E010803
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Práctica de laboratorio: Resolución de problemas de PPP básico con autenticación (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

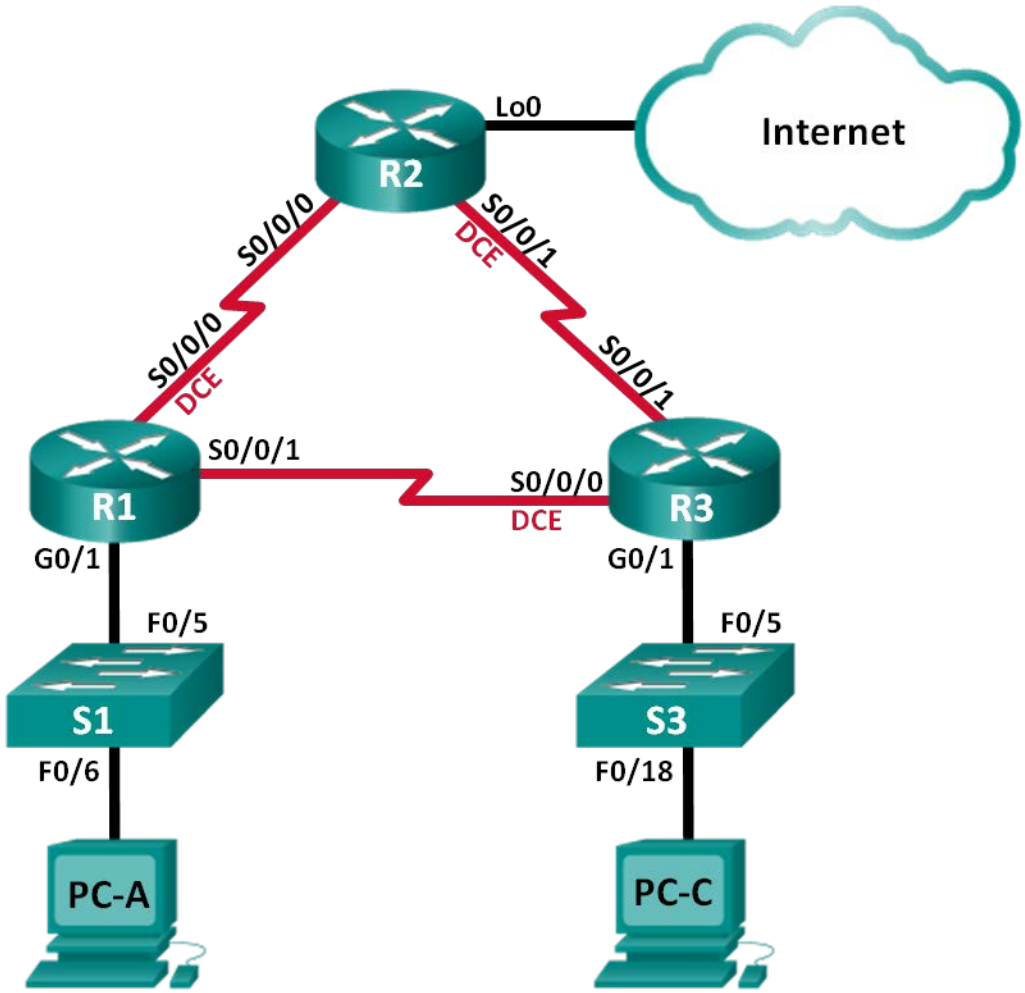


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: Armar la red y cargar las configuraciones de los dispositivos

Parte 2: Resolver problemas de la capa de enlace de datos

Parte 3: Resolver problemas de la capa de red

Información básica/situación

Un ingeniero de redes inexperto configuró los routers de la compañía. Varios errores en la configuración han resultado en problemas de conectividad. El gerente le solicitó que resuelva los problemas, corrija los errores de configuración y documente su trabajo. Según los conocimientos de PPP y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los enlaces seriales usen la autenticación CHAP de PPP y que se pueda llegar a todas las redes.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

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

Parte 1: Armar la red y cargar las configuraciones de los dispositivos

En la parte 1, establecerá la topología de la red, configurará los parámetros básicos en los equipos host y cargará las configuraciones en los routers.

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

Paso 2: Configurar los equipos host.

Paso 3: Cargar las configuraciones de los routers.

Cargue las siguientes configuraciones en el router apropiado. Todos los routers tienen las mismas contraseñas. La contraseña del modo EXEC privilegiado es **class**. La contraseña para el acceso a la consola y a VTY es **cisco**. Todas las interfaces seriales deben configurarse con la encapsulación PPP y autenticarse con CHAP con la contraseña **chap123**.

Configuración del router R1:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
! no shutdown
interface s0/0/1
 ip address 192.168.31.1 255.255.255.252
! ip address 192.168.13.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
! ppp authentication chap
! no shutdown
exit
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
```



```
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/1
 exit
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Configuración del router R2:

```
hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
! username R3 password chap123
! no username r3 password chap123
interface lo0
 ip address 209.165.200.225 255.255.255.252
interface s0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
! encapsulation ppp
! ppp authentication chap
 no shutdown
 exit
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 default-information originate
 exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
```



```
 password cisco
 login
```

Configuración del router R3:

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
!no username R3 password chap123
!username R1 password chap123
interface g0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.13.2 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
 exit
router ospf 1
 router-id 3.3.3.3
! network 192.168.3.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 passive-interface g0/1
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Paso 4: Guardar la configuración en ejecución.

Parte 2: Resolver problemas de la capa de enlace de datos

En la parte 2, utilizará comandos **show** para resolver problemas de la capa de enlace de datos. Asegúrese de verificar las configuraciones, como la frecuencia de reloj, la encapsulación, CHAP, los nombres de usuario y las contraseñas.

Paso 1: Examinar la configuración del R1.

a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

```
R1# show interfaces s0/0/0
Serial0/0/0 is administratively down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:04:41
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=up  RTS=down  CTS=down

R1# show interfaces s0/0/1
Serial0/0/1 is administratively down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.31.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:09:10
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
```

```
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=up  DTR=down  RTS=down  CTS=down
```

Sobre la base de los resultados de **show interfaces** para S0/0/0 y S0/0/1, ¿cuáles son los posibles problemas con los enlaces PPP?

_____

_____

El resultado indica lo siguiente: tanto S0/0/0 como S0/0/1 están inactivas. Se aplicó la encapsulación PPP a ambas interfaces, S0/0/0 y S0/0/1. Además del hecho de que las interfaces seriales están administrativamente inactivas, aún hay problemas con las configuraciones PPP, como la incompatibilidad de autenticación.

b. Utilice el comando **debug ppp authentication** para ver el resultado en tiempo real de la autenticación PPP durante la resolución de problemas.

```
R1# debug ppp authentication
PPP authentication debugging is on
```

c. Utilice el comando **show run interface s0/0/0** para examinar la configuración en S0/0/0.

```
R1# show run interface s0/0/0
Building configuration...

Current configuration : 143 bytes
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.252
 encapsulation ppp
 shutdown
 ppp authentication chap
 clock rate 128000
end
```

Resuelva todos los problemas que detecte para S0/0/0. Registre los comandos utilizados para corregir la configuración.

_____

```
R1(config)# interface s0/0/0
R1(config-if)# no shutdown
```

Después de corregir el problema, ¿qué información proporciona el resultado de debug?


```
R1(config-if)# no shutdown
*Jun 18 12:01:23.931: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Jun 18 12:01:23.931: Se0/0/0 PPP: Using default call direction
*Jun 18 12:01:23.931: Se0/0/0 PPP: Treating connection as a dedicated line
*Jun 18 12:01:23.931: Se0/0/0 PPP: Session handle[F900005A] Session id[90]
*Jun 18 12:01:23.943: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Jun 18 12:01:23.947: Se0/0/0 CHAP: I CHALLENGE id 1 len 23 from "R2"
*Jun 18 12:01:23.947: Se0/0/0 PPP: Sent CHAP SENDAUTH Request
*Jun #18 12:01:23.947: Se0/0/0 PPP: Received SENDAUTH Response PASS
*Jun 18 12:01:23.947: Se0/0/0 CHAP: Using hostname from configured hostname
*Jun 18 12:01:23.947: Se0/0/0 CHAP: Using password from AAA
*Jun 18 12:01:23.947: Se0/0/0 CHAP: O RESPONSE id 1 len 23 from "R1"
*Jun 18 12:01:23.947: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
*Jun 18 12:01:23.951: Se0/0/0 PPP: Sent CHAP LOGIN Request
*Jun 18 12:01:23.951: Se0/0/0 PPP: Received LOGIN Response PASS
*Jun 18 12:01:23.951: Se0/0/0 CHAP: O SUCCESS id 1 len 4
*Jun 18 12:01:23.951: Se0/0/0 CHAP: I SUCCESS id 1 len 4
```

El resultado de debug muestra un proceso de negociación CHAP que se realizó correctamente. Se estableció PPP en el enlace que conecta S0/0/0 del R1 a S0/0/0 del R2.

d. Utilice el comando **show run interface s0/0/1** para examinar la configuración en S0/0/1.

```
R1# show run interface s0/0/1
Building configuration...

Current configuration : 123 bytes
!
interface Serial0/0/1
 ip address 192.168.31.1 255.255.255.252
 encapsulation ppp
 shutdown
 ppp authentication pap
end
```

Resuelva todos los problemas que detecte para S0/0/1. Registre los comandos utilizados para corregir la configuración.

```
R1(config)# interface s0/0/1
R1(config-if)# ppp authentication chap
R1(config-if)# no shutdown
```

Después de corregir el problema, ¿qué información proporciona el resultado de debug?

```
*Jun 18 12:13:57.819: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up
*Jun 18 12:13:57.819: Se0/0/1 PPP: Using default call direction
*Jun 18 12:13:57.819: Se0/0/1 PPP: Treating connection as a dedicated line
*Jun 18 12:13:57.819: Se0/0/1 PPP: Session handle[F300005B] Session id[91]
*Jun 18 12:13:57.831: Se0/0/1 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Jun 18 12:13:57.831: Se0/0/1 CHAP: I CHALLENGE id 1 len 23 from "R3"
```

```
*Jun 18 12:13:57.831: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
*Jun 18 12:13:57.831: Se0/0/1 PPP: Received SENDAUTH Response PASS
*Jun 18 12:13:57.831: Se0/0/1 CHAP: Using hostname from configured hostname
*Jun 18 12:13:57.831: Se0/0/1 CHAP: Using password from AAA
*Jun 18 12:13:57.831: Se0/0/1 CHAP: O RESPONSE id 1 len 23 from "R1"
*Jun 18 12:14:01.819: Se0/0/1 PPP: Using default call direction
*Jun 18 12:14:01.819: Se0/0/1 PPP: Treating connection as a dedicated line
*Jun 18 12:14:01.819: Se0/0/1 PPP: Session handle[BC00005C] Session id[92]
*Jun 18 12:14:01.831: Se0/0/1 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Jun 18 12:14:01.851: Se0/0/1 CHAP: I CHALLENGE id 1 len 23 from "R3"
*Jun 18 12:14:01.851: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
*Jun 18 12:14:01.851: Se0/0/1 PPP: Sending AAA radius abort
R1(config-if)#
*Jun 18 12:14:04.860: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
*Jun 18 12:14:04.868: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
*Jun 18 12:14:06.856: Se0/0/1 PPP: Using default call direction
```

_____

_____

El resultado de debug muestra un proceso de negociación CHAP que no se realizó correctamente, y la interfaz se activa y se desactiva. Existen más errores de configuración para el enlace que conecta S0/0/1 del R1 a S0/0/0 del R3.

e. Utilice el comando **no debug ppp authentication** o **undebug all** para desactivar el resultado de la depuración de PPP.

f. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

```
R1# show running-config | include username
username R2 password 0 chap123
username R3 password 0 chap123
```

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

_____

No existe ningún problema.

Paso 2: Examinar la configuración del R2.

a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

```
R2# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.12.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
```



```
  Last input 00:00:06, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:18:22
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     53 packets input, 3055 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     52 packets output, 2772 bytes, 0 underruns
     0 output errors, 0 collisions, 34 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

R2# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.23.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:11, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     230 packets input, 4370 bytes, 0 no buffer
     Received 230 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     119 packets output, 3014 bytes, 0 underruns
     0 output errors, 0 collisions, 42 interface resets
     230 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     121 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

¿Se establecieron todos los enlaces? _____ No

Si la respuesta es negativa, ¿cuáles son los enlaces que se deben examinar? ¿Cuáles son los problemas posibles?

_____

No se estableció el enlace entre el R2 y el R3 porque la interfaz S0/0/1 está configurada con la encapsulación HDLC. Además del problema de encapsulación, la incompatibilidad de autenticación puede evitar el establecimiento del enlace.

b. Utilice el comando **show run interface** para examinar los enlaces que no se establecieron.

```
R2# show run interface s0/0/1
Building configuration...

Current configuration : 89 bytes
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
end
```

Resuelva todos los problemas que detecte para las interfaces. Registre los comandos utilizados para corregir la configuración.

_____

_____

```
R2(config)# interface s0/0/1
R2(config-if)# encapsulation ppp
R2(config-if)# ppp authentication chap
```

c. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

```
R2# show running-config | include username
username R1 password 0 chap123
username r3 password 0 chap123
```

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

_____

_____

```
R2(config)# no username r3 password chap123
R2(config)# username R3 password chap123
```

d. Utilice el comando **show ppp interface serial** para la interfaz serial cuyos problemas debe resolver.

```
R2# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.23.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
```



```
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:25:09
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     506 packets input, 27348 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     507 packets output, 28030 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

¿Se estableció el enlace? _____ Sí

Paso 3: Examinar la configuración del R3.

a. Utilice el comando **show interfaces** para determinar si se estableció PPP en ambos enlaces seriales.

```
R3# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.13.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:55:56
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 3 packets/sec
  5 minute output rate 0 bits/sec, 2 packets/sec
     3540 packets input, 70800 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3274 packets output, 60079 bytes, 0 underruns
```



```
     0 output errors, 0 collisions, 821 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     1573 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

```
R3# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.23.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:51:19
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     711 packets input, 35022 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     847 packets output, 36444 bytes, 0 underruns
     0 output errors, 0 collisions, 73 interface resets
     141 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     96 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

¿Se establecieron todos los enlaces? _____ No

Si la respuesta es negativa, ¿cuáles son los enlaces que se deben examinar? ¿Cuáles son los problemas posibles?

_____

No se estableció el enlace serial entre el R1 y el R3. La interfaz Serial0/0/0 está configurada con la encapsulación PPP y se encuentra activa. Por lo tanto, el problema posible es la incompatibilidad de autenticación.

b. Utilice el comando **show run interface** para examinar cualquier enlace serial que no se haya establecido.

```
R3# show run interface s0/0/0
Building configuration...
```



```
Current configuration : 134 bytes
!
interface Serial0/0/0
 ip address 192.168.13.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 2000000
end
```

Resuelva todos los problemas que detecte en las interfaces. Registre los comandos utilizados para corregir la configuración.

_____

No existe ningún problema con la configuración de S0/0/0.

c. Utilice el comando **show running-config | include username** para verificar la configuración correcta del nombre de usuario y la contraseña.

```
R3# show run | include username
username R2 password 0 chap123
username R3 password 0 chap123
```

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

_____

```
R3(config)# no username R3 password chap123
R3(config)# username R1 password chap123
```

d. Utilice el comando **show interface** para verificar que se hayan establecido los enlaces seriales.

```
R3# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.13.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:20, output 00:00:03, output hang never
  Last clearing of "show interface" counters 01:03:35
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4392 packets input, 88310 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
     3974 packets output, 74268 bytes, 0 underruns
     0 output errors, 0 collisions, 994 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     1919 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

e. ¿Se establecieron todos los enlaces PPP?_____ Sí

f. ¿Se puede hacer ping de la PC-A a Lo0? _____ Sí

g. ¿Puede PC-A hacer ping a PC-C? _____ No

Nota: puede ser necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

Parte 3: Resolver problemas de la capa de red

En la parte 3, verificará que se haya establecido la conectividad de capa 3 en todas las interfaces mediante el análisis de la configuración IPv4 y OSPF.

Paso 1: Verifique que las interfaces que se indican en la tabla de direccionamiento estén activas y configuradas con la información de dirección IP correcta.

Emita el comando **show ip interface brief** en todos los routers para verificar que las interfaces estén en estado up/up (activo/activo).

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                192.168.12.1    YES manual up                    up
Serial0/0/1                192.168.31.1    YES manual up                    up

R2# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                192.168.12.2    YES manual up                    up
Serial0/0/1                192.168.23.1    YES manual up                    up
Loopback0                  209.165.200.225 YES manual up                    up

R3# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.3.1     YES manual up                    up
Serial0/0/0                192.168.13.2    YES manual up                    up
Serial0/0/1                192.168.23.2    YES manual up                    up
```


Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

```
R1(config)# interface s0/0/1
R1(config-if)# ip address 192.168.13.1 255.255.255.252
```

Paso 2: Verificar el routing OSPF.

Emita el comando **show ip protocols** para verificar que OSPF se esté ejecutando y que todas las redes se anuncien.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:46
    2.2.2.2              110      00:01:46
  Distance: (default is 110)

R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.12.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
    209.165.200.224 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:03:53
    1.1.1.1              110      00:07:45
  Distance: (default is 110)
```

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.13.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:07:14
    2.2.2.2              110      00:07:14
  Distance: (default is 110)
```

Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

```
R3(config)# router ospf 1
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

¿Puede PC-A hacer ping a PC-C? _____ Sí

Si no hay conectividad entre todos los hosts, continúe con la resolución de cualquier problema restante.

Nota: puede ser necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos, final

Router R1

```
R1#show run
Building configuration...

Current configuration : 1821 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
```



```
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
username R2 password 0 chap123
username R3 password 0 chap123
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
interface Serial0/0/1
 ip address 192.168.13.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
```



```
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

R2 del router

```
R2#show run
Building configuration...

Current configuration : 1866 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
```



```
!
username R1 password 0 chap123
username R3 password 0 chap123
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.252
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
control-plane
!
```



```
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

R3 del router

```
R3#show run
Building configuration...

Current configuration : 1888 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
```



```
multilink bundle-name authenticated
!
username R2 password 0 chap123
username R1 password 0 chap123
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.13.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
interface Serial0/0/1
 ip address 192.168.23.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router ospf 1
 router-id 3.3.3.3
 passive-interface GigabitEthernet0/1
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
 password cisco
```



```
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Validación de PPP (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.

Objetivo

Usar los comandos **show** y **debug** para resolver problemas de PPP.

Nota para el instructor: esta actividad se debe completar en grupos de tres estudiantes, pero la pueden completar todas las personas en una clase al mismo tiempo.

Situación

Tres amigos que están inscritos en Cisco Networking Academy desean poner a prueba sus conocimientos acerca de la configuración de redes PPP.

Establecen un concurso en el que cada uno tiene que pasar una prueba de configuración de PPP con requisitos definidos y diversas opciones de situaciones de PPP. Cada persona elabora una situación de configuración diferente.

Al día siguiente, se reúnen y prueban la configuración de los otros con los requisitos de sus respectivas situaciones de PPP.

Recursos

- Software de Packet Tracer
- Cronómetro o temporizador

Paso 1: Abrir Packet Tracer.

a. Cree una topología de dos routers con una conexión serial.

b. Incluya una computadora y un switch conectados a cada router.

Paso 2: Completar las situaciones.

a. Comience con la configuración del Scenario 1 (Situación 1).

b. El instructor determina el momento en que se completa la situación; todos los estudiantes y grupos deben dejar de trabajar en la configuración en ese momento.

c. El instructor verifica la validez de la configuración completa de la situación.

1) Los dispositivos deben poder hacer pings correctamente de un extremo de la topología al otro.

2) Todas las opciones de situación requeridas deben estar presentes en la topología final.

3) El instructor puede solicitar que pruebe su trabajo mediante la elección de distintos comandos **show** y **debug** para mostrar el resultado de la configuración.

El estudiante o el grupo que complete la situación correctamente será el ganador.

d. Comience el mismo proceso con el Scenario 2 (Situación 2).

1) Elimine las configuraciones del Scenario 1, pero puede volver a utilizar las mismas.

2) Vuelva a completar los pasos 1 y 2 con los requisitos de la situación siguiente.

Las situaciones sugeridas incluyen lo siguiente:

Situación 1

- Asignar direcciones a la topología mediante IPv4.
- Configurar la encapsulación PPP con CHAP.
- Configurar el routing OSPF.
- Configurar el reloj para que lea la fecha de hoy.
- Cambiar las prioridades de router OSPF en ambas interfaces seriales.

Situación 2

- Asignar direcciones a la topología mediante IPv6.
- Configurar la encapsulación PPP con PAP.
- Configurar el routing EIGRP.
- Configurar el reloj para que lea la hora actual.
- Colocar una descripción en ambas interfaces seriales conectadas.

Situación 3

- Asignar direcciones a la topología mediante IPv6.
- Configurar un mensaje del día.
- Configurar PPP con CHAP
- Configurar el routing OSPF.
- Configurar el reloj para que lea la fecha y la hora de hoy.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- PPP
- CHAP
- PAP
- EIGRP
- OSPF
- Configuración de reloj (variaciones)
- Descripción de las interfaces
- Prioridades de interfaz

Tecnologías WAN emergentes (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.

Objetivo

Resolver problemas de WAN que afectan las comunicaciones de internetwork en una red de una pequeña a mediana empresa.

Notas para el instructor:

- Esta actividad permite que los estudiantes consideren otras opciones para obtener conectividad WAN. Estas opciones se mencionan en el currículo y permiten que los estudiantes exploren las opciones de comunicaciones WAN de redes emergentes disponibles actualmente para las redes de pequeñas a medianas empresas.
- Los estudiantes pueden trabajar de manera individual o en grupos pequeños para completar esta actividad.

Situación

Como administrador de red de su pequeña a mediana empresa, ya pasó de WAN de línea arrendada a conectividad de Frame Relay para la comunicación de red WAN. Usted es responsable de mantener todas las futuras actualizaciones de red al corriente.

Descubre que hay algunas opciones alternativas disponibles para la conectividad WAN para mantenerse al corriente con las tecnologías emergentes y en desarrollo. Algunos de estos programas incluyen los siguientes:

- Frame Relay
- DSL de banda ancha
- Cable módem de banda ancha
- GigaMAN
- VPN
- MPLS

Dado que desea ofrecerle a su empresa el servicio de red WAN de mejor calidad y menor costo, decide investigar, al menos, dos tecnologías emergentes y en desarrollo. Su objetivo es reunir información acerca de estas dos opciones de WAN alternativas para analizar de forma consciente los objetivos futuros de la red con su gerente comercial y con otros administradores de red.

Recursos

- Acceso a Internet para conectarse a la World Wide Web
- Software de presentación

Instrucciones

Paso 1: Elija dos de las siguientes tecnologías WAN emergentes y en desarrollo:

a. Frame Relay
b. DSL de banda ancha
c. Cable módem de banda ancha
d. GigaMAN

e. VPN
f. MPLS

Paso 2: Cree una matriz para registrar información sobre las dos tecnologías WAN que eligió. Como mínimo, incluya lo siguiente:

a. Una breve descripción de la tecnología
b. Los requisitos físicos para establecer la tecnología
   1) Los requisitos de cableado
   2) Los dispositivos de red necesarios para el funcionamiento de la tecnología WAN
   3) El proveedor de los dispositivos de red necesarios para el funcionamiento de la tecnología WAN
c. Los beneficios de este tipo de tecnología WAN
d. Las desventajas de implementar esta forma de tecnología WAN o de cambiar a ella
e. Los costos relacionados con este tipo de tecnología

Paso 3: Cree una presentación de cinco diapositivas para usar más adelante y analizar con su gerente comercial u otros administradores de red.

Matriz de solución de ejemplo para el instructor

Información basada en estos sitios:

Understanding the Gigaman Service
To LAN or not to LAN

Tecnología WAN GigaMAN	
Descripción	Tecnología WAN punto a punto mediante Ethernet a conexiones conmutadas de fibra óptica. Actualmente se limita a las áreas metropolitanas, pero se considera su expansión a través de distancias geográficas cada vez más grandes. Utiliza switches Gigabit Ethernet conectados a switches y routers de fibra óptica (dependientes de la empresa de telecomunicaciones). AT&T desarrolló esta tecnología y, en la actualidad, se considera uno de los principales proveedores de servicios de conexiones WAN GigaMAN.
Requisitos físicos	Si la pequeña o mediana empresa actualmente utiliza conectividad Gigabit Ethernet en sus switches, la empresa de telecomunicaciones proporciona conectividad a los switches de la empresa. No es necesario adquirir ningún equipo adicional.

Beneficios	Mayor disponibilidad de ancho de banda (hay investigaciones que sugieren que una línea ofrece más de 26 veces la velocidad de una línea T1). Proporciona una tecnología WAN segura (arrendada, punto a punto con tres variantes de entrega de datos a través de conexiones de fibra óptica). Capacidad para enviar o recibir archivos grandes debido a la mayor disponibilidad de ancho de banda (1 Gb/s; actualmente, algunas fuentes indican una capacidad de ancho de banda de GigaMAN de 10 Gb/s). Debido a su funcionamiento de sucursal a región, este tipo de tecnología resulta ideal para las empresas con varias sucursales, por ejemplo, los sistemas educativos.
Desventajas	En la actualidad, se limita al uso regional y de sucursales; mientras tanto, los proveedores de servicios trabajan para ampliar las limitaciones de distancia. Según los estándares actuales, GigaMAN puede funcionar a una distancia de hasta 180 mi (290 km) de extremo a extremo, con el uso de repetidores.
Costos relacionados	Aumento de los costos relacionados con el arrendamiento punto a punto, según el uso de ancho de banda y el plan de la empresa de telecomunicaciones, pero esto es relativo si se tiene en cuenta la compensación de más ancho de banda y la disponibilidad de opciones de seguridad.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Tecnologías WAN
- Redes WAN de conmutación de circuitos
- Redes WAN de conmutación de paquetes
- Conexiones de línea arrendada
- Conexiones punto a punto

Práctica de laboratorio: Configuración de Frame Relay y subinterfaces (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

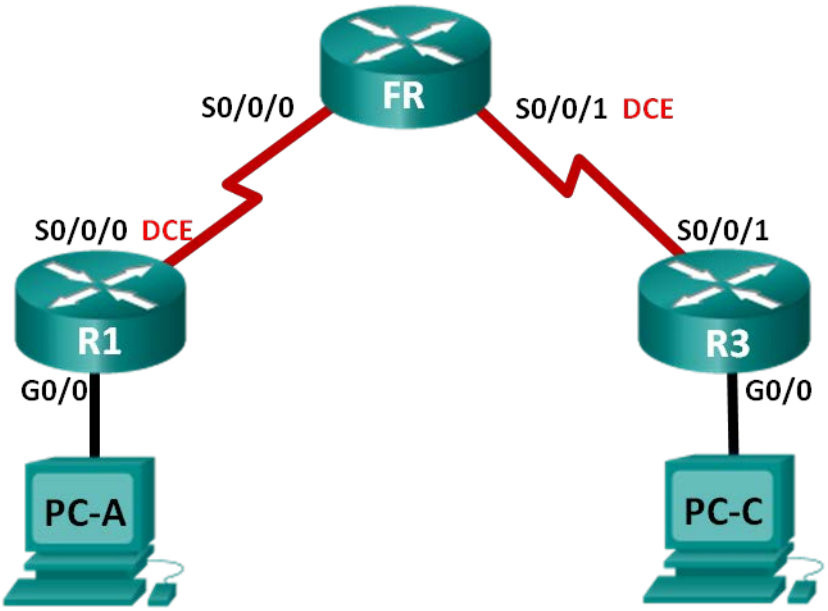


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4 e IPv6	Gateway predeterminado
R1	G0/0	192.168.1.1/24 2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0 (DCE)	10.1.1.1/30 2001:DB8:ACAD:B::1/64 FE80::1 link-local	N/A
FR	S0/0/0	N/A	N/A
	S0/0/1 (DCE)	N/A	N/A
R3	G0/0	192.168.3.1/24 2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/1	10.1.1.2/30 2001:DB8:ACAD:B::3/64 FE80::3 link-local	N/A
PC-A	NIC	192.168.1.3/24 2001:DB8:ACAD:A::A/64	192.168.1.1 FE80::1
PC-C	NIC	192.168.3.3/24 2001:DB8:ACAD:C::C/64	192.168.3.1 FE80::3

Objetivos

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

Parte 2: Configurar un switch Frame Relay

Parte 3: Configurar los parámetros básicos de Frame Relay

Parte 4: Resolver problemas de Frame Relay

Parte 5: Configurar una subinterfaz Frame Relay

Información básica/situación

Frame Relay es un protocolo WAN de alto rendimiento que funciona en las capas física y de enlace de datos del modelo de referencia OSI. A diferencia de las líneas arrendadas, Frame Relay solo requiere un circuito de acceso único al proveedor de servicios de Frame Relay para comunicarse con varios sitios conectados al mismo proveedor.

Frame Relay era uno de los protocolos WAN más utilizados, sobre todo debido a que era relativamente económico en comparación con las líneas dedicadas. Además, configurar el equipo del usuario en una red Frame Relay es bastante simple. Con la llegada de los servicios de banda ancha como DSL y cable módem, GigaMAN (servicio Ethernet punto a punto a través de cable de fibra óptica), VPN y conmutación de etiquetas multiprotocolo (MPLS), Frame Relay se convirtió en una solución menos deseable para acceder a la WAN. Sin embargo, algunas áreas rurales no tienen acceso a estas soluciones alternativas y aún dependen de Frame Relay para obtener conectividad a la WAN.

En esta práctica de laboratorio, configurará la encapsulación de Frame Relay en enlaces seriales. También configurará un router para que simule un switch Frame Relay. Revisará los estándares de Cisco y los estándares abiertos que se aplican a Frame Relay. También configurará subinterfaces punto a punto de Frame Relay.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

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

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

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

Paso 2: Inicializar y volver a cargar los routers según sea necesario.

Paso 3: Configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

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

c. Asigne **class** como la contraseña del modo EXEC privilegiado.

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

e. Configure **logging synchronous** para la línea de consola.

f. Cifre las contraseñas de texto no cifrado.

g. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

i. Configure las direcciones IPv4 e IPv6 que se indican en la tabla de direccionamiento para todas las interfaces. No active las interfaces seriales en este momento.

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

Paso 4: Configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

Paso 5: Probar la conectividad.

En este momento, las computadoras no pueden hacer ping entre sí, pero deben poder hacer ping a su gateway predeterminado. Pruebe ambos protocolos, IPv4 e IPv6. Verifique y resuelva los problemas, si es necesario.

Parte 2: Configurar un switch Frame Relay

En la parte 2, configurará un switch Frame Relay. Creará circuitos virtuales permanentes (PVC) y asignará los identificadores de conexión de enlace de datos (DLCI). Esta configuración crea dos PVC: uno del R1 al R3 (DLCI 103) y uno del R3 al R1 (DLCI 301).

Paso 1: Configurar el router FR como switch Frame Relay.

El comando **frame-relay switching** habilita el switching Frame Relay globalmente en un router, lo que le permite reenviar tramas según el DLCI entrante en lugar de una dirección IP.

```
FR(config)# frame-relay switching
```

Paso 2: Cambiar la encapsulación de la interfaz en S0/0/0.

Cambie el tipo de encapsulación de la interfaz a Frame Relay. Al igual que HDLC o PPP, Frame Relay es un protocolo de capa de enlace de datos que especifica el entramado del tráfico de capa 2.

```
FR(config)# interface s0/0/0
FR(config-if)# encapsulation frame-relay
```

Paso 3: Cambiar el tipo de interfaz a DCE.

Cambiar el tipo de interfaz a DCE le indica al router que envíe keepalives de interfaz de administración local (LMI) y permite que se apliquen instrucciones de ruta de Frame Relay.

Nota: los tipos de interfaces de Frame Relay no necesitan coincidir con el tipo de interfaz física subyacente. Una interfaz serial DTE física puede funcionar como una interfaz DCE de Frame Relay, y una interfaz DCE física puede funcionar como una interfaz DTE lógica de Frame Relay.

```
FR(config)# interface s0/0/0
FR(config-if)# frame-relay intf-type dce
```

Paso 4: Configurar DLCI.

Configure el router para reenviar el tráfico entrante de la interfaz S0/0/0 con el DLCI 103 a la S0/0/1 con un resultado de DLCI de 301.

```
FR(config-if)# frame-relay route 103 interface s0/0/1 301
FR(config-if)# no shutdown
```

Paso 5: Configurar Frame Relay en S0/0/1.

```
FR(config)# interface s0/0/1
FR(config-if)# encapsulation frame-relay
FR(config-if)# frame-relay intf-type dce
FR(config-if)# frame-relay route 301 interface s0/0/0 103
FR(config-if)# no shutdown
```


Paso 6: Verifique la configuración de Frame Relay.

a. Utilice el comando **show frame-relay pvc** para verificar que Frame Relay se haya configurado correctamente.

```
FR# show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

             Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       0            1            0            0
  Unused         0            0            0            0

DLCI = 103, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  connected to interface Serial0/0/1 301
  pvc create time 00:00:53, last time pvc status changed 00:00:53

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

             Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       0            1            0            0
  Unused         0            0            0            0

DLCI = 301, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/1

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
```



```
Detailed packet drop counters:
no out intf 0            out intf down 0          no out PVC 0
in PVC down 0            out PVC down 0           pkt too big 0
shaping Q full 0         pkt above DE 0           policing drop 0
connected to interface Serial0/0/0 103
pvc create time 00:00:16, last time pvc status changed 00:00:16
```

b. Emita el comando **show frame-relay route**. Esta es la ruta de capa 2 que toma el tráfico de Frame Relay a través de la red. (No confundir con el routing IP de capa 3).

```
FR# show frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0/0     103             Serial0/0/1     301             inactive
Serial0/0/1     301             Serial0/0/0     103             inactive
```

Parte 3: Configuración básica de Frame Relay

En la parte 3, configurará Frame Relay en los routers R1 y R3. Después de configurar Frame Relay, habilitará el protocolo de routing EIGRP para proporcionar conectividad de extremo a extremo.

Paso 1: Configurar R1 para Frame Relay.

ARP inverso permite que los extremos distantes de un enlace Frame Relay se detecten entre sí dinámicamente y proporciona un método dinámico para asignar direcciones IP a los DLCI. Si bien ARP inverso es útil, no siempre es confiable. La práctica recomendada es asignar direcciones IP a los DLCI de forma estática y deshabilitar ARP inverso.

a. Cambie la encapsulación en S0/0/0 a Frame Relay.

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation frame-relay
```

b. Utilice el comando **no frame-relay inverse-arp** para deshabilitar ARP inverso.

```
R1(config)# interface s0/0/0
R1(config-if)# no frame-relay inverse-arp
```

c. Utilice el comando **frame-relay map** para asignar una dirección IP a un DLCI de forma estática. Además de asignar una dirección IP a un DLCI, el software IOS de Cisco permite que se asignen otras varias direcciones de protocolo de capa 3. En el siguiente comando, la palabra clave **broadcast** envía cualquier tráfico de multidifusión o difusión destinado a este enlace a través del DLCI. La mayoría de los protocolos de routing requieren la palabra clave **broadcast** para funcionar correctamente a través de Frame Relay. Puede utilizar la palabra clave **broadcast** en varios DLCI en la misma interfaz. El tráfico se reproduce a todos los PVC.

Nota: la asignación de Frame Relay IPv6 a una dirección de unidifusión global no incluye la palabra clave **broadcast**. Sin embargo, la palabra clave **broadcast** se utiliza en la asignación a la dirección link-local. Los protocolos de routing IPv6 utilizan direcciones link-local para las actualizaciones de routing de multidifusión. Por lo tanto, solo el mapa de direcciones link-local requiere la palabra clave **broadcast** para reenviar paquetes de multidifusión.

```
R1(config)# interface s0/0/0
R1(config-if)# frame-relay map ip 10.1.1.2 103 broadcast
R1(config-if)# frame-relay map ipv6 2001:db8:acad:b::3 103
R1(config-if)# frame-relay map ipv6 fe80::3 103 broadcast
```

d. Para que el router haga ping a su propia interfaz, se debe crear el DLCI para que se asigne a la interfaz local.


```
R1(config)# interface s0/0/0
R1(config-if)# frame-relay map ip 10.1.1.1 103
R1(config-if)# frame-relay map ipv6 2001:db8:acad:b::1 103
```

e. Utilice el comando **no shutdown** para activar S0/0/0.

```
R1(config-if)# no shutdown
```

Paso 2: Configurar el R3 para Frame Relay.

```
R3(config)# interface s0/0/1
R3(config-if)# encapsulation frame-relay
R3(config-if)# no frame-relay inverse-arp
R3(config-if)# frame-relay map ip 10.1.1.1 301 broadcast
R3(config-if)# frame-relay map ipv6 2001:db8:acad:b::1 301
R3(config-if)# frame-relay map ipv6 fe80::1 301 broadcast
R3(config-if)# frame-relay map ip 10.1.1.2 301
R3(config-if)# frame-relay map ipv6 2001:db8:acad:b::3 301
R3(config-if)# no shutdown
```

¿Por qué se utiliza el comando **no shutdown** después del comando **no frame-relay inverse-arp**?

_____

_____

_____

Si introduce primero el comando **no shutdown**, ARP inverso puede provocar que Frame Relay descubra asignaciones de capa 2 a capa 3 que quizá no desee. Al desactivar ARP inverso de Frame Relay antes de emitir el comando **no shutdown**, se asegura de que solo las conexiones asignadas estáticamente que usted desea formen parte de los mapas de Frame Relay.

Paso 3: Verificar que Frame Relay esté activo.

a. Ahora debería poder hacer ping del R1 al R3. Es probable que la activación de los PVC demore varios segundos después de activar las interfaces.

```
R1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/40 ms
R1# ping 2001:db8:acad:b::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

b. Haga ping a R1 desde R3.

```
R3# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```



```
R3# ping 2001:db8:acad:b::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/26/28 ms
```

c. Emita el comando **show frame-relay pvc** para mostrar la información de estado del PVC en el R1 y en el R3.

```
R1# show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

                Active     Inactive      Deleted       Static
  Local            1            0            0            0
  Switched         0            0            0            0
  Unused           0            0            0            0

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

  input pkts 22            output pkts 154          in bytes 2240
  out bytes 10860          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 134       out bcast bytes 8780
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:59:40, last time pvc status changed 01:55:14

R3# show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

                Active     Inactive      Deleted       Static
  Local            1            0            0            0
  Switched         0            0            0            0
  Unused           0            0            0            0

DLCI = 301, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

  input pkts 158           output pkts 22           in bytes 11156
  out bytes 2240           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 2         out bcast bytes 160
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:57:20, last time pvc status changed 01:56:19
```

d. Emita el comando **show frame-relay route** en el FR para verificar el estado de las instrucciones de mapa de Frame Relay.

```
FR# show frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0/0     103             Serial0/0/1     301             active
Serial0/0/1     301             Serial0/0/0     103             active
```

e. Emita el comando **show frame-relay map** en el R1 y el R3 para mostrar un resumen de las asignaciones estáticas y dinámicas de las direcciones de capa 3 a los DLCI. Debido a que se desactivó ARP inverso, solo hay mapas estáticos.

```
R1# show frame-relay map
Serial0/0/0 (up): ipv6 FE80::3 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ip 10.1.1.1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::3 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ip 10.1.1.2 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active

R3# show frame-relay map
Serial0/0/1 (up): ipv6 FE80::1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1 (up): ipv6 2001:DB8:ACAD:B::3 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.2 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ipv6 2001:DB8:ACAD:B::1 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
```

Nota: el router FR funciona como dispositivo de capa 2, por lo que no es necesario asignar direcciones de capa 3 a los DLCI de capa 2.

Paso 4: Configurar EIGRP en el R1 y el R3.

a. Habilite el routing IPv6 en el R1 y el R3.

```
R1(config)# ipv6 unicast-routing

R3(config)# ipv6 unicast-routing
```


b. Con el AS 1, habilite EIGRP para IPv4 e IPv6 en el R1 y el R3 para todas las redes. Establezca la ID del router para el R1 en 1.1.1.1 y en 3.3.3.3 para el R3.

```
R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)# network 10.1.1.0 0.0.0.3
R1(config-router)# network 192.168.1.0
R1(config-rtr)# no shutdown

R1(config-router)# ipv6 router eigrp 1
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# interface g0/0
R1(config-if)# ipv6 eigrp 1
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 eigrp 1

R3(config)# router eigrp 1
R3(config-router)# no auto-summary
R3(config-router)# eigrp router-id 3.3.3.3
R3(config-router)# network 10.1.1.0 0.0.0.3
R3(config-router)# network 192.168.3.0
R3(config-router)# ipv6 router eigrp 1
R3(config-rtr)# router-id 3.3.3.3
R3(config-rtr)# no shutdown
R3(config-rtr)# interface g0/0
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface s0/0/1
R3(config-if)# ipv6 eigrp 1
```

Paso 5: Verificar la conectividad de extremo a extremo.

Haga ping de la PC-A a la PC-C. Si los pings no se realizaron correctamente, resuelva los problemas hasta tener conectividad de extremo a extremo.

Nota: quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Parte 4: Resolución de problemas de Frame Relay

En la parte 4, interrumpirá la conexión Frame Relay establecida anteriormente y utilizará algunas herramientas para resolver problemas de Frame Relay. Existe una variedad de herramientas para llevar a cabo la resolución de problemas de conectividad de Frame Relay.

Paso 1: Depurar la interfaz de administración local (LMI).

a. Emita el comando **debug frame-relay lmi** en el R1. El resultado proporciona información detallada sobre todos los datos de LMI. Los keepalives se envían cada 10 segundos de manera predeterminada, de modo que es probable que deba esperar para ver algún resultado. El resultado muestra un paquete LMI saliente con el número de secuencia 50. El último mensaje de LMI recibido del FR tenía el número de

secuencia 49. El resultado también muestra un mensaje de LMI entrante del FR al R1 con el número de secuencia 50. El DLCI 103 es el único DLCI en este enlace y actualmente está activo.

```
R1# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#
*Jun 26 18:28:45.922: Serial0/0/0(out): StEnq, myseq 50, yourseen 49, DTE up
*Jun 26 18:28:45.922: datagramstart = 0xC318D54, datagramsize = 13
*Jun 26 18:28:45.922: FR encap = 0xFCF10309
*Jun 26 18:28:45.922: 00 75 01 01 01 03 02 32 31
*Jun 26 18:28:45.922:
*Jun 26 18:28:45.922: Serial0/0/0(in): Status, myseq 50, pak size 13
*Jun 26 18:28:45.922: RT IE 1, length 1, type 1
*Jun 26 18:28:45.922: KA IE 3, length 2, yourseq 50, myseq 50
*Jun 26 18:28:45.922: PVC IE 0x7 , length 0x6 , dlci 103 , status 0x2 , bw 0
```

b. Emita el comando **undebug all** para desactivar la depuración.

Nota: este comando se puede abreviar a **u all**. Esto es útil cuando la información de depuración satura la pantalla.

```
R1# undebug all
All possible debugging has been turned off
```

Paso 2: Eliminar el mapa de tramas IPv4 del R1.

a. Emita el comando **no frame-relay map** para eliminar el mapa de tramas IPv4 en el R1.

```
R1(config)# interface s0/0/0
R1(config-if)# no frame-relay map ip 10.1.1.2 103 broadcast
```

b. Emita el comando **debug ip icmp** en el R1.

```
R1# debug ip icmp
ICMP packet debugging is on
```

c. Haga ping a R1 desde R3. Los pings no deberían realizarse correctamente. Sin embargo, los mensajes de depuración en el R1 muestran que los paquetes ICMP del R3 llegan al R1.

Nota: debería ver mensajes de consola que informan que la adyacencia EIGRP se activa y se desactiva. Esto a veces se denomina “inestabilidad”.

```
R3# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)


R1#
*Jun 26 20:12:35.693: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2, topology
BASE, dscp 0 topoid 0
R1#
*Jun 26 20:12:37.689: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2, topology
BASE, dscp 0 topoid 0
R1#
```



```
*Jun 26 20:12:39.689: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2, topology
BASE, dscp 0 topoid 0
R1#
*Jun 26 20:12:41.689: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2, topology
BASE, dscp 0 topoid 0
R1#
*Jun 26 20:12:43.689: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2, topology
BASE, dscp 0 topoid 0
```

¿Por qué falla el ping?

_____

_____

El ping falla porque el R1 no tiene forma de responder. Sin una forma de asignar la dirección IP del R3 a un DLCI de capa 2, no puede enrutar la respuesta y descarta el paquete.

d. Emita el comando **show frame-relay map** en el R1. Falta el mapa IPv4 para el R3 en la lista.

```
R1# show frame-relay map
Serial0/0/0 (up): ipv6 FE80::3 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ip 10.1.1.1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::3 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
```

e. Emita el comando **undebug all** para desactivar la depuración en el R1.

```
R1# undebug all
All possible debugging has been turned off
```

f. Vuelva a aplicar el comando **frame-relay map ip** a S0/0/0 en el R1, pero sin utilizar la palabra clave **broadcast**.

```
R1(config)# interface s0/0/0
R1(config-if)# frame-relay map ip 10.1.1.2 103
```

g. Haga ping a R1 desde R3. Los pings deberían realizarse correctamente, pero la adyacencia EIGRP sigue siendo inestable. Pueden pasar unos minutos entre cada mensaje debido a los temporizadores de EIGRP.

```
R3# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1(config-if)#
*Jun 26 20:25:10.871: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is down: Interface PEER-TERMINATION received
*Jun 26 20:28:13.673: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is up: new adjacency
R1(config-if)#
```



```
*Jun 26 20:31:18.185: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is down: retry limit exceeded
R1(config-if)#
*Jun 26 20:32:00.977: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is up: new adjacency
R1(config-if)#
*Jun 26 20:35:05.489: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is down: retry limit exceeded
```

¿Por qué la adyacencia EIGRP sigue siendo inestable?

_____

Sin la palabra clave **broadcast**, el tráfico de multidifusión no se reenvía a través del DLCI especificado en la instrucción de mapa de tramas.

h. Reemplace la instrucción de mapa de Frame Relay y, esta vez, incluya la palabra clave **broadcast**.

```
R1(config-if)# frame-relay map ip 10.1.1.2 103 broadcast
```

i. Verifique que se haya restaurado la tabla de routing completa y que tenga conectividad de extremo a extremo.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
D     192.168.3.0/24 [90/2172416] via 10.1.1.2, 00:01:54, Serial0/0/0
```

Paso 3: Cambiar el tipo de encapsulación de Frame Relay.

El software IOS de Cisco admite dos tipos de encapsulación de Frame Relay: la encapsulación predeterminada de Cisco y la encapsulación IETF basada en estándares.

a. Cambie la encapsulación de Frame Relay en S0/0/1 en el R3 a IETF.

```
R3(config)# interface s0/0/1
R3(config-if)# encapsulation frame-relay ietf
```

b. Emita el comando **show interfaces s0/0/1** en el R3 y el FR. Aunque la encapsulación es diferente en cada interfaz, el enlace sigue activo. Esto se debe a que los routers Cisco comprenden ambos tipos de tramas entrantes. Sin embargo, si tiene routers de diferentes proveedores y utiliza Frame Relay, se debe utilizar el estándar IETF.


```
R3# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY IETF, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  1898, LMI stat recvd 1900, LMI upd recvd 0, DTE LMI up
<resultado omitido>

FR# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  0, LMI stat recvd 0, LMI upd recvd 0
```

c. Restablezca la encapsulación de Frame Relay del R3 a Cisco (la predeterminada).

```
R3(config)# interface s0/0/1
R3(config-if)# encapsulation frame-relay
```

Paso 4: Cambiar el tipo de LMI.

a. Emita el comando **frame-relay lmi-type ansi** en la interfaz S0/0/1 en el R3.

```
R3(config-if)# frame-relay lmi-type ansi
```

b. Deje pasar por lo menos 60 segundos y emita el comando **show interfaces s0/0/1** en el R3. Al cabo de 60 segundos, el estado de la interfaz cambia a activo y después a inactivo, porque el R3 espera LMI de ANSI, y el FR envía LMI de Cisco.

```
R3# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is down
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  2157, LMI stat recvd 2136, LMI upd recvd 0, DTE LMI down
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE  segmentation inactive
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 733/0, interface broadcast
<resultado omitido>
```


c. En el R3, emita el comando **show frame-relay lmi** para mostrar la información de LMI, incluidos el tipo de LMI, el número de tiempos de espera, y el tiempo que pasó desde la última actualización completa.

```
R3# show frame-relay lmi

LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 2158             Num Status msgs Rcvd 2136
  Num Update Status Rcvd 0              Num Status Timeouts 23
  Last Full Status Req 00:00:05         Last Full Status Rcvd 00:04:35
```

d. En el R3, emita el comando **debug frame-relay lmi**. Los paquetes de LMI ya no se muestran de a pares. Si bien se registran todos los mensajes de LMI salientes, no se muestran los mensajes entrantes porque el R3 espera LMI de ANSI, y el FR envía LMI de Cisco.

```
R3# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R3#
*Jun 26 21:49:10.829: Serial0/0/1(out): StEnq, myseq 104, yourseen 0, DTE down
*Jun 26 21:49:10.829: datagramstart = 0xC313554, datagramsize = 14
*Jun 26 21:49:10.829: FR encap = 0x00010308
*Jun 26 21:49:10.829: 00 75 95 01 01 00 03 02 68 00
*Jun 26 21:49:10.829:
R3#
*Jun 26 21:49:20.829: Serial0/0/1(out): StEnq, myseq 105, yourseen 0, DTE down
*Jun 26 21:49:20.829: datagramstart = 0xC317554, datagramsize = 14
*Jun 26 21:49:20.829: FR encap = 0x00010308
*Jun 26 21:49:20.829: 00 75 95 01 01 00 03 02 69 00
*Jun 26 21:49:20.829:
```

e. Restaure el tipo de LMI en el R3 a Cisco. Observe que los mensajes de depuración cambian después de emitir este comando. El número de secuencia de LMI se restableció a 1. El R3 comenzó a comprender los mensajes de LMI provenientes del FR. Una vez que el R3 y el FR intercambiaron mensajes de LMI correctamente, el estado de la interfaz cambia a activo.

```
R3(config)# interface s0/0/1
R3(config-if)# frame-relay lmi-type cisco
R3(config-if)#
*Jun 26 21:51:20.829: Serial0/0/1(out): StEnq, myseq 117, yourseen 0, DTE down
*Jun 26 21:51:20.829: datagramstart = 0xC31F254, datagramsize = 14
*Jun 26 21:51:20.829: FR encap = 0x00010308
*Jun 26 21:51:20.829: 00 75 95 01 01 00 03 02 75 00
*Jun 26 21:51:20.829:
R3(config-if)#
*Jun 26 21:51:30.829: Serial0/0/1(out): StEnq, myseq 1, yourseen 0, DTE down
*Jun 26 21:51:30.829: datagramstart = 0xC31F3D4, datagramsize = 13
*Jun 26 21:51:30.829: FR encap = 0xFCF10309
*Jun 26 21:51:30.829: 00 75 01 01 00 03 02 01 00
```

```
*Jun 26 21:51:30.829:
*Jun 26 21:51:30.829: Serial0/0/1(in): Status, myseq 1, pak size 21
*Jun 26 21:51:30.829: RT IE 1, length 1, type 0
*Jun 26 21:51:30.829: KA IE 3, length 2, yourseq 1 , myseq 1
*Jun 26 21:51:30.829: PVC IE 0x7 , length 0x6 , dlci 301, stat
R3(config-if)#us 0x2 , bw 0
R3(config-if)#
*Jun 26 21:51:40.829: Serial0/0/1(out): StEnq, myseq 2, yourseen 1, DTE down
*Jun 26 21:51:40.829: datagramstart = 0xC313B54, datagramsize = 13
*Jun 26 21:51:40.829: FR encap = 0xFCF10309
*Jun 26 21:51:40.829: 00 75 01 01 01 03 02 02 01
*Jun 26 21:51:40.829:
*Jun 26 21:51:40.829: Serial0/0/1(in): Status, myseq 2, pak size 21
*Jun 26 21:51:40.829: RT IE 1, length 1, type 0
*Jun 26 21:51:40.829: KA IE 3, length 2, yourseq 2 , myseq 2
*Jun 26 21:51:40.829: PVC IE 0x7 , length 0x6 , dlci 301, stat
R3(config-if)#us 0x2 , bw 0
*Jun 26 21:51:51.829: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config-if)#
```

f. Emita el comando **undebug all** para finalizar la depuración.

```
R3# undebug all
All possible debugging has been turned off
```

Parte 5: Configurar una subinterfaz Frame Relay

Frame Relay admite dos tipos de subinterfaces: punto a punto y punto a multipunto. Las subinterfaces punto a multipunto admiten topologías de accesos múltiples sin difusión. Por ejemplo, una topología hub-and-spoke utiliza una subinterfaz punto a multipunto. En la parte 5, creará una subinterfaz punto a punto.

Paso 1: Crear nuevos PVC entre el R1 y el R3 en el router FR.

```
FR(config)# interface s0/0/0
FR(config-if)# frame-relay route 113 interface s0/0/1 311
FR(config-if)# interface s0/0/1
FR(config-if)# frame-relay route 311 interface s0/0/0 113
```

Paso 2: Crear y configurar una subinterfaz punto a punto en el R1 y el R3.

Nota: se debe especificar la encapsulación de Frame Relay en la interfaz física antes de que se puedan crear las subinterfaces.

a. Cree la subinterfaz 113 como interfaz punto a punto en el R1.

```
R1(config)# interface s0/0/0.113 point-to-point
R1(config-subif)# ip address 10.1.1.5 255.255.255.252
R1(config-subif)# ipv6 address 2001:db8:acad:d::1/64
R1(config-subif)# ipv6 address fe80::1 link-local
R1(config-subif)# frame-relay interface-dlci 113
R1(config-fr-dlci)#
```


b. Cree la subinterfaz 311 como subinterfaz punto a punto en el R3.

```
R3(config)# interface s0/0/1.311 point-to-point
R3(config-subif)# ip address 10.1.1.6 255.255.255.252
R3(config-subif)# ipv6 address 2001:db8:acad:d::3/64
R3(config-subif)# ipv6 address fe80::3 link-local
R3(config-subif)# frame-relay interface-dlci 311
R3(config-fr-dlci)#
```

c. Verifique la conectividad.

```
R1# ping 10.1.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1# ping 2001:db8:acad:d::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:D::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3# ping 10.1.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R3# ping 2001:db8:acad:d::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:D::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

d. Emita el comando **show frame-relay pvc** en el R1 y el R3 para mostrar el estado del PVC.

```
R1# show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

             Active     Inactive      Deleted       Static
  Local          2            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

  input pkts 1170          output pkts 1408         in bytes 92566
  out bytes 105327         dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
```



```
  out bcast pkts 1160      out bcast bytes 89034
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 07:53:13, last time pvc status changed 00:35:58

DLCI = 113, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.113

  input pkts 86            output pkts 494          in bytes 20916
  out bytes 45208          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 464       out bcast bytes 42088
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:35:58, last time pvc status changed 00:35:58

R3# show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          2            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 301, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

  input pkts 1406          output pkts 1176         in bytes 105143
  out bytes 93110          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 1038      out bcast bytes 80878
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 07:51:07, last time pvc status changed 00:37:16

DLCI = 311, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1.311

  input pkts 513           output pkts 114          in bytes 47072
  out bytes 30360          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 74        out bcast bytes 26200
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:11:06, last time pvc status changed 00:37:16
```


e. Emita el comando **show frame-relay route** en el FR para verificar el estado de las instrucciones de mapa de Frame Relay.

```
FR# show frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0/0     103             Serial0/0/1     301             active
Serial0/0/0     113             Serial0/0/1     311             active
Serial0/0/1     301             Serial0/0/0     103             active
Serial0/0/1     311             Serial0/0/0     113             active
```

f. Emita el comando **show frame-relay map** en el R1 y el R3 para verificar el estado de las instrucciones de mapa de Frame Relay.

```
R1# show frame-relay map
Serial0/0/0 (up): ip 10.1.1.2 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 FE80::3 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ip 10.1.1.1 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0 (up): ipv6 2001:DB8:ACAD:B::3 dlci 103(0x67,0x1870), static,
              CISCO, status defined, active
Serial0/0/0.113 (up): point-to-point dlci, dlci 113(0x71,0x1C10), broadcast
          status defined, active

R3# show frame-relay map
Serial0/0/1 (up): ipv6 FE80::1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1 (up): ipv6 2001:DB8:ACAD:B::3 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.2 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ipv6 2001:DB8:ACAD:B::1 dlci 301(0x12D,0x48D0), static,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.1 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1.311 (up): point-to-point dlci, dlci 311(0x137,0x4C70), broadcast
          status defined, active
```


Reflexión<X1/>

1. ¿Qué es un PVC y cómo se utiliza?

   _____

   _____

   _____

   Un PVC es un circuito virtual permanente. Esto es una conexión de capa 2 creada entre las terminales a través de una nube de Frame Relay. Puede haber varios PVC por interfaz física, lo que permite que haya varias conexiones punto a punto o punto a multipunto.

2. ¿Cuál es el propósito de un DLCI?

   _____

   Un DLCI es una dirección de Frame Relay de capa 2 que ARP inverso utiliza para obtener una dirección IP de capa 3 asociada.

3. ¿Cuál es el propósito de la interfaz de administración local (LMI) en una red Frame Relay?

   _____

   _____

   _____

   _____

   La LMI es un protocolo de señalización que intercambia información entre un router y un switch Frame Relay. La LMI intercambia información sobre los keepalives, el estado del PVC (activo, inactivo, eliminado, sin utilizar) y las direcciones IP (cuando ARP inverso está habilitado). Esta información se usa como mecanismo de estado entre el router (DTE) y el switch Frame Relay (DCE).

4. ¿Por qué utilizaría subinterfaces con Frame Relay?

   _____

   _____

   _____

   _____

   Las subinterfaces se ocupan de las limitaciones de las redes Frame Relay al proporcionar una forma de subdividir una red Frame Relay de malla parcial en una cantidad de subredes más pequeñas de malla completa o punto a punto. A cada subred se le asigna su propio número de red y aparece ante los protocolos como si se pudiera llegar a ella mediante una interfaz diferente.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router R1 (después de las partes 1 y 2 de esta práctica de laboratorio)

```
R1# show run
Building configuration...

Current configuration : 1606 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
```



```
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 shutdown
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:B::1/64
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 password 7 070C285F4D06
 logging synchronous
 login
line aux 0
line 2
```



```
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 094F471A1A0A
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router FR (después de las partes 1 y 2 de esta práctica de laboratorio)

```
FR# show run
Building configuration...

Current configuration : 1671 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FR
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
frame-relay switching
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
```



```
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 103 interface Serial0/0/1 301
!
interface Serial0/0/1
 no ip address
 encapsulation frame-relay
 clock rate 128000
 frame-relay intf-type dce
 frame-relay route 301 interface Serial0/0/0 103
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 094F471A1A0A
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 01100F175804
 login
```



```
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R3 (después de las partes 1 y 2 de esta práctica de laboratorio)

```
R3# sh run
Building configuration...

Current configuration : 1674 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:C::3/64
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
```



```
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 shutdown
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:B::3/64
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 0822455D0A16
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 070C285F4D06
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R1 (después de la parte 3 de esta práctica de laboratorio)

```
R1# sh run
Building configuration...

Current configuration : 2055 bytes
!
```



```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 eigrp 1
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:B::1/64
 ipv6 eigrp 1
 clock rate 128000
 frame-relay map ipv6 2001:DB8:ACAD:B::1 103
 frame-relay map ip 10.1.1.1 103
```



```
 frame-relay map ipv6 FE80::3 103 broadcast
 frame-relay map ipv6 2001:DB8:ACAD:B::3 103
 frame-relay map ip 10.1.1.2 103 broadcast
 no frame-relay inverse-arp
!
interface Serial0/0/1
 no ip address
 shutdown
!
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 eigrp router-id 1.1.1.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 password 7 070C285F4D06
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 094F471A1A0A
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Router FR (después de la parte 3 de esta práctica de laboratorio)

```
FR# show run
Building configuration...

Current configuration : 1671 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FR
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
frame-relay switching
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
```



```
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 103 interface Serial0/0/1 301
!
interface Serial0/0/1
 no ip address
 encapsulation frame-relay
 clock rate 128000
 frame-relay intf-type dce
 frame-relay route 301 interface Serial0/0/0 103
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 094F471A1A0A
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 01100F175804
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R3 (después de la parte 3 de esta práctica de laboratorio)

```
R3# show run
Building configuration...

Current configuration : 2123 bytes
!
version 15.2
service timestamps debug datetime msec
```



```
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:C::3/64
 ipv6 eigrp 1
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:B::3/64
```



```
 ipv6 eigrp 1
 frame-relay map ipv6 2001:DB8:ACAD:B::3 301
 frame-relay map ip 10.1.1.2 301
 frame-relay map ipv6 FE80::1 301 broadcast
 frame-relay map ipv6 2001:DB8:ACAD:B::1 301
 frame-relay map ip 10.1.1.1 301 broadcast
 no frame-relay inverse-arp
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 eigrp router-id 3.3.3.3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 eigrp router-id 3.3.3.3
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 0822455D0A16
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 070C285F4D06
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R1 (final)

```
R1# show run
Building configuration...
```



```
Current configuration : 2296 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 eigrp 1
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
```



```
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:B::1/64
 ipv6 eigrp 1
 clock rate 128000
 frame-relay map ip 10.1.1.2 103 broadcast
 frame-relay map ipv6 FE80::3 103 broadcast
 frame-relay map ipv6 2001:DB8:ACAD:B::1 103
 frame-relay map ip 10.1.1.1 103
 frame-relay map ipv6 2001:DB8:ACAD:B::3 103
 no frame-relay inverse-arp
!
interface Serial0/0/0.113 point-to-point
 ip address 10.1.1.5 255.255.255.252
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:D::1/64
 frame-relay interface-dlci 113
!
interface Serial0/0/1
 no ip address
 shutdown
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
 eigrp router-id 1.1.1.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 password 7 104D000A0618
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```



```
 stopbits 1
line vty 0 4
 password 7 121A0C041104
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router FR (final)

```
FR# show run
Building configuration...

Current configuration : 1769 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FR
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
frame-relay switching
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
```



```
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 103 interface Serial0/0/1 301
 frame-relay route 113 interface Serial0/0/1 311
!
interface Serial0/0/1
 no ip address
 encapsulation frame-relay
 clock rate 128000
 frame-relay intf-type dce
 frame-relay route 301 interface Serial0/0/0 103
 frame-relay route 311 interface Serial0/0/0 113
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 0822455D0A16
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 14141B180F0B
 login
 transport input all
!
scheduler allocate 20000 1000
```



```
!
end
```

Router R3 (final)

```
R3# show run
Building configuration...

Current configuration : 2298 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:C::3/64
 ipv6 eigrp 1
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```



```
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:B::3/64
 ipv6 eigrp 1
 frame-relay map ipv6 FE80::1 301 broadcast
 frame-relay map ipv6 2001:DB8:ACAD:B::3 301
 frame-relay map ip 10.1.1.2 301
 frame-relay map ipv6 2001:DB8:ACAD:B::1 301
 frame-relay map ip 10.1.1.1 301 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
!
interface Serial0/0/1.311 point-to-point
 ip address 10.1.1.6 255.255.255.252
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:ACAD:D::3/64
 frame-relay interface-dlci 311
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 eigrp router-id 3.3.3.3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ipv6 router eigrp 1
 eigrp router-id 3.3.3.3
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 104D000A0618
 logging synchronous
 login
line aux 0
```



```
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 030752180500
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Práctica de laboratorio: Resolución de problemas de Frame Relay básico (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

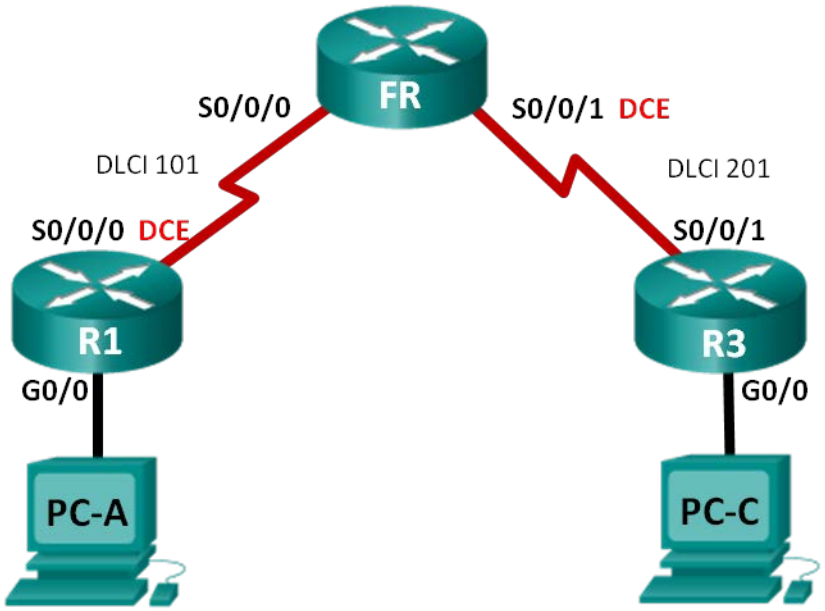


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
FR	S0/0/0	N/A	N/A	N/A
	S0/0/1 (DCE)	N/A	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.1.1.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: Armar la red y cargar las configuraciones de los dispositivos

Parte 2: Resolver problemas de conectividad de capa 3

Parte 3: Resolver problemas de Frame Relay

Información básica/situación

Frame Relay es un protocolo WAN que funciona en las capas física y de enlace de datos del modelo de referencia OSI. A diferencia de las líneas arrendadas, Frame Relay solo requiere un circuito de acceso único al proveedor de servicios de Frame Relay para comunicarse con varios sitios conectados al mismo proveedor. En general, la configuración de Frame Relay en el sitio del cliente es simple; sin embargo, pueden ocurrir problemas de configuración.

En esta práctica de laboratorio, el R1 y el R3 experimentan problemas para comunicarse entre sí. EIGRP no funciona, y también puede haber problemas con la configuración de Frame Relay. Le asignaron el trabajo de buscar y corregir todos los problemas en el R1 y en el R3.

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

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

Nota: el router FR funciona como switch Frame Relay y NO tiene ningún problema de configuración que deba resolver.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Armar la red y cargar las configuraciones de los dispositivos

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

Paso 2: Configurar el direccionamiento en las computadoras.

Paso 3: Cargar los archivos de configuración del router.

Cargue las siguientes configuraciones en el router apropiado. El R1 y el R3 tienen las mismas contraseñas. La contraseña cifrada del modo EXEC privilegiado es **class**, y la contraseña para el acceso a la consola y a VTY es **cisco**.

Configuración del router R1:

```
hostname R1
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
! no shutdown
interface Serial0/0/0
```



```
 ip address 10.1.1.5 255.255.255.252
!ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 clock rate 128000
 frame-relay map ip 10.1.1.2 101
 !frame-relay map ip 10.1.1.2 101 broadcast
 !frame-relay map ip 10.1.1.1 101
 no frame-relay inverse-arp
 no shutdown
router eigrp 1
 network 10.1.0.0 0.0.0.3
 !network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 eigrp router-id 1.1.1.1
 no auto-summary
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
end
```

Configuración del router R3:

```
hostname R3
enable secret class
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.30.1 255.255.255.0
!ip address 192.168.3.1 255.255.255.0
no shutdown
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.2 201
 frame-relay map ip 10.1.1.1 202 broadcast
!frame-relay map ip 10.1.1.1 201 broadcast
 no frame-relay inverse-arp
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
!network 192.168.3.0
 eigrp router-id 3.3.3.3
line con 0
 password cisco
```



```
 logging synchronous
 login
line vty 0 4
 password cisco
 login
end
```

Configuración del switch Frame Relay (router FR):

```
hostname FR
frame-relay switching
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 101 interface Serial0/0/1 201
 no shutdown
interface Serial0/0/1
 no ip address
 encapsulation frame-relay
 clock rate 2000000
 frame-relay intf-type dce
 frame-relay route 201 interface Serial0/0/0 101
 no shutdown
end
```

Paso 4: Guarde su configuración.

Parte 2: Resolver problemas de conectividad de capa 3

En la parte 2, verificará que se haya establecido la conectividad de capa 3 en todas las interfaces. Deberá probar la conectividad IPv4 para todas las interfaces de los dispositivos.

Paso 1: Verifique que las interfaces que se indican en la tabla de direccionamiento estén activas y configuradas con la información de dirección IP correcta.

a. Emita el comando **show ip interface brief** en el R1 y el R3 para verificar que las interfaces estén en estado up/up (activo/activo).

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         192.168.1.1     YES manual administratively down down
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                10.1.1.5        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down

R3# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
```

```
GigabitEthernet0/0         192.168.30.1    YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.1.1.2        YES manual up                    up
```

b. Emita el comando **show run | section interface** para ver todos los comandos relacionados con interfaces.

R1:

```
R1# show run | section interface
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 ip address 10.1.1.5 255.255.255.252
 encapsulation frame-relay
 clock rate 128000
 frame-relay map ip 10.1.1.2 101
 no frame-relay inverse-arp
interface Serial0/0/1
 no ip address
 shutdown
```

R3:

```
R3# show run | section interface
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 202 broadcast
 frame-relay map ip 10.1.1.2 201
 no frame-relay inverse-arp
```

c. Resuelva todos los problemas que detecte. Registre los comandos utilizados para corregir la configuración.

_____

_____

_____

_____

```
R1(config)# interface g0/0
R1(config-if)# no shutdown
R1(config-if)# interface s0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.252

R3(config)# interface g0/0
R3(config-if)# ip address 192.168.3.1 255.255.255.0
```

d. Mediante el uso de los comandos **show**, verifique que las interfaces de los routers R1 y R3 coincidan con las direcciones IP en la tabla de direccionamiento.

Paso 2: Verificar la configuración EIGRP en el R1 y el R3.

a. Emita el comando **show ip protocols** en el R1 y el R3.

R1:

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
```



```
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.0.0/30
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

R3:

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 3.3.3.3
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.1.0/30
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

b. Resuelva todos los problemas que detecte. Registre sus respuestas a continuación.

_____

_____

_____

_____

```
R1(config)# router eigrp 1
R1(config-router)# no network 10.1.0.0 0.0.0.3
```



```
R1(config-router)# network 10.1.1.0 0.0.0.3

R3(config)# router eigrp 1
R3(config-router)# network 192.168.3.0
```

c. Emita un comando **show ip route** en el R1 y el R3. ¿Se muestra alguna ruta EIGRP en la tabla de routing del R1 o el R3? _____ No

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0

R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.2/32 is directly connected, Serial0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

Parte 3: Resolución de problemas de Frame Relay

Paso 1: Probar la conectividad IPv4 de extremo a extremo.

Nota: el FR (el switch Frame Relay) NO tiene ninguna interfaz para hacer ping.

Haga ping a todas las interfaces activas en el R1 y el R3. ¿Tuvieron éxito los pings? Registre los resultados de los pings en la tabla siguiente:

Router	Interfaces activas de los routers			
	G0/0 del R1	S0/0/0 del R1	G0/0 del R3	S0/0/1 del R3
R1	Sí	No	No	No
R3	No	No	Sí	Sí

Debido a que se verificaron y se corrigieron los problemas de direccionamiento IPv4 y de configuración EIGRP, es probable que existan problemas con la configuración de Frame Relay.

Paso 2: Verificar la configuración de Frame Relay en el R1 y el R3.

a. Emita el comando **show frame-relay pvc** en el R1 y el R3.

```
R1# show frame-relay pvc
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

                Active      Inactive      Deleted       Static
  Local            1             0            0            0
  Switched         0             0            0            0
  Unused           0             0            0            0

DLCI = 101, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

  input pkts 10             output pkts 15           in bytes 1040
  out bytes 1560            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0           in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 04:20:07, last time pvc status changed 00:59:58

R3# show frame-relay pvc
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

                Active      Inactive      Deleted       Static
  Local            1             0            1            0
  Switched         0             0            0            0
  Unused           0             0            0            0
```



```
DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

  input pkts 20             output pkts 10           in bytes 2080
  out bytes 1040            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0           in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 04:16:10, last time pvc status changed 01:03:33

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = DELETED, INTERFACE = Serial0/0/1

  input pkts 0              output pkts 0            in bytes 0
  out bytes 0               dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0           in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 04:16:10, last time pvc status changed 01:06:12
```

b. Emita el comando **show frame-relay map** en el R1 y el R3.

R1:

```
R1# show frame-relay map
Serial0/0/0 (up): ip 10.1.1.2 dlci 101(0x65,0x1850), static,
              CISCO, status defined, active
```

R3:

```
R3# show frame-relay map
Serial0/0/1 (up): ip 10.1.1.2 dlci 201(0xC9,0x3090), static,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.1 dlci 202(0xCA,0x30A0), static,
              broadcast,
              CISCO, status deleted
```

c. Emita el comando **show frame-relay lmi** en el R1 y el R3.

R1:

```
R1# show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 6220             Num Status msgs Rcvd 6221
```



```
  Num Update Status Rcvd 0              Num Status Timeouts 0
  Last Full Status Req 00:00:40         Last Full Status Rcvd 00:00:40
```

R3:

```
R3# show frame-relay lmi

LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 6227             Num Status msgs Rcvd 6228
  Num Update Status Rcvd 0              Num Status Timeouts 0
  Last Full Status Req 00:00:56         Last Full Status Rcvd 00:00:56
```

d. Resuelva todos los problemas que detecte. Registre sus respuestas a continuación.

_____

_____

_____

_____

_____

```
R1(config)# interface s0/0/0
R1(config-if)# frame-relay map ip 10.1.1.2 101 broadcast
R1(config-if)# frame-relay map ip 10.1.1.1 101

R3(config)# interface s0/0/1
R3(config-if)# no frame-relay map ip 10.1.1.1 202 broadcast
R3(config-if)# frame-relay map ip 10.1.1.1 201 broadcast
R3(config-if)# frame-relay map ip 10.1.1.2 201
```

Nota: después de introducir los comandos anteriores para solucionar los problemas de Frame Relay, la comunicación entre el R1, el R3 y el switch Frame Relay puede demorar unos minutos antes de que se resuelva toda la comunicación DLCI.

Paso 3: Verificar las configuraciones de Frame Relay y EIGRP.

a. Emita un comando **show ip route eigrp** en el R1 y el R3. ¿Se indican las redes LAN en el resultado? _____ Sí

```
R1# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```



```
Gateway of last resort is not set

D     192.168.3.0/24 [90/2172416] via 10.1.1.2, 00:26:36, Serial0/0/0

R3# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.1.0/24 [90/2172416] via 10.1.1.1, 00:27:32, Serial0/0/1
```

b. Emita un comando **show frame-relay map** en el R1 y el R3. ¿Los DLCI están activos? _____ Sí

```
R1# show frame-relay map
Serial0/0/0 (up): ip 10.1.1.1 dlci 101(0x65,0x1850), static,
              CISCO, status defined, active
Serial0/0/0 (up): ip 10.1.1.2 dlci 101(0x65,0x1850), static,
              broadcast,
              CISCO, status defined, active

R3# show frame-relay map
Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.2 dlci 201(0xC9,0x3090), static,
              CISCO, status defined, active
```

Reflexión<X1/>

Describa la metodología de resolución de problemas que utilizó para resolver los problemas en esta práctica de laboratorio. Describa los pasos que se necesitaron para realizar correctamente la tarea.

Las respuestas varían. Se espera que los estudiantes respondan que dividir un problema en pasos más pequeños facilita la resolución de problemas. Resolver por separado los problemas de direccionamiento IP, después los de EIGRP y después los de Frame Relay en lugar de todos a la vez puede facilitar la resolución de problemas.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router R1

```
R1#sh run
Building configuration...

Current configuration : 1482 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain lookup
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
```



```
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 clock rate 128000
 frame-relay map ip 10.1.1.1 101
 frame-relay map ip 10.1.1.2 101 broadcast
 no frame-relay inverse-arp
!
interface Serial0/0/1
 no ip address
 shutdown
!
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 eigrp router-id 1.1.1.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
```



```
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

R3 del router

```
R3#sh run
Building configuration...

Current configuration : 1448 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain lookup
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
```



```
 frame-relay map ip 10.1.1.2 201
 no frame-relay inverse-arp
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 eigrp router-id 3.3.3.3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Propuesta presupuestaria de Frame Relay (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.

Objetivo

Describir el funcionamiento de Frame Relay.

Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños y después se puede compartir entre los grupos o con la clase.

Situación

Se decidió que en su empresa se utilizará la tecnología Frame Relay para proporcionar conectividad de video entre la ubicación de la oficina principal y dos sucursales. Además, la empresa utilizará la nueva red para redundancia en caso de que la conectividad de la red ISP actual se interrumpa por algún motivo.

Como suele suceder con cualquier tipo de actualización de red, debe desarrollar un presupuesto para el administrador.

Después de investigar, decide utilizar este sitio web de Frame Relay para realizar el análisis de costos. Los costos que se indican en el sitio son una representación de los costos reales de ISP; solo se mencionan para ayudarlo a diseñar el análisis de costos.

Para obtener instrucciones más detalladas, abra el PDF que acompaña a esta actividad.

Recursos

- Software de Packet Tracer
- Software de procesamiento de texto o de hoja de cálculo

Instrucciones

Paso 1: Utilice Packet Tracer para mostrar la oficina doméstica y dos sucursales.

a. Utilice la herramienta Note (Nota) para asignar un nombre a los tres routers requeridos.

b. Incluya un router Frame Relay para mostrar dónde se colocará la conectividad en la nube ISP.

c. Incluya la nube ISP en la topología de modo que los administradores puedan visualizar dónde se conectará el nuevo servicio de Frame Relay al dispositivo o router Frame Relay.

Paso 2: Decida cuántas conexiones DLCI necesita desde la oficina doméstica hasta las sucursales.

a. Determine si debe utilizar líneas T1 de 1,544 para todos los circuitos DLCI o una combinación de conexiones de ancho de banda de distintos anchos de banda.

b. Prepárese para justificar las decisiones que tomó en el paso 2a.

Paso 3: Cree una matriz de propuesta de costos de Frame Relay. Incluya los costos aproximados que se encuentran en el sitio web de Frame Relay. Incluya lo siguiente en la matriz:

a. Costos de acceso al ISP
   1) Tarifas del área de servicio
   2) Tarifas del área interestatal
b. Costo de los puertos de Frame Relay
c. Costos de DLCI

Instructor: los estudiantes pueden elegir diseñar más de una matriz para su propuesta de costos; sin embargo, una matriz es suficiente para indicar todos los costos, o bien se pueden diseñar dos para mostrar los costos por única vez y los costos mensuales.

Asegúrese de que todos los estudiantes sepan que los costos de Frame Relay son aproximados y varían según la prestadora de servicios ISP, y que los diferentes ISP cobran distintas tarifas por diferentes servicios.

Paso 4: Presente el análisis de costos para solicitar los comentarios y la aprobación de los administradores de la empresa.

Instructor: solución de ejemplo para la actividad

Ejemplo de topología de Frame Relay

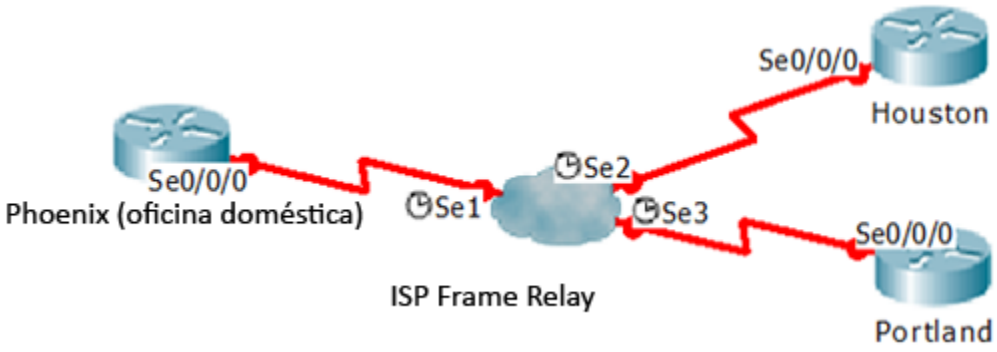


Tabla 1: circuitos virtuales DLCI solicitados

Phoenix a Houston Houston a Phoenix Phoenix a Portland Portland a Phoenix Houston a Portland Portland a Houston
6 Circuitos virtuales DLCI

Tabla 2: análisis de costos de Frame Relay

Costos de acceso (tarifa del área de servicio)	Instalación de la línea T1 en tres sitios (costo por única vez) 3 x USD 634	USD 1902
	Costo mensual de tres líneas T1 3 x USD 175 por mes	$525
Costos de acceso (tarifa interestatal)	Instalación de la línea T1 (consulte el costo del área de servicio; incluido en el costo por única vez, sin costo en este ejemplo únicamente)	USD 0
	Costo mensual de tres líneas T1 (tarifa interestatal) 3 x USD 120 por mes	USD 360
Costo de puertos de Frame Relay	Tres puertos T1 (instalación por única vez) 3 x USD 375	USD 1125
	Costo mensual de tres puertos T1 3 x USD 500 por mes	$1500
Costos de circuitos virtuales DLCI	Seis circuitos virtuales DLCI (consulte la tabla 1) 6 x USD 15 por cada DLCI, por mes	USD 90
		Total de costos por única vez: USD 3027*
*__No__ incluye los costos del equipo local del cliente de internetwork, el cual podría cobrar el ISP o puede comprar la empresa para obtener conectividad de Frame Relay; por ejemplo, CSU/DSU.		
		Total de Costos mensuales: USD 2475
		Costo total de Frame Relay el primer mes: USD 5502

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Puertos de Frame Relay
- Costo de ancho de banda
- Dispositivo Frame Relay
- Requisitos de DLCI
- Topología de Frame Relay

NAT conceptual (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.

Objetivo

Describa las características de NAT.

En esta actividad, se presenta el concepto de la traducción de direcciones de red a los estudiantes.

Situación

Usted trabaja para una universidad o un sistema escolar grande. Por ser el administrador de red, muchos profesores, trabajadores administrativos y otros administradores de red necesitan su ayuda con las redes todos los días. Lo llaman durante toda la jornada laboral y, debido a la cantidad de llamadas telefónicas, no puede completar sus tareas regulares de administración de red.

Debe encontrar la manera de decidir el momento para atender llamadas y las personas a quienes atender. También debe ocultar su número de teléfono para que, cuando llame a alguien, el destinatario vea otro número.

En esta situación, se describe un problema muy frecuente para la mayoría de las pequeñas y medianas empresas. Visite “How Network Address Translation Works”, ubicado en http://computer.howstuffworks.com/nat.htm/printable, para obtener más información sobre la forma en que el mundo digital aborda este tipo de interrupciones de la jornada laboral.

Utilice el PDF que se incluye con esta actividad para seguir reflexionando sobre cómo un proceso, conocido como NAT, podría ser la respuesta al desafío de esta situación.

Recursos

Conexión a Internet

Instrucciones

Paso 1: leer la información del sitio de Internet.

a. Acceda al artículo “How Network Address Translation Works”, ubicado en http://computer.howstuffworks.com/nat.htm/printable.

b. Lea la información proporcionada para presentar los conceptos básicos de NAT.

c. Registre cinco datos que le resulten interesantes sobre el proceso de NAT.

Paso 2: ver los gráficos de NAT.

a. En la misma página de Internet, observe los tipos de NAT que están disponibles para la configuración en la mayoría de las redes.

b. Defina los cuatro tipos de NAT:

1) NAT estática

2) NAT dinámica

3) Sobrecarga de NAT

4) NAT con superposición

Paso 3: reunirse con toda la clase.

a. Comparta sus cinco datos sobre NAT con la clase.

b. A medida que los demás estudiantes compartan los datos que les resultan interesantes con la clase, tilde los datos que usted había registrado.

c. Si un estudiante menciona un dato que usted no registró, agréguelo a la lista.

Información de recursos para el instructor

- Se sugiere mostrar la página web utilizada como base para esta actividad mientras se comparan los datos que comparten los estudiantes después de leer el artículo.
- Antes de continuar con el contenido del currículo, corrija cualquier confusión que se haya generado durante la lectura del artículo.
- Al final de la clase o de la reunión grupal, reitere que NAT es un proceso que se usa para conservar las asignaciones de direcciones de red y para proporcionar una medida de seguridad para los usuarios.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- NAT
- NAT estática
- NAT dinámica
- Sobrecarga de NAT
- NAT con superposición

Práctica de laboratorio: configuración de NAT dinámica y estática (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

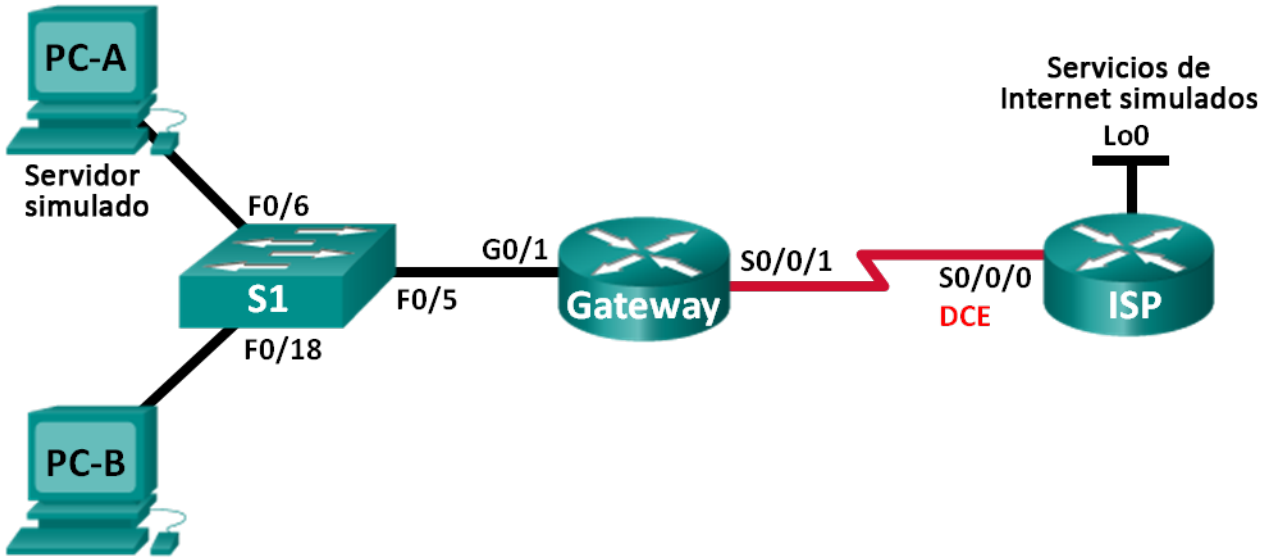


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (Simulated Server)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

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

Parte 1: armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

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

Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2: configurar los equipos host.

Paso 3: inicializar y volver a cargar los routers y los switches según sea necesario.

Paso 4: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

c. Establezca la frecuencia de reloj en **128000** para las interfaces seriales DCE.

d. Configure el nombre del dispositivo como se muestra en la topología.

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Paso 5: crear un servidor web simulado en el ISP.

a. Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Habilite el servicio del servidor HTTP en el ISP.

```
ISP(config)# ip http server
```

c. Configure el servicio HTTP para utilizar la base de datos local.

```
ISP(config)# ip http authentication local
```

Paso 6: configurar el routing estático.

a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

Paso 8: Verificar la conectividad de la red

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

Parte 2: configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Paso 1: configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```


Paso 2: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Paso 3: probar la configuración.

a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = _____ 209.165.200.225

¿Quién asigna la dirección global interna?

_____

El router del pool de la NAT.

¿Quién asigna la dirección local interna?

_____

El administrador de la estación de trabajo.

b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? _____ 1, las respuestas varían.

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? _____ tcp

¿Cuáles son los números de puerto que se usaron?

Global/local interno: _____ 1034, las respuestas varían.

Global/local externo: _____ 23

d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

f. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Parte 3: configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Paso 1: borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```


Paso 2: definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Paso 3: verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  FastEthernet0/1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Paso 4: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Paso 5: definir la NAT desde la lista de origen interna hasta el conjunto externo.

Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Paso 6: probar la configuración.

a. En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

192.168.1.21 = _____ 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? _____ 1, las respuestas varían.

b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

c. Muestre la tabla de NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

¿Qué protocolo se usó en esta traducción? _____ tcp

¿Qué números de puerto se usaron?

Interno: _____ 1038 a 1052. Las respuestas varían

Externo: _____80

¿Qué número de puerto bien conocido y qué servicio se usaron? _____
puerto 80, www o http

d. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
```



```
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Paso 7: eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Borre las NAT y las estadísticas.

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

d. Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```


Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión<X1/>

1. ¿Por qué debe utilizarse la NAT en una red?

   _____

   _____

   _____

   Las respuestas varían, pero deberían incluir: siempre que no haya suficientes direcciones IP públicas y para evitar el costo de adquisición de direcciones públicas de un ISP. NAT también puede proporcionar una medida de seguridad al ocultar las direcciones internas de las redes externas.

2. ¿Cuáles son las limitaciones de NAT?

   _____

   _____

   _____

   NAT necesita la información de IP o de números de puerto en el encabezado IP y el encabezado TCP de los paquetes para la traducción. Esta es una lista parcial de los protocolos que no se pueden utilizar con NAT: SNMP, LDAP, Kerberos versión. 5.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Gateway (después de la parte 2)

```
Gateway# show run
Building configuration...

Current configuration : 1666 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
```



```
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
```



```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source static 192.168.1.20 209.165.200.225
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Gateway (final)

```
Gateway# show run
Building configuration...

Current configuration : 1701 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
```



```
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
```



```
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224
ip nat inside source list 1 pool public_access
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


ISP (final)

```
ISP# show run
Building configuration...

Current configuration : 1557 bytes
!
! Last configuration change at 09:16:34 UTC Sun Mar 24 2013
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
username webuser privilege 15 secret 4 ZMYyKvmzVsyor8jHyP9ox.cMoz9loLfZN75illtozY2
!
!
!
!
!
interface Loopback0
 ip address 192.31.7.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
```



```
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.201.17 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 209.165.201.18
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
```



```
 password cisco
login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Práctica de laboratorio: Configuración de la traducción de la dirección del puerto (PAT) (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

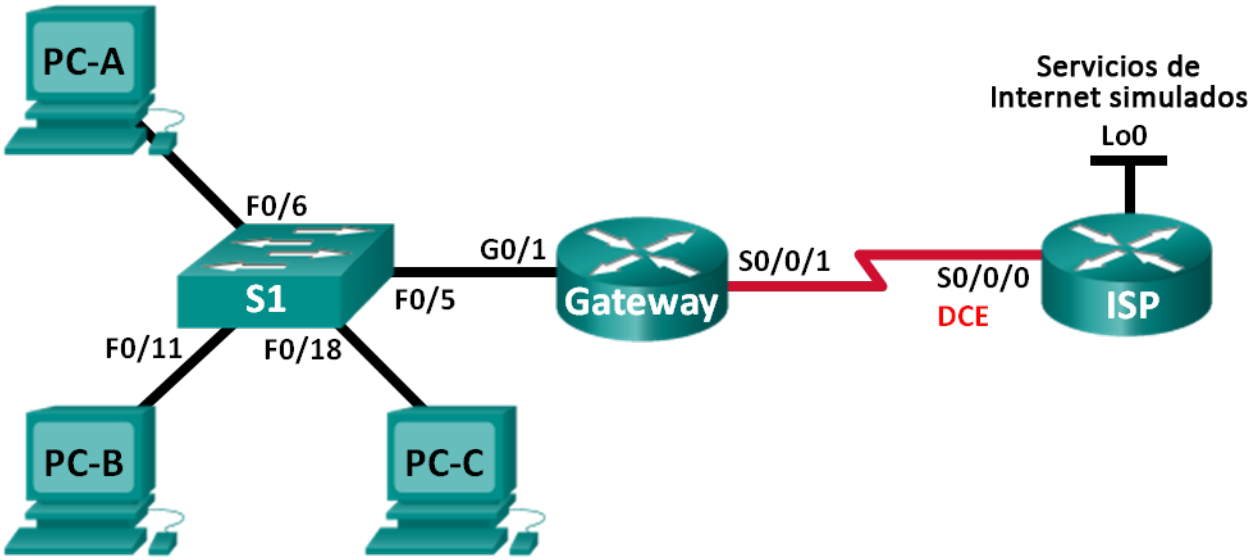


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto. La sobrecarga del conjunto de NAT es una traducción de la dirección del puerto (PAT) que sobrecarga un grupo de direcciones IPv4 públicas.

En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará PAT para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

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

Parte 1: armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

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

Paso 2: configurar los equipos host.

Paso 3: inicializar y volver a cargar los routers y los switches.

Paso 4: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.

c. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

d. Configure el nombre del dispositivo como se muestra en la topología.

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Paso 5: configurar el routing estático.

a. Cree una ruta estática desde el router ISP hasta el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Paso 6: Verificar la conectividad de la red

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Parte 2: configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Paso 1: definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Paso 2: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225  209.165.200.230
netmask 255.255.255.248
```

Paso 3: definir la NAT desde la lista de origen interna hasta el conjunto externo.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Paso 4: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```


Paso 5: verificar la configuración del conjunto de NAT con sobrecarga.

a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
 pool public_access: netmask 255.255.255.248
        start 209.165.200.225 end 209.165.200.230
        type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

c. Muestre las NAT en el router Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1     192.31.7.1:1       192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1     192.31.7.1:1       192.31.7.1:2
```

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? _____ 3

¿Cuántas direcciones IP globales internas se indican? _____ 1

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas? _____ 3

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

_____

_____

El ping fallaría debido a que el router conoce la ubicación de la dirección global interna en la tabla de routing, pero la dirección local interna no se anuncia.

Parte 3: configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Paso 1: borrar las NAT y las estadísticas en el router Gateway.

Paso 2: verificar la configuración para NAT.

a. Verifique que se hayan borrado las estadísticas.

b. Verifique que las interfaces externa e interna estén configuradas para NAT.

c. Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c?

_____

```
Gateway# show ip nat statistics
```

Paso 3: eliminar el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Paso 4: eliminar la traducción NAT de la lista de origen interna al conjunto externo.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Paso 5: asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Paso 6: probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
```

```
Queued Packets: 0
```

c. Muestre las traducciones NAT en el Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.18:3  192.168.1.20:1     192.31.7.1:1       192.31.7.1:3
icmp 209.165.201.18:1  192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.201.18:4  192.168.1.22:1     192.31.7.1:1       192.31.7.1:4
```

Reflexión<X1/>

¿Qué ventajas tiene la PAT?

_____

Las respuestas varían, pero deben incluir que PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para “ocultar” las direcciones privadas de las redes externas.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router Gateway (después de la parte 2)

```
Gateway# show run
Building configuration...

Current configuration : 1790 bytes
```



```
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
```



```
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
ip nat inside source list 1 pool public_access overload
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
login
 transport input all
!
```



```
scheduler allocate 20000 1000
!
end
```

Router Gateway (después de la parte 3)

```
Gateway# show run
Building configuration...

Current configuration : 1711 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
```



```
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface Serial0/0/1 overload
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
!
Control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
```



```
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

ISP del router

```
ISP# show run
Building configuration...

Current configuration : 1487 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
```



```
!
!
!
!
interface Loopback0
 ip address 192.31.7.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.201.17 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 209.165.201.18
!
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
```



```
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Práctica de laboratorio: resolución de problemas de configuración NAT (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
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Objetivos

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

Parte 2: resolver problemas de la NAT estática

Parte 3: resolver problemas de la NAT dinámica

Información básica/situación

En esta práctica de laboratorio, la configuración del router Gateway estuvo a cargo de un administrador de red inexperto de la empresa. Varios errores en la configuración produjeron problemas de NAT. El jefe le solicitó a usted que resuelva y corrija los errores de NAT, y que documente su trabajo. Asegúrese de que la red admita lo siguiente:

- La PC-A funciona como servidor web con una NAT estática y se debe poder llegar a dicha computadora desde el exterior a través de la dirección 209.165.200.254.
- La PC-B funciona como equipo host y recibe dinámicamente una dirección IP del conjunto de direcciones creado con el nombre NAT_POOL, que usa el rango 209.165.200.240/29.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

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

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

En la parte 1, establecerá la topología de la red y configurará los routers con los parámetros básicos. Se incluyen configuraciones adicionales relacionadas con NAT. La configuración NAT para el router Gateway contiene los errores que usted identificará y corregirá a medida que avance con la práctica de laboratorio.

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

Paso 2: configurar los equipos host.

Paso 3: inicializar y volver a cargar el switch y los routers.

Paso 4: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Configure las direcciones IP como se indica en la tabla de direccionamiento.

d. Establezca la frecuencia de reloj en **128000** para las interfaces seriales DCE.

e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Paso 5: configurar el routing estático.

a. Cree una ruta estática del router ISP al rango de direcciones de red públicas 209.165.200.224/27 asignado por el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 s0/0/0
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Paso 6: cargar las configuraciones de los routers.

Se incluyen las configuraciones de los routers. La configuración del router Gateway contiene errores. Identifique y corrija los errores de configuración.

Configuración del router Gateway

```
interface g0/1
 ip nat outside
! ip nat inside
 no shutdown
interface s0/0/0
 ip nat outside
! no ip nat outside
interface s0/0/1
! ip nat outside
 no shutdown
ip nat inside source static 192.168.2.3 209.165.200.254
! ip nat inside source static 192.168.1.3 209.165.200.254
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
! ip nat inside source list NAT_ACL pool NAT_POOL
ip access-list standard NAT_ACL
 permit 192.168.10.0 0.0.0.255
! permit 192.168.1.0 0.0.0.255
banner motd $AUTHORIZED ACCESS ONLY$
end
```

Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

Parte 2: resolver problemas de la NAT estática

En la parte 2, examinará la NAT estática de la PC-A para determinar si se configuró correctamente. Resolverá los problemas de la situación hasta que se verifique la NAT estática correcta.

a. Para resolver problemas de NAT, use el comando **debug ip nat**. Active la depuración de NAT para ver las traducciones en tiempo real a través del router Gateway.

```
Gateway# debug ip nat
```

b. En la PC-A, haga ping a Lo0 en el router ISP. ¿Aparece alguna traducción de depuración NAT en el router Gateway?

_____

No.

c. En el router Gateway, introduzca el comando que permite ver todas las traducciones NAT actuales en dicho router. Escriba el comando en el espacio que se incluye a continuación.

_____

show ip nat translations

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.254    192.168.2.3        ---                ---
```

¿Por qué ve una traducción NAT en la tabla pero no se produjo ninguna cuando se hizo ping de la PC-A a la interfaz loopback del ISP? ¿Qué se necesita para corregir el problema?

_____

La traducción estática es para una dirección local interna incorrecta.

d. Registre todos los comandos que se necesitan para corregir el error de configuración NAT estática.

_____

_____

```
Gateway(config)# no ip nat inside source static 192.168.2.3 209.165.200.254
Gateway(config)# ip nat inside source static 192.168.1.3 209.165.200.254
```

e. En la PC-A, haga ping a Lo0 en el router ISP. ¿Aparece alguna traducción de depuración NAT en el router Gateway?

_____

No

f. En el router Gateway, introduzca el comando que permite observar la cantidad total de NAT actuales. Escriba el comando en el espacio que se incluye a continuación.

_____

show ip nat statistics

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 1, occurred 00:08:12 ago
Outside interfaces:
  GigabitEthernet0/1, Serial0/0/0
Inside interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT_ACL pool NATPOOL refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

¿La NAT estática se realiza correctamente? ¿Por qué?

_____

No se realiza ninguna traducción NAT porque las interfaces G0/1 y S0/0/0 se configuraron con el comando **ip nat outside**. No se asignó ningún área de interfaz activa como interna.

g. En el router Gateway, introduzca el comando que permite ver la configuración actual del router. Escriba el comando en el espacio que se incluye a continuación.

_____

show running-config

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

Current configuration : 1806 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
```



```
 no ip address
 ip nat outside
 ip virtual-reassembly in
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
ip nat inside source static 192.168.1.3 209.165.200.254
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip access-list standard NAT_ACL
 permit 192.168.10.0 0.0.0.255
!
!
!
!
control-plane
!
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
```

```
end
```

h. ¿Existe algún problema en la configuración actual que impida que se realice la NAT estática?

Sí. Las interfaces NAT interna y externa están mal configuradas.

i. Registre todos los comandos que se necesitan para corregir los errores de configuración NAT estática.

```
Gateway(config)# interface g0/1
Gateway(config-if)# no ip nat outside
Gateway(config-if)# ip nat inside
Gateway(config-if)# exit
Gateway(config)# interface s0/0/0
Gateway(config-if)# no ip nat outside
Gateway(config-if)# exit
Gateway(config)# interface s0/0/1
Gateway(config-if)# ip nat outside
Gateway(config-if)# exit
```

j. En la PC-A, haga ping a Lo0 en el router ISP. ¿Aparece alguna traducción de depuración NAT en el router Gateway?

Sí

```
*Mar 18 23:53:50.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [187]
*Mar 18 23:53:50.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [187]
Gateway#
*Mar 18 23:53:51.711: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [188]
*Mar 18 23:53:51.719: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [188]
*Mar 18 23:53:52.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [189]
Gateway#
*Mar 18 23:53:52.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [189]
*Mar 18 23:53:53.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [190]
Gateway#
*Mar 18 23:53:53.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [190]
```

k. Use el comando **show ip nat translations verbose** para verificar la funcionalidad de la NAT estática.

Nota: el valor de tiempo de espera para ICMP es muy corto. Si no ve todas las traducciones en el resultado, vuelva a hacer el ping.

```
Gateway# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.254:1   192.168.1.3:1      198.133.219.1:1    198.133.219.1:1
    create 00:00:04, use 00:00:01 timeout:60000, left 00:00:58,
    flags:
extended, use_count: 0, entry-id: 12, lc_entries: 0
--- 209.165.200.254      192.168.1.3        ---                ---
    create 00:30:09, use 00:00:04 timeout:0,
```



```
    flags:
static, use_count: 1, entry-id: 2, lc_entries: 0
```

¿La traducción de NAT estática se realiza correctamente? _____ Sí

Si no se realiza la NAT estática, repita los pasos anteriores para resolver los problemas de configuración.

Parte 3: resolución de problemas de la NAT dinámica

a. En la PC-B, haga ping a Lo0 en el router ISP. ¿Aparece alguna traducción de depuración NAT en el router Gateway?

_____ No

b. En el router Gateway, introduzca el comando que permite ver la configuración actual del router. ¿Existe algún problema en la configuración actual que impida que se realice la NAT dinámica?

_____

Sí. El conjunto de NAT está mal identificado en la instrucción de origen. La lista de acceso de NAT tiene una instrucción network incorrecta.

c. Registre todos los comandos que se necesitan para corregir los errores de configuración NAT dinámica.

_____

_____

_____

```
Gateway(config)# no ip nat inside source list NAT_ACL pool NATPOOL
Gateway(config)# ip nat inside source list NAT_ACL pool NAT_POOL
Gateway(config)# ip access-list standard NAT_ACL
Gateway(config-std-nacl)# no permit 192.168.10.0 0.0.0.255
Gateway(config-std-nacl)# permit 192.168.1.0 0.0.0.255
```

d. En la PC-B, haga ping a Lo0 en el router ISP. ¿Aparece alguna traducción de depuración NAT en el router Gateway?

_____

Sí

```
*Mar 19 00:01:17.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [198]
*Mar 19 00:01:17.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [198]
Gateway#
*Mar 19 00:01:18.307: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [199]
*Mar 19 00:01:18.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [199]
*Mar 19 00:01:19.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [200]
Gateway#
*Mar 19 00:01:19.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [200]
*Mar 19 00:01:20.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [201]
*Mar 19 00:01:20.311: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [201]
```

e. Use el comando **show ip nat statistics** para ver el uso de NAT.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Peak translations: 3, occurred 00:02:58 ago
Outside interfaces:
  Serial0/0/1
```

```
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT_ACL pool NAT_POOL refcount 1
 pool NAT_POOL: netmask 255.255.255.248
 start 209.165.200.241 end 209.165.200.246
 type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

¿La NAT se realiza correctamente? _____ Sí

¿Qué porcentaje de direcciones dinámicas se asignó? _____ El 16 %

f. Desactive toda depuración con el comando **undebug all**.

Reflexión<X1/>

1. ¿Cuál es el beneficio de una NAT estática?

_____

_____

Una traducción NAT estática permite que los usuarios fuera de la LAN tengan acceso a la computadora o al servidor en la red interna.

2. ¿Qué problemas surgirían si 10 equipos host en esta red intentaran comunicarse con Internet al mismo tiempo?

_____

_____

No existen suficientes direcciones públicas en el conjunto de NAT para satisfacer 10 sesiones de usuario simultáneas, pero a medida que se reduzcan los hosts, distintos hosts podrán obtener las direcciones del conjunto para acceder a Internet.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuración de dispositivos

Router Gateway

```
Gateway#show run
Building configuration...

Current configuration : 1805 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
```



```
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
redundancy
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NAT_POOL
ip nat inside source static 192.168.1.3 209.165.200.254
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
```



```
ip access-list standard NAT_ACL
 permit 192.168.1.0 0.0.0.255
!
!
!
!
control-plane
!
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

ISP del router

```
ISP#show run
Building configuration...

Current configuration : 1482 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
```



```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
!
!
!
!
!
!
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 198.133.219.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.200.226 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
```



```
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 Serial0/0/0
!
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
line vty 5 15
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Revisión de NAT (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.

Objetivo

Configure, verifique y analice la NAT estática, la NAT dinámica y la NAT con sobrecarga.

Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños o grandes.

Situación

La traducción de direcciones de red no se incluye actualmente en el diseño de red de su empresa. Se decidió configurar algunos dispositivos para que utilicen los servicios de NAT para conectarse al servidor de correo.

Antes de implementar la NAT real en la red, usted crea un prototipo mediante un programa de simulación de redes.

Recursos

- Software Packet Tracer
- Software de presentación o de procesamiento de texto

Instrucciones

Paso 1: crear una topología de red muy pequeña con Packet Tracer que incluya, como mínimo, lo siguiente:

a. Dos routers 1941 interconectados
b. Dos switches LAN, uno por router
c. Un servidor de correo conectado a la LAN en un router
d. Una computadora de escritorio o portátil conectada a la LAN en el otro router

Paso 2: asignar direcciones en la topología.

a. Use el direccionamiento privado para todas las redes, los hosts y los dispositivos.
b. El direccionamiento DHCP de la computadora de escritorio o portátil es optativo.
c. El direccionamiento estático para el servidor de correo es obligatorio.

Paso 3: configurar un protocolo de routing para la red.

Paso 4: validar la conectividad de la red completa sin los servicios de NAT.

a. Haga ping de un extremo de la topología y viceversa para asegurarse de que la red funcione plenamente.
b. Resuelva y corrija cualquier problema que impida la funcionalidad total de la red.

Paso 5: configurar los servicios de NAT en uno de los routers del equipo host de escritorio o portátil al servidor de correo.

Paso 6: producir resultados que validen las operaciones de NAT en la red simulada.

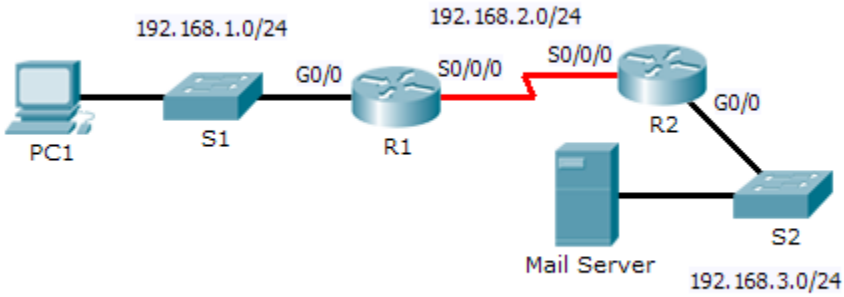
a. Use los comandos **show ip nat statistics**, **show access-lists** y **show ip nat translations** para recopilar información sobre el funcionamiento de NAT en el router.

b. Copie y pegue la información de la topología y de los resultados o guarde capturas de pantalla de dicha información en un documento de presentación o de procesamiento de texto.

Paso 7: explicar el diseño y el resultado de NAT a otro grupo o a la clase.

Ejemplo sugerido de la actividad (los diseños de los estudiantes varían):

Diagrama de topología de NAT




```
R2# show ip nat translations

Pro Inside global   Inside local    Outside local   Outside global
icmp 192.168.1.1:2   192.168.1.2:2   192.168.3.2:2   192.168.3.2:2
```

```
R2# show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: Serial0/0/0
Hits: 2 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool R1 refCount 1
 pool R1: netmask 255.255.255.0
    start 192.168.1.1 end 192.168.1.254
    type generic, total addresses 254 , allocated 1 (0%), misses 0
```

```
R2# show access-lists
Standard IP access list 1
  permit 192.168.1.0 0.0.0.255 (6 match(es))
```

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

NAT

1. Configuración
2. Operación
3. Resolución de problemas

Variedades de banda ancha (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.

Objetivo

Seleccionar las soluciones de banda ancha para admitir la conectividad remota en una red de una pequeña a mediana empresa.

Nota para el instructor:

- Esta actividad se puede completar en forma individual o en grupos pequeños.
- Esta actividad se centra en los tres tipos principales de transmisión de banda ancha que se especifican en el contenido del capítulo.

Situación

Las oportunidades de empleo a distancia en su área local se expanden todos los días. Le ofrecieron empleo como trabajador a distancia para una empresa importante. El nuevo empleador requiere que los trabajadores a distancia tengan acceso a Internet para cumplir con sus responsabilidades laborales.

Investigue los siguientes tipos de conexión a Internet por banda ancha que están disponibles en su área geográfica:

- DSL
- Cable
- Satélite

Considere las ventajas y desventajas de cada variante de banda ancha a medida que registra su investigación, las cuales pueden incluir el costo, la velocidad, la seguridad y la facilidad de implementación o instalación.

Recursos

- Acceso a la World Wide Web
- Software de procesamiento de texto

Paso 1: Investigar tres tipos principales de conexiones a Internet por banda ancha:

- DSL
- Cable
- Satélite

Paso 2: Decidir cuáles serían las opciones de banda ancha importantes para usted como trabajador a distancia en su pequeña oficina u oficina doméstica:

- Costo
- Velocidad
- Seguridad
- Facilidad de implementación
- Confiabilidad

Paso 3: Con las opciones del paso 2, cree una matriz donde se indiquen las ventajas y las desventajas de cada tipo de banda ancha.

Paso 4: Compartir la investigación con la clase o con otro grupo.

Ejemplos sugeridos para la actividad:

Variaciones de banda ancha*

Tipo de banda ancha	Ventajas	Desventajas
DSL	Descargas de alta velocidad de hasta 1,5 Mb/s, que pueden ser más o menos veloces en función del ISP. El servicio de DSL de nivel empresarial ofrece velocidades de datos garantizadas. Utiliza el cableado telefónico existente, pero permite el uso de Internet y el uso de un teléfono de línea al mismo tiempo.	No funcionan todas las líneas telefónicas; es posible que el ISP deba realizar un análisis. La velocidad desciende cuanto más lejos se esté de la oficina central de la compañía telefónica. Puede ser que no tenga tanta disponibilidad como el cable.
Cable	Las velocidades no dependen de la distancia desde la oficina central. Cuenta con velocidades máximas más rápidas que DSL (más de 2 Mb/s), lo cual depende del ISP. Puede ser más económico que DSL, especialmente cuando está unido al servicio de televisión.	Es posible que se requiera la instalación por parte de un profesional. La línea se comparte con otras personas en los vecindarios; las velocidades pueden variar. Es posible que el ISP determine límites de descarga y subida de datos.
Satélite	Proporciona una opción de banda ancha a las áreas rurales o a ubicaciones no tradicionales, aunque prácticamente no hay restricciones geográficas. Las velocidades de descarga son similares a las de DSL y el cable, con descargas de 1 Mb/s.	Puede experimentar interrupciones debido al clima. Puede ser más costoso que DSL o el cable debido al equipo requerido (antena parabólica). Se pueden presentar velocidades más bajas debido a la latencia de las señales satelitales.
*http://reviews.cnet.com/4520-6536_7-726601-5.html (información sobre DSL y cable) *http://www.fcc.gov/guides/getting-broadband (información sobre satélite)		

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Tipos de banda ancha
- DSL
- Cable
- Satélite
- Opciones disponibles para los tipos de banda ancha
- Ventajas y desventajas de banda ancha

Práctica de laboratorio: Investigación de las tecnologías de acceso a Internet por banda ancha (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: Investigar la distribución de banda ancha

Parte 2: Investigar las opciones de acceso por banda ancha para situaciones específicas

Información básica/situación

Si bien las opciones de acceso a Internet por banda ancha aumentaron drásticamente en los últimos años, el acceso por banda ancha varía en gran medida según la ubicación. En esta práctica de laboratorio, investigará la distribución actual de banda ancha y las opciones de acceso por banda ancha para situaciones específicas.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Investigar la distribución de banda ancha

En la parte 1, investigará la distribución de banda ancha en una ubicación geográfica.

Paso 1: Investigar la distribución de banda ancha.

Utilice Internet para investigar las siguientes preguntas:

a. Para el país en el que reside, ¿qué porcentaje de la población está suscrito al servicio de Internet por banda ancha? _____

Desde octubre de 2012, el 72,4% de los estadounidenses tiene una conexión a Internet por banda ancha (88 millones de hogares).

b. ¿Qué porcentaje de la población no cuenta con opciones de Internet por banda ancha? _____

En la actualidad, el 9% de los estadounidenses no cuenta con opciones de Internet por banda ancha.

Paso 2: Investigar la distribución de banda ancha en los Estados Unidos.

Navegue hasta el sitio web www.broadbandmap.gov. El National Broadband Map (Mapa nacional de banda ancha) permite que los usuarios busquen y ubiquen en un mapa la disponibilidad de banda ancha en todo el territorio de los Estados Unidos.

Nota: para obtener información sobre las opciones de acceso y los ISP para ubicaciones fuera de los Estados Unidos, realice una búsqueda en Internet con las palabras clave “acceso por banda ancha XYZ”, donde XYZ representa el nombre del país.

a. Introduzca el código postal, la ciudad y el país que desea investigar y haga clic en **Find Broadband** (Buscar banda ancha). Indique el código postal o la ciudad en el espacio proporcionado.
_____ Las respuestas varían.

b. Haga clic en **Show Wired** (Mostrar cableadas) y **Expand All** (Expandir todo). Si las hubiera, ¿cuáles son las conexiones a Internet por banda ancha cableadas disponibles en esta ubicación? Complete la siguiente tabla. Las respuestas varían. Consulte la siguiente tabla para ver ejemplos.

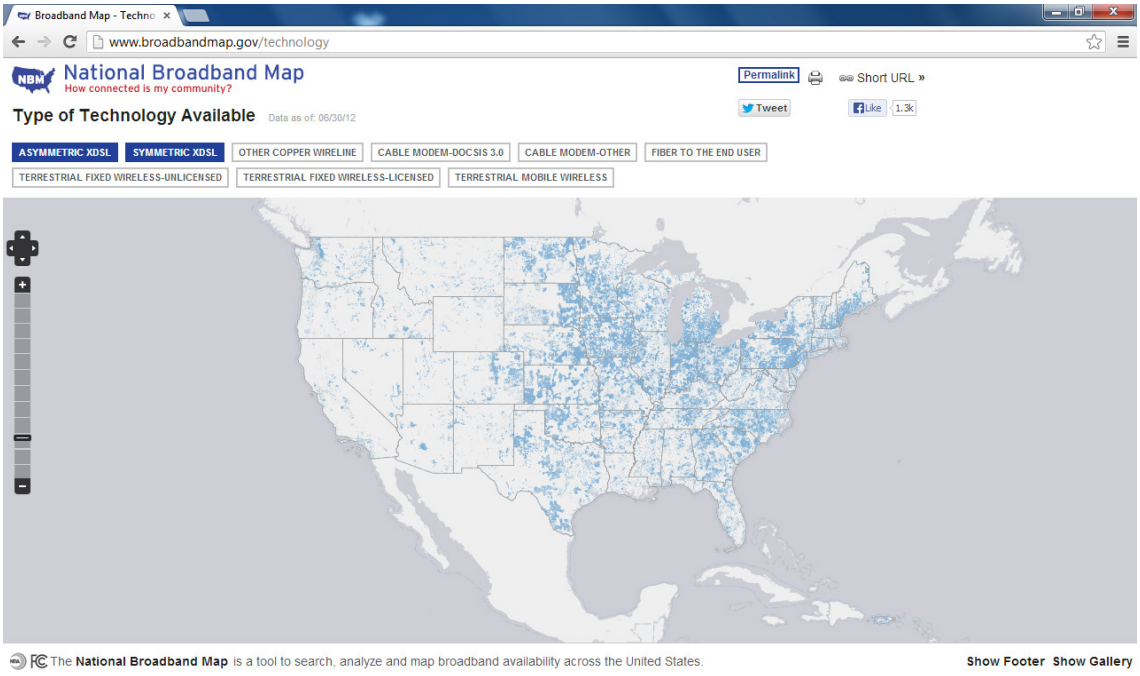
ISP	Tipo de conexión	Velocidad de descarga
Time Warner	Cable	De 10 Mb/s a 25 Mb/s
Frontier	ADSL	De 6 Mb/s a 10 Mb/s

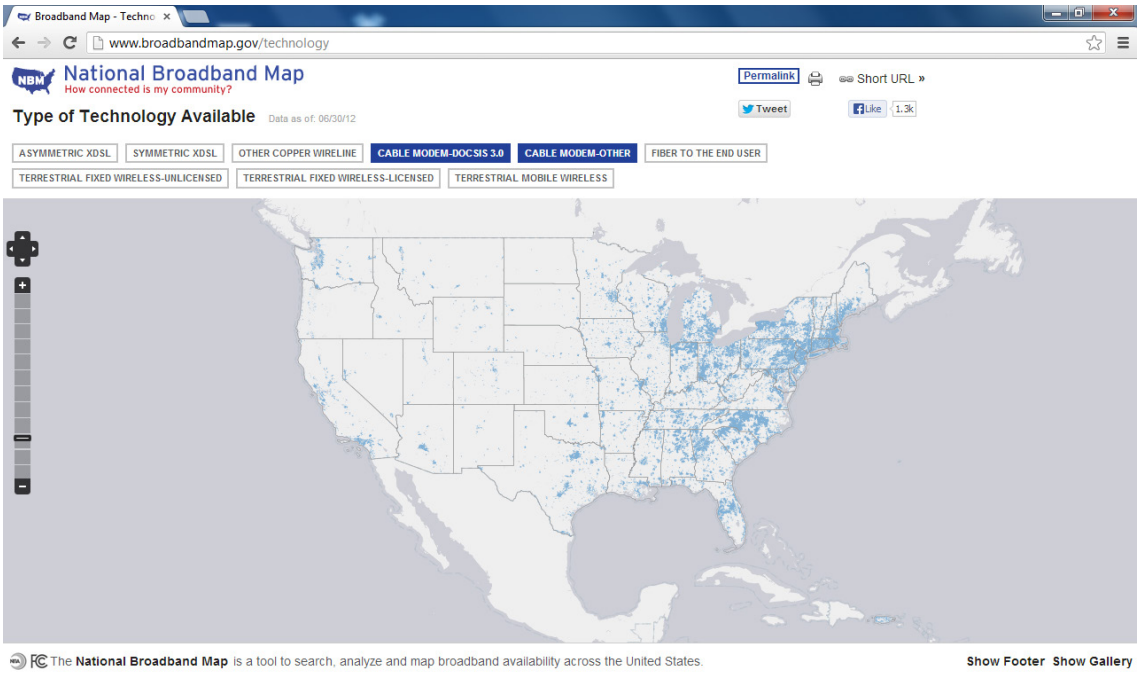
c. Haga clic en **Show Wireless** (Mostrar inalámbricas) y **Expand All** (Expandir todo). Si las hubiera, ¿cuáles son las conexiones a Internet por banda ancha inalámbricas disponibles en esta ubicación? Complete la siguiente tabla. Las respuestas varían. Consulte la siguiente tabla para ver ejemplos.

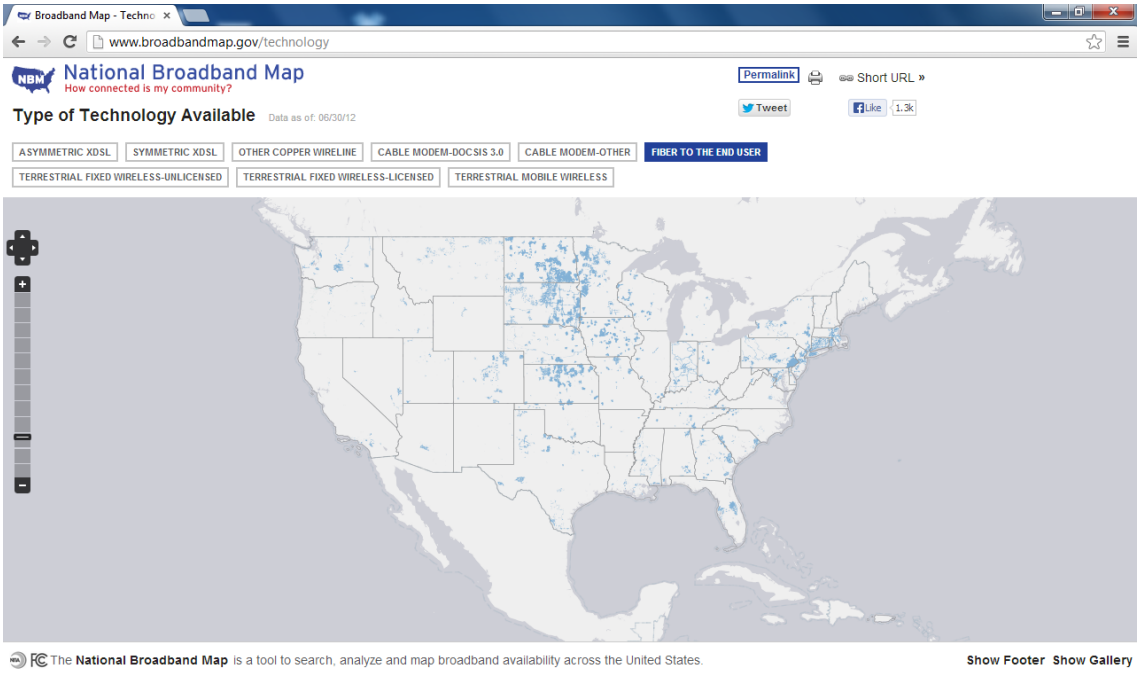
ISP	Tipo de conexión	Velocidad de descarga
Omnicity	Conexión inalámbrica fija	De 1,5 Mb/s a 3 Mb/s
Verizon	Conexión inalámbrica móvil	768 Kpbs-1.5 Mp/s
Sprint-Nextel	Conexión inalámbrica móvil	768 Kpbs-1.5 Mp/s

d. Vuelva a la página de inicio y haga clic en **Explore Map** (Explorar mapa). El mapa interactivo le permite explorar la disponibilidad geográfica de varias opciones de Internet por banda ancha.

e. Resalte cada una de las conexiones cableadas por separado (DSL, cable y fibra óptica). Las selecciones se resaltan en azul oscuro.





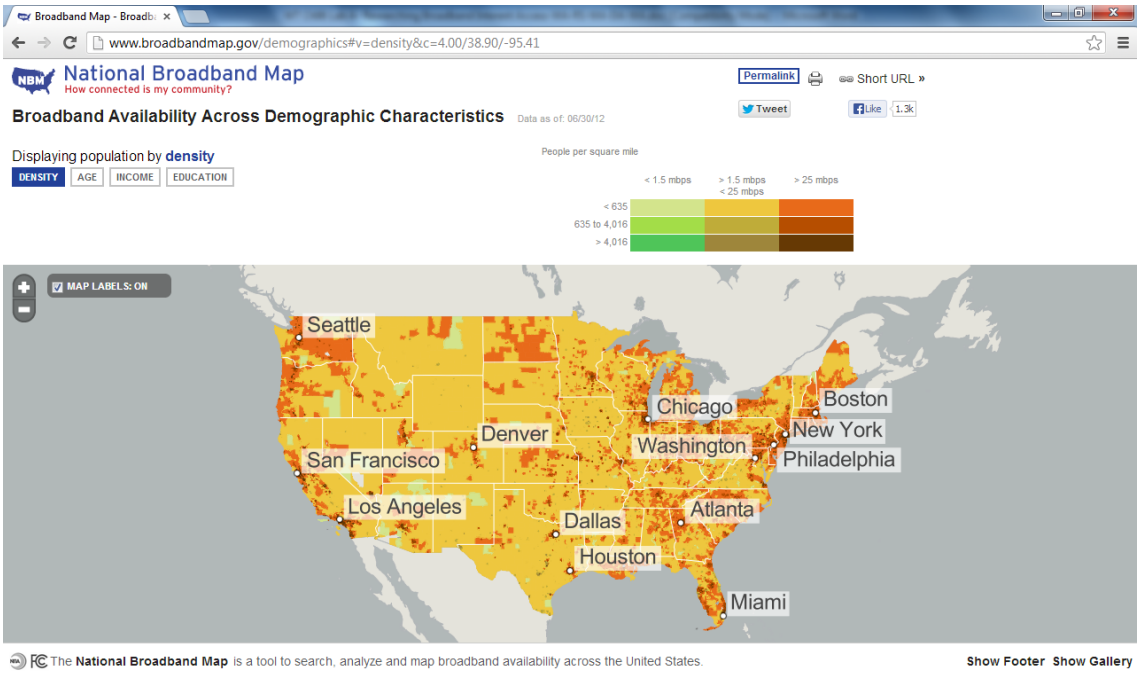


Para las conexiones cableadas, ordene las conexiones de banda ancha cableadas de menor a mayor en términos de área geográfica cubierta. Indique su respuesta en el espacio proporcionado.

_____

Fibra óptica, cable y DSL

f. En la galería de mapas en la parte inferior de la página web, seleccione **Broadband Availability Across Demographic Characteristics** (Disponibilidad de banda ancha a través de las características demográficas). Muestre la población por **Density** (Densidad) y compare la conexión de banda ancha con la distribución de población de los Estados Unidos. ¿Qué correlaciones se pueden extraer?



En general, el acceso por banda ancha y la velocidad son proporcionales a la densidad demográfica.

Parte 2: Investigar las opciones de acceso por banda ancha para situaciones específicas

En la parte 2, investigará y detallará las opciones de banda ancha para las siguientes situaciones, y seleccionará la mejor tecnología de última milla para satisfacer las necesidades de los consumidores. Puede utilizar el sitio http://www.broadbandmap.gov como punto de partida para la búsqueda.

Situación 1: se va a mudar a Kansas City, Misuri, y está investigando las conexiones a Internet domésticas. Investigue y detalle dos conexiones a Internet que pueda seleccionar en esta área metropolitana.

ISP	Tipo de conexión	Costo por mes	Velocidad de descarga
Google Fiber	Fibra	USD 70	1 Gb/s
Time Warner	Cable	$79	50 Mb/s

Elija uno de la lista de ISP locales que seleccionó. Justifique la elección de ese ISP en particular.

Las respuestas varían. Por lo general, los motivos se basan en el precio mensual, las velocidades de Internet o los paquetes que se ofrecen.

Situación 2: se va a mudar a una zona en las afueras de Billings, Montana, y está investigando las conexiones a Internet domésticas. Estará fuera del alcance del servicio de las conexiones por cable o DSL. Investigue y detalle dos conexiones a Internet que pueda seleccionar en esta área.

ISP	Tipo de conexión	Costo por mes	Velocidad de descarga
Banda ancha rural	Conexión inalámbrica fija	$40	3 Mb/s
Hughes Net	Satélite	USD 60	5 Mb/s

Elija uno de la lista de ISP locales que seleccionó. Justifique la elección de ese ISP en particular.

_____

_____

_____

Las respuestas varían. Por lo general, los motivos se basan en el precio mensual, las velocidades de Internet o los paquetes que se ofrecen.

Situación 3: se va a mudar la ciudad de Nueva York, y su trabajo requiere que tenga acceso las 24 horas en cualquier momento y lugar. Investigue y detalle dos conexiones a Internet que pueda seleccionar en esta área.

ISP	Tipo de conexión	Costo por mes	Velocidad de descarga
Borrar	Conexión inalámbrica móvil	USD 50	6 Mb/s
Sprint	Conexión inalámbrica móvil	12 Mb por USD 80	6 Mb/s

Elija uno de la lista de ISP locales que seleccionó. Justifique la elección de ese ISP en particular.

_____

_____

_____

Las respuestas varían. Por lo general, los motivos se basan en el precio mensual, las velocidades de Internet o los paquetes que se ofrecen.

Situación 4: usted es propietario de una pequeña empresa con 10 empleados que trabajan a distancia en el área de Fargo, Dakota del Norte. Los trabajadores a distancia viven en un lugar fuera del alcance de las conexiones a Internet por cable. Investigue y detalle dos conexiones a Internet que pueda seleccionar en esta área.

ISP	Tipo de conexión	Costo por mes	Velocidad de descarga
Century Link	DSL	USD 29,99	12 Mb/s
I29	WiMAX	USD 39,99	3 Mb/s

Elija uno de la lista de ISP locales que seleccionó. Justifique la elección de ese ISP en particular.

_____

_____

_____

Las respuestas varían. Por lo general, los motivos se basan en el precio mensual, las velocidades de Internet o los paquetes que se ofrecen.

Situación 5: su empresa, ubicada en Washington, D. C., se expande a 25 empleados y debe actualizar el acceso por banda ancha para incluir la colocación de equipos y el alojamiento web. Investigue y detalle dos conexiones a Internet que pueda seleccionar en esta área.

ISP	Tipo de conexión	Costo por mes	Velocidad de descarga
Comcast	Cable	USD 369,95	100 Mb/s
Windstream	DSL	USD 129,99	6 Mb/s

Elija uno de la lista de ISP locales que seleccionó. Justifique la elección de ese ISP en particular.

_____

_____

_____

Las respuestas varían. Por lo general, los motivos se basan en el precio mensual, las velocidades de Internet o los paquetes que se ofrecen.

Reflexión<X1/>

¿Cómo cree que cambiará el acceso a Internet por banda ancha en el futuro?

_____

_____

_____

_____

Las respuestas varían. El acceso a Internet por banda ancha aumentará en tamaño geográfico y en velocidad con el desarrollo continuo de la tecnología y la infraestructura por cable e inalámbrica. Las opciones y las velocidades de acceso seguirán aumentando y tendrán una mayor disponibilidad en áreas que no pueden acceder al servicio o donde el servicio no es suficiente.

Práctica de laboratorio: Configuración de un router como cliente PPPoE para conectividad DSL (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

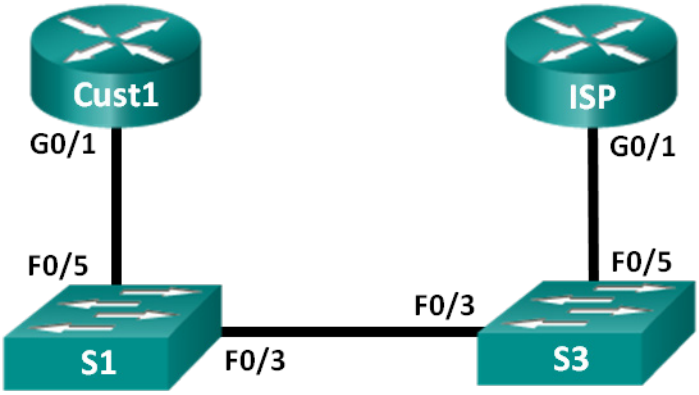


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Cust1	G0/1	Obtenida mediante PPP	Obtenida mediante PPP	Obtenida mediante PPP
ISP	G0/1	No aplicable	No aplicable	No aplicable

Objetivos

Parte 1: Armar la red

Parte 2: Configurar el router ISP

Parte 3: Configurar el router Cliente1

Información básica/situación

Por lo general, los ISP utilizan el protocolo punto a punto por Ethernet (PPPoE) en los enlaces DSL a sus clientes. PPP admite la asignación de información de direcciones IP a un dispositivo en el extremo remoto de un enlace PPP. Lo más importante es que PPP admite la autenticación CHAP. Los ISP pueden revisar los registros contables para ver si la factura de un cliente figura como paga antes de permitirles conectarse a Internet.

En esta práctica de laboratorio, configurará el lado de la conexión tanto del cliente como del ISP para configurar PPPoE. Generalmente, solo se configura el extremo del cliente.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: Crear la red

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

Paso 2: inicializar y volver a cargar los routers y los switches.

Paso 3: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un aviso de mensaje del día (MOTD) que advierta a los usuarios que se prohíbe el acceso no autorizado.

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

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

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Guarde su configuración.

Parte 2: Configurar el router ISP

En la parte 2, configurará el router ISP con los parámetros de PPPoE para la conexión desde el router Cust1.

Nota: muchos de los comandos de configuración de PPPoE del router ISP exceden el ámbito del curso; sin embargo, son necesarios para completar la práctica de laboratorio. Se pueden copiar y pegar en el router ISP, en la petición de entrada del modo de configuración global.

a. Cree el nombre de usuario **Cust1** para la base de datos local, con la contraseña **ciscopppoe**.

```
ISP(config)# username Cust1 password ciscopppoe
```


b. Cree el conjunto de direcciones que se asignará a los clientes.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

c. Cree la plantilla virtual y asóciela a la dirección IP de G0/1. Asocie la plantilla virtual al conjunto de direcciones. Configure CHAP para autenticar a los clientes.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

d. Asigne la plantilla al grupo de PPPoE.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

e. Asocie bba-group a la interfaz física G0/1.

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global
ISP(config-if)# no shutdown
```

Parte 3: Configurar el router Cust1

En la parte 3, configurará el router Cust1 con los parámetros de PPPoE.

a. Configure la interfaz G0/1 para la conectividad PPPoE.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

b. Asocie la interfaz G0/1 a una interfaz de marcador. Utilice el nombre de usuario **Cust1** y la contraseña **ciscopppoe** que se configuraron en la parte 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

c. Establezca una ruta estática predeterminada que apunte a la interfaz del marcador.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

d. Establezca la depuración en el router Cust1 para mostrar la negociación PPP y PPPoE.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```


e. Habilite la interfaz G0/1 en el router Cust1 y observe el resultado de debug a medida que se establece la sesión del marcador de PPPoE y que ocurre la autenticación CHAP.

```
Cust1(config)# interface g0/1
Cust1(config-if)# no shutdown
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Jul 30 19:29:03.839:  padi timer expired
*Jul 30 19:29:03.839:  Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887:  PPPOE: we've got our pado and the pado timer went off
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
```

f. Emita un comando **show ip interface brief** en el router Cust1 para mostrar la dirección IP que asignó el router ISP. A continuación, se muestra un ejemplo de resultado. ¿Mediante qué método se obtuvo la dirección IP? _____ PPP

```
Cust1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer1                    10.0.0.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
```



```
Virtual-Access2            unassigned      YES unset  up                    up
```

g. Emita un comando **show ip route** en el router Cust1. A continuación, se muestra un ejemplo de resultado.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

h. Emita un comando **show pppoe session** en el router Cust1. A continuación, se muestra un ejemplo de resultado.

```
Cust1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                 VT  VA         State
           SID  LocMAC                                  VA-st      Type
    N/A      1  30f7.0da3.0b01  Gi0/1                Di1 Vi2        UP
                30f7.0da3.0bc1                           UP
```

i. Haga ping a 10.0.0.254 desde el router Cust1. El ping debería realizarse correctamente. De lo contrario, resuelva los problemas hasta que haya conectividad.

```
Cust1# ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Reflexión<X1/>

¿Por qué los ISP que utilizan DSL usan principalmente PPPoE con sus clientes?

_____

El protocolo PPP admite la autenticación a través de un enlace Ethernet. Los ISP pueden autenticar a los clientes y emitir una dirección IP.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router Cust1

```
Cust1# show run
Building configuration...
Current configuration : 1433 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Cust1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
```



```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust1
 ppp chap password 0 ciscopppoe
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Dialer1
!
control-plane
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
```



```
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

ISP del router

```
ISP# show run
Building configuration...

Current configuration : 1485 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username Cust1 password 0 ciscopppoe
!
bba-group pppoe global
 virtual-template 1
```



```
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Virtual-Template1
 ip address 10.0.0.254 255.255.255.0
 mtu 1492
 peer default ip address pool PPPoEPOOL
 ppp authentication chap callin
!
ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
```



```
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Propuesta de trabajo a distancia (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.

Objetivo

Describir los requisitos comerciales del trabajo a distancia.

(Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños).

Situación

Se acaba de adjudicar un contrato grande de diseño de marketing a su pequeña o mediana empresa. Debido a que el espacio de la oficina es limitado, se recomendó contratar trabajadores a distancia para ayudar en el contrato.

Por lo tanto, se debe diseñar un programa muy general de trabajo a distancia para la empresa, ya que se anticipa que esta crezca. A medida que se adjudiquen más contratos, revise y expanda el programa para que se ajuste a las necesidades de la empresa.

Elabore una descripción básica de la propuesta de trabajo a distancia para que la empresa la tenga en cuenta como base para un programa de trabajo a distancia.

Recursos

- Acceso a la World Wide Web
- Software de procesamiento de texto

Paso 1: Investigar los programas de trabajo a distancia registrados con Internet.

a. Tome nota de la información que considere importante sobre los programas de trabajo a distancia establecidos y registre el URL que utilizó como fuente para esta investigación.

b. Como mínimo, incluya las siguientes áreas de la propuesta:

   1) Las tareas del trabajo a distancia que se deben tener en cuenta.

   2) Los métodos que se utilizarán para seleccionar a los empleados.

   3) El equipo que puede necesitar el trabajador a distancia.

   4) Los posibles métodos de comunicación.

   5) Las técnicas que se pueden utilizar para evaluar el programa de trabajo a distancia.

Paso 2: Diseñar un esquema de los requisitos básicos de un programa de trabajo a distancia.

Paso 3: Compartir la propuesta con otro estudiante, con la clase o con otro grupo.

Ejemplo sugerido para la actividad (todas las actividades varían):*

Planificación de la propuesta para los requisitos básicos del nuevo programa de trabajo a distancia

1. Tareas de trabajo a distancia sugeridas
   a. Programación informática
   b. Realización de negocios por teléfono
   c. Trabajo de diseño

   d. Investigación, redacción y edición
   e. Visitas de campo a los clientes
   f. Mantenimiento de información y bases de datos
   g. Administración de proyectos
2. Características propuestas para la selección de los empleados
   a. Emprendedor y responsable
   b. Bien organizado y disciplinado
   c. Orientado a los resultados
   d. Se comunica de forma eficaz
   e. Flexible
   f. Sensible a las necesidades de sus compañeros de trabajo y los clientes con respecto al programa
3. Equipos necesarios
   a. Computadora con acceso a Internet
   b. Cuenta de correo electrónico
   c. Software (VPN cliente)
   d. Soporte técnico para trabajadores a distancia
4. Métodos de comunicación
   a. Teleconferencias
   b. Correo electrónico
   c. Telefono
   d. Repositorios remotos de cliente a servidor
5. Métodos de evaluación del programa
   a. Encuestas
      1) Clientes
      2) Trabajadores a distancia
      3) Líderes de departamento
   b. Progreso del programa de trabajo a distancia
      1) Calidad del trabajo completado
      2) Fechas de entrega cumplidas

*las fuentes de información para el esquema incluyen lo siguiente: *Launching Telework- The Nuts and Bolts for Employers* y *The Managers & Supervisor's Quick & Easy Guide to Telework*

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Características del trabajador a distancia
- Planificación del programa de trabajo a distancia
- Software de cliente VPN
- Repositorios de cliente a servidor

Resumen sobre las VPN (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.

Objetivo

Explicar el uso de las VPN para aportar seguridad a la conectividad de sitio a sitio en una red de una pequeña o mediana empresa. Nota para el instructor: esta es una actividad individual basada en el estudiante que después se convierte en una actividad basada en grupos pequeños para fines de análisis y de diseño. Una vez que se complete la actividad basada en grupos pequeños, los estudiantes darán una presentación a toda la clase.

Situación

Una pequeña o mediana empresa crece y necesita que los clientes, los trabajadores a distancia y los empleados que se conectan por cable y de forma inalámbrica puedan acceder a la red principal desde cualquier ubicación. Como administrador de red de la empresa, usted decidió implementar las VPN para aportar seguridad, facilitar el acceso a la red y ahorrar costos.

Su trabajo es asegurar que todos los administradores de red comiencen el proceso de planificación de VPN con el mismo conjunto de conocimientos.

Se deben investigar cuatro áreas informativas básicas de VPN, y dichas áreas se deben presentar al equipo de administración de la red:

- Definición concisa de las VPN
- Algunos datos generales sobre las VPN
- IPsec como opción de seguridad de VPN
- Formas en las que las VPN usan el tunneling

Recursos

- Acceso a la World Wide Web
- Software de presentación o de procesamiento de texto

Instrucciones

Paso 1: Los estudiantes deben investigar por su cuenta los cuatro temas siguientes y tomar notas durante la investigación:

a. Tema 1: una definición concisa de las VPN

b. Tema 2: cinco datos generales sobre las VPN

c. Tema 3: IPsec definido como opción de seguridad al utilizar VPN

d. Tema 4: un gráfico que muestre la forma en que las VPN utilizan el tunneling

Paso 2: Una vez que los estudiantes hayan investigado los temas, se forman grupos de cuatro estudiantes para analizar las investigaciones individuales.

a. Cada grupo debe acordar lo siguiente:

1) Una definición concisa de las VPN

2) Cinco datos que describan las VPN

3) Una definición de IPsec como opción de seguridad para las VPN

4) Un gráfico que muestre una red VPN que utilice tunneling

Paso 3: Cada grupo debe diseñar una presentación de cuatro diapositivas (una diapositiva por tema) para presentar a la clase para su análisis.

Instructor: solución de ejemplo para la actividad (todas las presentaciones grupales varían)

Tema 1, definición de VPN: How VPNs Work

Una VPN es una red privada que utiliza una red pública (por lo general, Internet) para conectar sitios o usuarios remotos entre sí. La VPN utiliza conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa hasta el sitio remoto o el trabajador a distancia. Mediante una VPN, las empresas garantizan la seguridad: cualquiera que intercepte los datos cifrados no podrá leerlos.

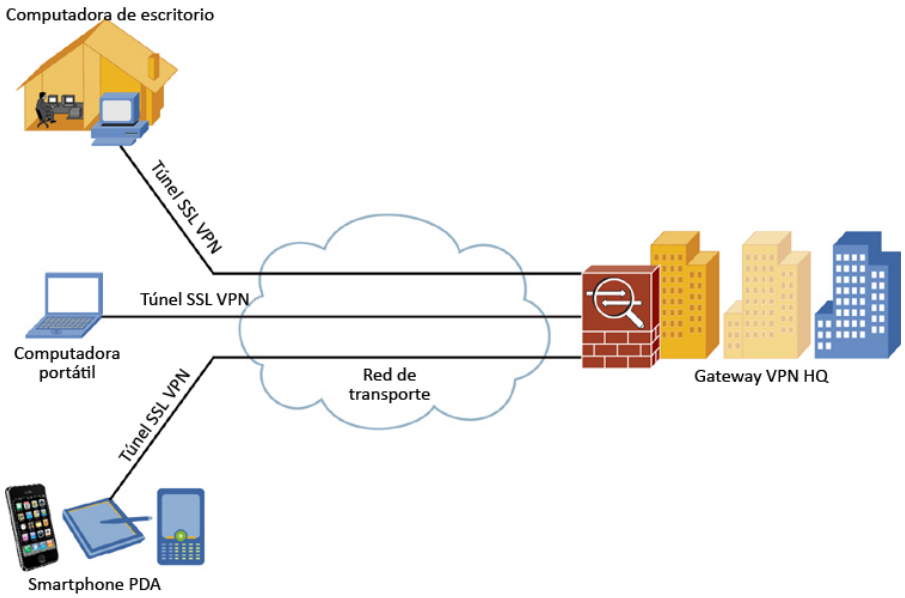
Tema 2, cinco datos generales sobre las VPN: VPN - Virtual Private Network

- Una VPN utiliza redes públicas para enviar y recibir datos de redes privadas mediante protocolos especiales.
- Las VPN utilizan un enfoque de cliente y servidor.
- Los clientes VPN autentican a los usuarios.
- En la mayoría de los sistemas de VPN, los datos están cifrados.
- Las VPN utilizan servidores para configurar el tunneling en la red.

Tema 3, IPsec como opción de seguridad: Encryption and Security Protocols in a VPN

IPsec es un protocolo ampliamente utilizado para proteger el tráfico en las redes IP, incluida Internet. IPsec puede cifrar datos entre diversos dispositivos, incluso de router a router, de firewall a router, de computadora de escritorio a router y de computadora de escritorio a servidor.

Tema 4, un gráfico que muestre una VPN que utilice tunneling: Deploying Cisco ASA AnyConnect Remote-Access SSL VPN Solutions



Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Definición de VPN
- Datos sobre las VPN
- Seguridad relacionada con las VPN (IPsec)
- Tunneling VPN

Práctica de laboratorio: Configuración de un túnel VPN GRE de punto a punto (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

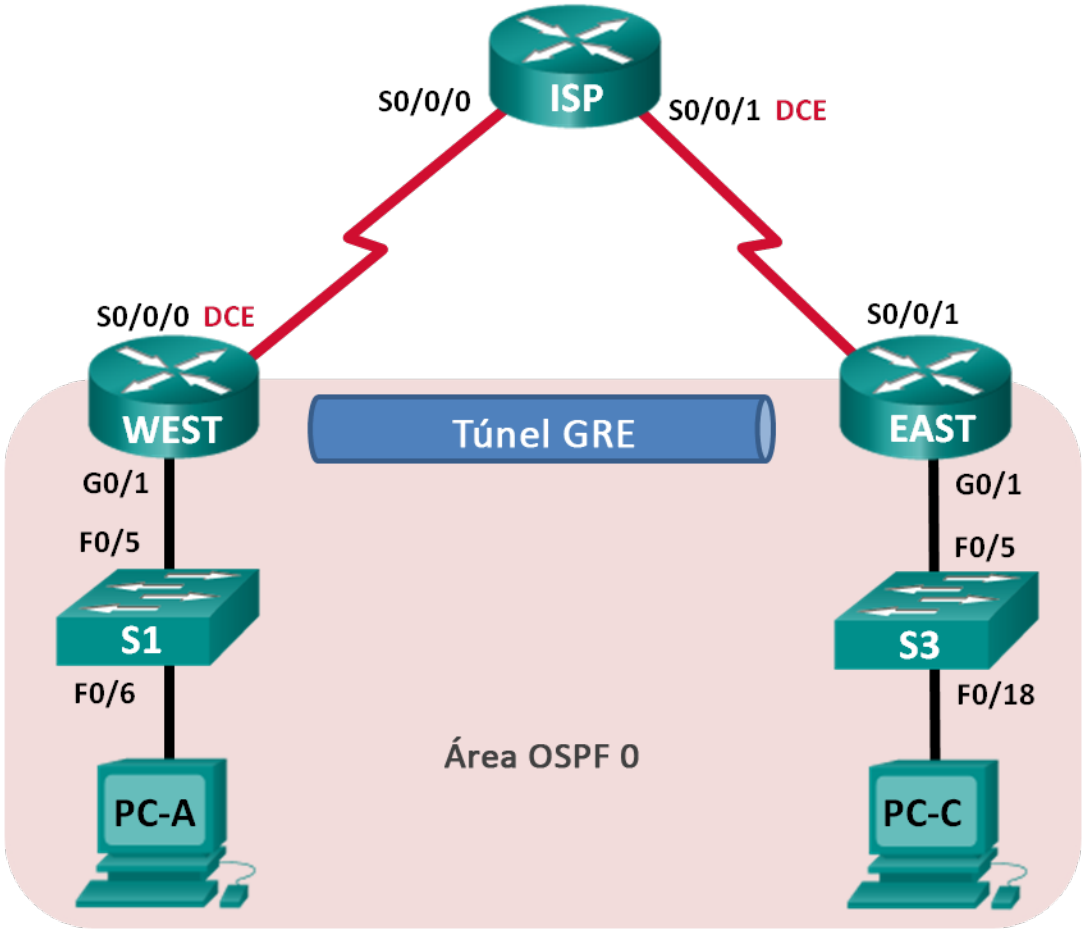


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
WEST	G0/1	172.16.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
EAST	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objetivos

Parte 1: configurar los parámetros básicos de los dispositivos

Parte 2: Configurar un túnel GRE

Parte 3: Habilitar el routing por el túnel GRE

Información básica/situación

La encapsulación de routing genérico (GRE) es un protocolo de tunneling que puede encapsular diversos protocolos de capa de red entre dos ubicaciones a través de una red pública, como Internet.

GRE se puede utilizar con lo siguiente:

- La conexión de redes IPv6 a través de redes IPv4
- Paquetes de multidifusión, como OSPF, EIGRP y aplicaciones de transmisión

En esta práctica de laboratorio, configurará un túnel VPN GRE de punto a punto sin cifrar y verificará que el tráfico de la red utilice el túnel. También configurará el protocolo de routing OSPF dentro del túnel VPN GRE. El túnel GRE se encuentra entre los routers EAST y WEST en el área OSPF 0. El ISP no tiene conocimiento del túnel GRE. La comunicación entre los routers EAST, WEST e ISP se logra mediante rutas estáticas predeterminadas.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos del router, como las direcciones IP de las interfaces, el routing, el acceso a los dispositivos y las contraseñas.

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

Paso 2: inicializar y volver a cargar los routers y los switches.

Paso 3: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un aviso de mensaje del día (MOTD) que advierta a los usuarios que se prohíbe el acceso no autorizado.

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

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

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Aplique las direcciones IP a las interfaces Serial y Gigabit Ethernet según la tabla de direccionamiento y active las interfaces físicas. Todavía NO configure las interfaces Tunnel0.

i. Establezca la frecuencia de reloj en **128000** para las interfaces seriales DCE.

Paso 4: Configurar las rutas predeterminadas al router ISP.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Paso 5: Configurar las PC.

Asigne direcciones IP y gateways predeterminados a las computadoras según la tabla de direccionamiento.

Paso 6: Verificar la conectividad.

En este momento, las computadoras no pueden hacerse ping entre sí. Cada computadora debe poder hacer ping a su gateway predeterminado. Los routers pueden hacer ping a las interfaces seriales de los demás routers en la topología. De lo contrario, lleve a cabo la resolución de problemas hasta que pueda verificar la conectividad.

Paso 7: Guardar la configuración en ejecución.

Parte 2: Configurar un túnel GRE

En la parte 2, configurará un túnel GRE entre los routers EAST y WEST.

Paso 1: Configurar la interfaz de túnel GRE.

a. Configure la interfaz de túnel en el router WEST. Utilice S0/0/0 en el router WEST como interfaz de origen del túnel y 10.2.2.1 como destino del túnel en el router EAST.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

b. Configure la interfaz de túnel en el router EAST. Utilice S0/0/1 en el router EAST como interfaz de origen del túnel y 10.1.1.1 como destino del túnel en el router WEST.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source 10.2.2.1
EAST(config-if)# tunnel destination 10.1.1.1
```

Nota: para el comando **tunnel source**, tanto el nombre de la interfaz como la dirección IP se pueden utilizar como origen.

Paso 2: Verificar que el túnel GRE funcione.

a. Verifique el estado de la interfaz de túnel en los routers EAST y WEST.

```
WEST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Tunnel0                    172.16.12.1     YES manual up                    up

EAST# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
```

b. Emita el comando **show interfaces tunnel 0** para verificar el protocolo de tunneling, el origen y el destino de túnel que se utilizan en este túnel.

¿Qué protocolo de tunneling se utiliza? ¿Cuáles son las direcciones IP de origen y destino de túnel asociadas al túnel GRE en cada router?

_____

El protocolo de tunneling que se utiliza es GRE. Para el router WEST, el origen del túnel es 10.1.1.1 (Serial0/0/0) y el destino es 10.2.2.1. Para el router EAST, el origen del túnel es 10.2.2.1 y el destino es 10.1.1.1.

```
WEST# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.12.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Serial0/0/0
          Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on
interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:12, output 00:00:12, output hang never
  Last clearing of "show interface" counters 00:01:29
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 620 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 620 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

EAST# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.12.2/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
```

```
  Keepalive not set
  Tunnel source 10.2.2.1, destination 10.1.1.1
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Serial0/0/1
          Set of tunnels with source Serial0/0/1, 1 member (includes iterators), on
interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:01:28, output 00:01:28, output hang never
  Last clearing of "show interface" counters 00:02:50
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 620 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 620 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

c. Haga ping a través del túnel desde el router WEST hasta el router EAST con la dirección IP de la interfaz de túnel.

```
WEST# ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

d. Utilice el comando **traceroute** en el router WEST para determinar la ruta a la interfaz de túnel en el router EAST. ¿Cuál es la ruta al router EAST?

_____ 172.16.12.1 > 172.16.12.2

```
WEST# traceroute 172.16.12.2
Type escape sequence to abort.
Tracing the route to 172.16.12.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.12.2 20 msec 20 msec *
```

e. Haga ping a la ruta a través del túnel y rastréela desde el router EAST hasta el router WEST con la dirección IP de la interfaz de túnel.

¿Cuál es la ruta al router WEST desde el router EAST? _____
172.16.12.2 > 172.16.12.1

¿A qué interfaces se asocian estas direcciones IP? ¿Por qué?

_____

_____

A las interfaces de túnel 0 tanto en el router WEST como en el router EAST. El tráfico utiliza el túnel.

f. Los comandos **ping** y **traceroute** deberían realizarse correctamente. De lo contrario, lleve a cabo la resolución de problemas antes de continuar con la parte siguiente.

Parte 3: Habilitar el routing por el túnel GRE

En la parte 3, configurará el routing OSPF de modo que las LAN en los routers EAST y WEST se puedan comunicar mediante el túnel GRE.

Después de configurar el túnel GRE, se puede implementar el protocolo de routing. Para los túneles GRE, una instrucción network incluye la red IP del túnel, en lugar de la red asociada a la interfaz serial, tal como sucedería con otras interfaces, como Serial y Ethernet. Recuerde que el router ISP no participa en este proceso de routing.

Paso 1: Configurar el routing OSPF para el área 0 a través del túnel.

a. Configure la ID de proceso OSPF 1 con el área 0 en el router WEST para las redes 172.16.1.0/24 y 172.16.12.0/24.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Configure la ID de proceso OSPF 1 con el área 0 en el router EAST para las redes 172.16.2.0/24 y 172.16.12.0/24.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Paso 2: Verificar el enrutamiento OSPF.

a. Desde el router WEST, emita el comando **show ip route** para verificar la ruta a la LAN 172.16.2.0/24 en el router EAST.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
```



```
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

¿Cuál es la interfaz de salida y la dirección IP para llegar a la red 172.16.2.0/24?

Para llegar a 172.16.2.0/24, se utiliza la interfaz de túnel 0 con la dirección IP 172.16.12.2.

b. Desde el router EAST, emita el comando para verificar la ruta a la LAN 172.16.1.0/24 en el router WEST.

¿Cuál es la interfaz de salida y la dirección IP para llegar a la red 172.16.1.0/24?

Para llegar a 172.16.1.0/24, se utiliza la interfaz de túnel 0 con la dirección IP 172.16.12.1.

```
EAST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.2.2.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O        172.16.1.0/24 [110/1001] via 172.16.12.1, 00:02:44, Tunnel0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/1
L        172.16.2.1/32 is directly connected, GigabitEthernet0/1
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.2/32 is directly connected, Tunnel0
```

Paso 3: Verificar la conectividad de extremo a extremo.

a. Haga ping de la PC-A a la PC-C. Esto debe tener éxito. De lo contrario, lleve a cabo la resolución de problemas hasta que haya conectividad de extremo a extremo.

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

b. Utilice traceroute desde la PC-A hasta la PC-C. ¿Cuál es la ruta desde la PC-A hasta la PC-C?

172.16.1.1 > 172.16.12.2 (interfaz de túnel en el router EAST) > 172.16.2.3

Reflexión

1. ¿Qué otra configuración se necesita para crear un túnel GRE protegido?

   Se puede configurar IPsec a fin de cifrar los datos para un túnel GRE seguro.

2. Si agregara más redes LAN al router WEST o EAST, ¿qué debería hacer para que la red utilice el túnel GRE para el tráfico?

   Se deberían agregar las nuevas redes a los mismos protocolos de routing que la interfaz del túnel.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router WEST

```
WEST# show run
Building configuration...

Current configuration : 1798 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```



```
!
hostname WEST
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!

!
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 ip address 172.16.12.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 10.2.2.1
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
```



```
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 05080F1C2243
 login
 transport input all
```



```
!
scheduler allocate 20000 1000
!
end
```

ISP del router

```
ISP# show run
Building configuration...

Current configuration : 1406 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
redundancy
!
!
!
!
```



```
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
```



```
line con 0
 password 7 02050D480809
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 045802150C2E
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router EAST

```
EAST# show run
Building configuration...

Current configuration : 1802 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname EAST
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
```



```
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 ip address 172.16.12.2 255.255.255.252
 tunnel source 10.2.2.1
 tunnel destination 10.1.1.1
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
```



```
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
router ospf 1
 network 172.16.2.0 0.0.0.255 area 0
 network 172.16.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
!
!
!
control-plane
!
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 030752180500
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Diseño de planificación VPN (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.

Objetivo

Explicar el uso de las VPN para aportar seguridad a la conectividad de sitio a sitio en una red de una pequeña o mediana empresa.

Nota para el instructor: conviene realizar esta actividad en grupos pequeños. Después se puede compartir con otro grupo, la clase o el instructor (como proyecto de grupo).

Situación

Su pequeña o mediana empresa recibió algunos contratos nuevos recientemente. Esto aumentó la necesidad de contratar trabajadores a distancia y servicios externos para la carga de trabajo. Los proveedores y clientes de los nuevos contratos también necesitan acceso a la red a medida que progresan los proyectos.

Como administrador de red de la empresa, usted reconoce que se deben incorporar VPN como parte de la estrategia de red para admitir un acceso seguro para los trabajadores a distancia, los empleados y los proveedores o clientes.

A fin de preparar la implementación de las VPN en la red, elabora una lista de comprobación de planificación para presentarla en la siguiente reunión del departamento.

Recursos

- Acceso a la World Wide Web
- Software Packet Tracer
- Software de procesamiento de texto

Paso 1: Visitar la página VPN Discovery Tool, o cualquier otro sitio de Internet con ejemplos de implementación o de listas de comprobación de planificación de VPN.

Paso 2: Utilice Packet Tracer para dibujar la topología actual para la red; no es necesario configurar los dispositivos. Incluya lo siguiente:

- Dos sucursales: la nube de Internet y una ubicación de oficina central
- Dispositivos de red actuales: servidores, switches, routers y routers principales, dispositivos ISR de banda ancha y estaciones de trabajo de usuarios locales

Paso 3: En la topología de Packet Tracer, indique lo siguiente:

a. ¿Dónde implementaría las VPN?

b. ¿Qué tipos de VPN se necesitarían?

   1) Sitio a sitio

   2) Acceso remoto

Paso 4: Con un programa de software de procesamiento de texto, cree una pequeña lista de comprobación de planificación de VPN sobre la base de la investigación realizada en el paso 1.

Paso 5: Comparta su trabajo con la clase, con otro grupo o con el instructor.

Solución de ejemplo sugerida para la actividad:

Objetivos del proyecto de VPN: (escriba "1" junto al objetivo más importante, "2" junto al que le sigue en importancia, etc.)

_____Reducir los costos de las telecomunicaciones existentes.

_____Proporcionar un sistema de comunicaciones de VPN seguras para los trabajadores a distancia, los usuarios móviles y los clientes.

_____Utilizar los equipos existentes para no tener que rediseñar demasiado la red (consideración de costos).

_____Aprovechar las nuevas tecnologías (software y hardware).

Plazo para cumplir los objetivos:

☐ 3 meses ☐ 6 meses ☐ 9 meses ☐ 1 año

Enfoque por etapas: ☐ Sí ☐ No

Factores de VPN que se deben admitir: (1=el más importante, 2=muy importante, 3=poco importante, 4=No es importante)

Factor	Hardware	Software
Escalabilidad		
Costo		
Interoperabilidad		
Seguridad		
Calidad de servicio		
Mantenimiento de la red		
Soporte de aplicaciones		

Usuarios y aplicaciones de VPN que se deben admitir:

Usuarios internos de la red	Clientes y proveedores	Trabajadores a distancia
Cantidad de usuarios: _____	Cantidad aproximada de usuarios: _____	Cantidad de usuarios: _____

Tipo de conexión VPN:

_____Sitio a sitio _____Acceso remoto (Internet)

Recursos de red disponibles para los usuarios de la VPN:

_____Aplicaciones/archivos de software _____Servidores (FTP, web, correo electrónico, etc.)

Protocolos de VPN que se utilizan:

_____ SSL _____IPsec _____Ambos

Protocolos de red que se utilizan:

_____EIGRP _____OSPF

Tecnologías actualmente en uso:

_____Traducción de direcciones de red (NAT) _____Filtrado de paquetes (ACL) _____DHCP _____DNS

Autenticación que se utiliza:

_____Certificados digitales _____Claves secretas compartidas _____SSL _____Contraseñas _____IPsec

Cifrado que se utiliza:

_____DES _____3DES _____AES

Método de mensaje HASH que se utiliza:

_____MD-5 _____SHA-1

Método de intercambio de claves de cifrado que se utiliza:

_____Intercambio de claves de Internet (IKE) _____Intercambio manual

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Planificación de la red VPN
- Tipos de topología de VPN
- Métodos de seguridad
  - Autenticación
  - Cifrado
  - Tipo de mensaje HASH
  - Tipo de intercambio de claves

Desarrollo de mantenimiento 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.

Objetivo

Describir los diferentes niveles de mensajes de registro del router.

Nota para el instructor: conviene realizar esta actividad en grupos de dos a tres estudiantes.

Situación

Actualmente, no hay políticas o procedimientos formales para registrar los problemas que se experimentan en la red de su empresa. Además, cuando ocurren problemas de red, debe probar varios métodos para encontrar las causas, y este enfoque de resolución de problemas lleva tiempo.

Usted sabe que debe de existir una mejor manera de resolver estos problemas. Decide crear un plan de mantenimiento de red para conservar los registros de reparación e identificar las causas de los errores en la red.

Recursos

- Software de procesamiento de texto

Instrucciones

Paso 1: Intercambiar ideas sobre los distintos tipos de registros de mantenimiento de red que desea guardar.

Paso 2: Ordenar los tipos de registros en categorías principales. Las categorías sugeridas incluyen lo siguiente:

- Equipos (routers y switches)
- Tráfico
- Seguridad

Paso 3: Crear una descripción para orientar el proceso de planificación del mantenimiento de red para la empresa.

Instructor: solución de ejemplo para la actividad

Opciones para los registros del mantenimiento de red

I. Equipos (routers y switches)
   a. Confiabilidad
      i. Motivos para el tiempo de inactividad
      ii. Porcentajes del tiempo de inactividad
   b. Actualizaciones y parches del IOS
   c. Mensajes de error
      i. Fechas/horas
      ii. Tipo de error
      iii. Descripción del error
      iv. Método para resolver el error

II. Tráfico
    a. Uso del tráfico por cable e inalámbrico
        i. Uso del tráfico de la red por aplicación
        ii. Congestión del tráfico de la red
    b. Sistema y servidores
        i. Uso de aplicaciones
            1. Correo electrónico
            2. Software basado en Web
        ii. Errores con aplicaciones
        iii. Métodos utilizados para resolver errores

III. Seguridad
    a. Actualizaciones
    b. Métodos de autenticación
    c. Métodos de cifrado
    d. Mensajes de error
    e. Las ACL
    f. Seguridad por cable e inalámbrica
    g. Métodos para resolver errores

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Mantenimiento de la red
- Registro de red
- Análisis del mantenimiento de la red

Práctica de laboratorio: Configuración de syslog y NTP (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

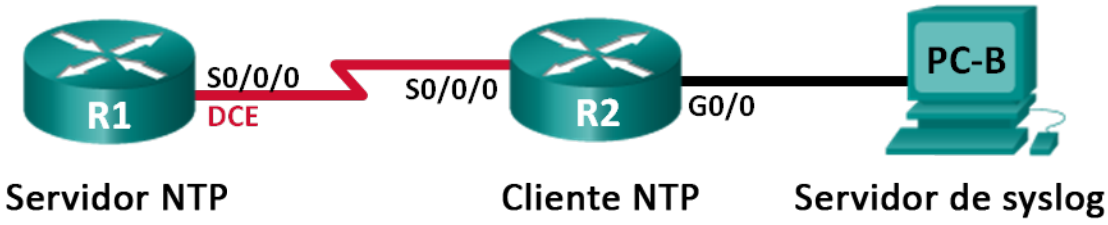


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0	172.16.2.1	255.255.255.0	N/A
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objetivos

Parte 1: configurar los parámetros básicos de los dispositivos

Parte 2: configurar NTP

Parte 3: Configurar syslog

Información básica/situación

Los mensajes de syslog que generan los dispositivos de red se pueden recopilar y archivar en un servidor de syslog. La información se puede utilizar para fines de control, depuración y resolución de problemas. El administrador puede controlar dónde se almacenan y se muestran los mensajes. Los mensajes de syslog se pueden marcar con la hora para analizar la secuencia de eventos de red; por lo tanto, es importante sincronizar el reloj a través de los dispositivos de red con un servidor de protocolo NTP.

En esta práctica de laboratorio, configurará el R1 como servidor NTP y el R2 como cliente syslog y NTP. La aplicación de servidor de syslog, como Tftp32d u otro programa similar, se ejecutará en la PC-B. Además, usted controlará el nivel de gravedad de los mensajes de registro que se recopilan y se archivan en el servidor de syslog.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 computadora (Windows 7, Vista o XP, con un programa de emulación de terminal, como Tera Term, y software de syslog, como tftpd32)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de las interfaces, el routing, el acceso a los dispositivos y las contraseñas.

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

Paso 2: Inicializar y volver a cargar los routers según sea necesario.

Paso 3: Configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un aviso de mensaje del día (MOTD) que advierta a los usuarios que se prohíbe el acceso no autorizado.

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

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

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Aplique las direcciones IP a las interfaces Serial y Gigabit Ethernet según la tabla de direccionamiento y active las interfaces físicas.

i. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

Paso 4: Configurar el routing.

Habilite OSPF de área única en los routers con la ID de proceso 1. Agregue todas las redes al proceso OSPF para el área 0.

Paso 5: Configurar la PC-B.

Configure la dirección IP y el gateway predeterminado para la PC-B según la tabla de direccionamiento.

Paso 6: Verificar la conectividad de extremo a extremo.

Verifique que cada dispositivo pueda hacer ping a todos los demás dispositivos en la red correctamente. De lo contrario, lleve a cabo la resolución de problemas hasta que haya conectividad de extremo a extremo.

Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

Parte 2: Configurar NTP

En la parte 2, configurará el R1 como servidor NTP y el R2 como cliente NTP del R1. La sincronización del tiempo es importante para las funciones de syslog y de depuración. Si no se sincroniza el tiempo, es difícil determinar qué evento de red causó el mensaje.

Paso 1: Mostrar la hora actual.

Emita el comando **show clock** para mostrar la hora actual en el R1.

```
R1# show clock
*12:30:06.147 UTC Tue May 14 2013
```

En la siguiente tabla, registre la información relacionada con la hora actual que se muestra.

Fecha	La respuesta varía. En este ejemplo: 14 de mayo de 2013
Tiempo	La respuesta varía. En este ejemplo: 12:30:06.147
Huso horario	La respuesta varía. En este ejemplo: UTC

Paso 2: Establecer la hora.

Utilice el comando **clock set** para configurar la hora en el R1. El siguiente es un ejemplo de configuración de la fecha y la hora.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by
console.
```

Nota: la hora también se puede configurar mediante el comando **clock timezone** del modo de configuración global. Para obtener más información sobre este comando, investigue el comando **clock timezone** en www.cisco.com a fin de determinar la zona de su región.

Paso 3: Configurar el maestro NTP.

Configure el R1 como maestro NTP mediante el comando **ntp master** *número-capa* del modo de configuración global. El número de capa indica a cuántos saltos NTP se encuentra un origen de hora autoritativo. En esta práctica de laboratorio, el nivel de capa de este servidor NTP es el número 5.

```
R1(config)# ntp master 5
```

Paso 4: Configurar el cliente NTP

a. Emita el comando **show clock** en el R2. En la siguiente tabla, registre la hora actual que se muestra en el R2.

Fecha	La respuesta varía.
Tiempo	La respuesta varía.
Huso horario	La respuesta varía.

b. Configure el R2 como cliente NTP. Utilice el comando **ntp server** para señalar a la dirección IP o al nombre de host del servidor NTP. El comando **ntp update-calendar** actualiza el calendario periódicamente con la hora de NTP.


```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```

Paso 5: Verificar la configuración NTP.

a. Utilice el comando **show ntp associations** para verificar que el R2 tenga una asociación NTP con el R1.

```
R2# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.1.1.1        127.127.1.1      5     11     64   177 11.312  -0.018  4.298
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

b. Emita el comando **show clock** en el R1 y el R2 para comparar la marca de hora.

Nota: es posible que la sincronización de la marca de hora del R2 con la del R1 demore unos minutos.

```
R1# show clock
09:43:32.799 UTC Fri Jul 5 2013
R2# show clock
09:43:37.122 UTC Fri Jul 5 2013
```

Parte 3: Configurar syslog

Los mensajes de syslog de los dispositivos de red se pueden recopilar y archivar en un servidor de syslog. En esta práctica de laboratorio, se utilizará Tftpd32 como software de servidor de syslog. El administrador de red puede controlar los tipos de mensajes que se pueden enviar al servidor de syslog.

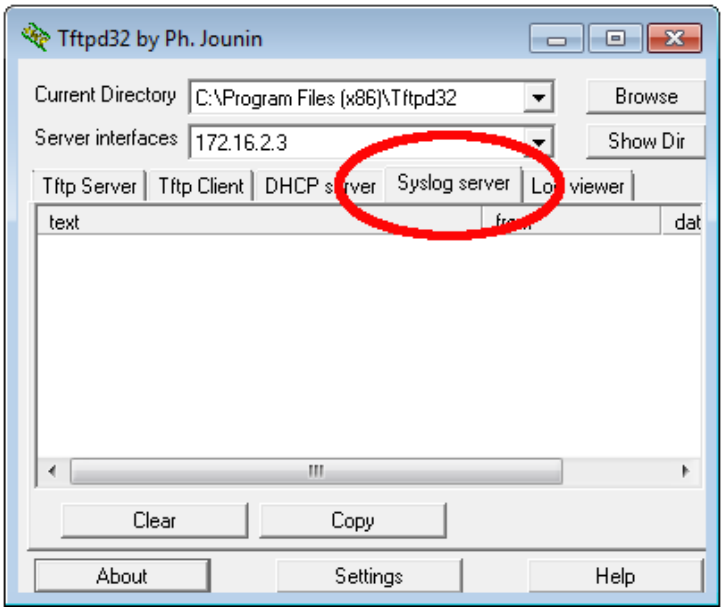
Paso 1: (Optativo) Instalar el servidor de syslog.

Si todavía no se instaló un servidor de syslog en la computadora, descargue e instale la versión más reciente de un servidor de syslog, como Tftpd32, en la computadora. La versión más reciente de Tftpd32 se puede encontrar en el siguiente enlace:

http://tftpd32.jounin.net/

Paso 2: Iniciar el servidor de syslog en la PC-B.

Después de iniciar la aplicación Tftpd32, haga clic en la ficha **Syslog server** (Servidor de syslog).



Paso 3: Verificar que el servicio de marca horaria esté habilitado en el R2.

Utilice el comando **show run** para verificar que el servicio de marca horaria esté habilitado para el registro en el R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

Si el servicio de marca horaria no está habilitado, utilice el siguiente comando para habilitarlo.

```
R2(config)# service timestamps log datetime msec
```

Paso 4: Configurar el R2 para registrar mensajes en el servidor de syslog.

Configure el R2 para enviar mensajes de syslog al servidor de syslog, la PC-B. La dirección IP del servidor de syslog PC-B es 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Paso 5: Mostrar la configuración de registro predeterminada.

Utilice el comando **show logging** para mostrar la configuración de registro predeterminada.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)


No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 47 messages logged, xml disabled,
                     filtering disabled
```



```
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 47 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 49 message lines logged
        Logging to 172.16.2.3  (udp port 514, audit disabled,
              link up),
              6 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
```

¿Cuál es la dirección IP del servidor de syslog? _____ 172.16.2.3

¿Qué protocolo y qué puerto usa syslog? _____ Puerto UDP 514

¿En qué nivel se encuentra habilitado el registro de traps? _____ Informativo

Paso 6: Configurar y observar el efecto de registrar los niveles de gravedad en el R2.

a. Utilice el comando **logging trap ?** para determinar la disponibilidad de los distintos niveles de traps. Al configurar un nivel, los mensajes que se envían al servidor de syslog son del nivel de trap configurado y de cualquier nivel más bajo.

```
R2(config)# logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

Si se emitió el comando **logging trap warnings**, ¿cuáles son los niveles de seguridad de mensajes que se registran?

_____

Advertencias (nivel 4) errores (nivel 3), crítico (nivel 2), alertas (nivel 1), y emergencia (nivel 0)

b. Cambie el nivel de gravedad de registro a 4.

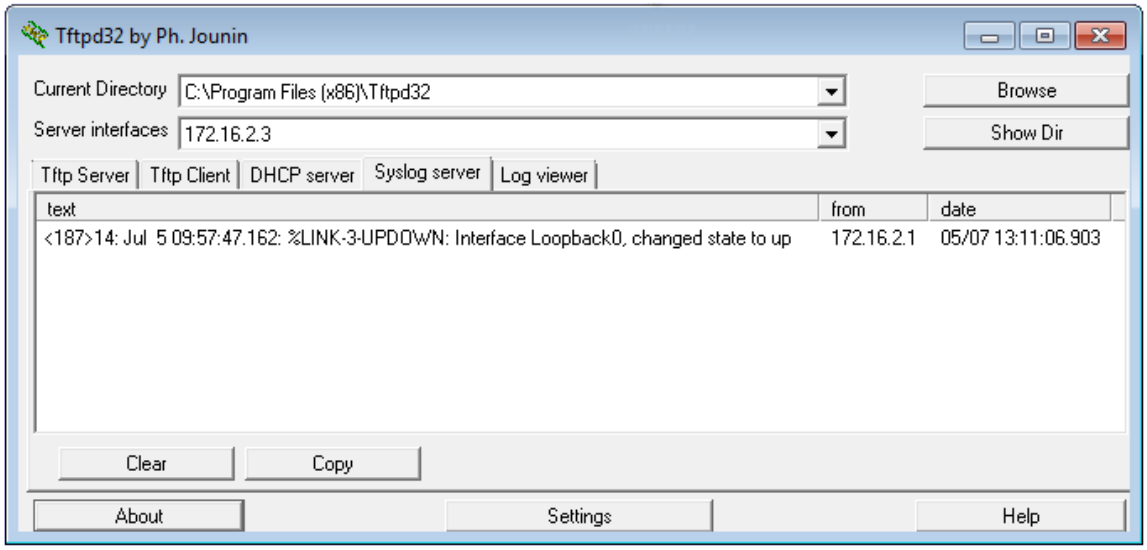
```
R2(config)# logging trap warnings
```

o


```
R2(config)# logging trap 4
```

c. Cree la interfaz Loopback0 en el R2 y observe los mensajes de registro en la ventana de la terminal y en la ventana del servidor de syslog en la PC-B.

```
R2(config)# interface lo 0
R2(config-if)#
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
```



d. Elimine la interfaz Loopback0 del R2 y observe los mensajes de registro.

```
R2(config-if)# no interface lo 0
R2(config)#
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
```

En el nivel de gravedad 4, ¿hay algún mensaje de registro en el servidor de syslog? Si apareció algún mensaje de registro, explique qué apareció y por qué.

_____

_____

_____

_____

Hubo un mensaje de registro de advertencia resumido que indicaba un cambio en el estado de la interfaz. La incorporación de la interfaz no fue suficiente para activar y enviar mensajes informativos más detallados al servidor de syslog en el nivel 4.

e. Cambie el nivel de gravedad de registro a 6.

```
R2(config)# logging trap informational
```

o

```
R2(config)# logging trap 6
```

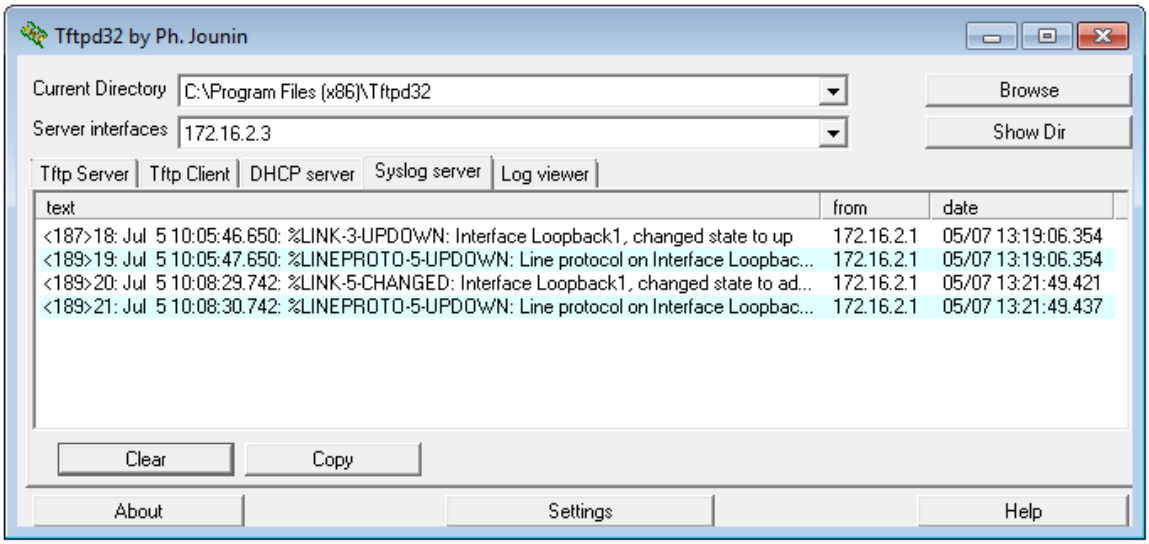

f. Borre las entradas de syslog de la PC-B. Haga clic en **Clear** (Borrar) en el cuadro de diálogo de Tftpd32.

g. Cree la interfaz Loopback 1 en el R2.

```
R2(config)# interface lo 1
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

h. Elimine la interfaz Loopback 1 del R2.

```
R2(config-if)# no interface lo 1
R2(config-if)#
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to
administratively down
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to down
```



i. Observe el resultado del servidor de syslog. Compare este resultado con los resultados del nivel de trap 4. ¿Cuál es su observación?

_____

_____

_____

Se atraparon más mensajes de registro cuando se estableció la gravedad en 6 (informativa) que cuando se estableció en 4 (advertencias).

Reflexión

¿Cuál es el problema de configurar un nivel de gravedad demasiado alto (el número más bajo) o demasiado bajo (el número de nivel más alto) para syslog?

_____

_____

_____

Cuando se establece un nivel de gravedad demasiado alto (el número más bajo), pueden faltar mensajes importantes pero no fundamentales en el registro generado. Sin embargo, una configuración demasiado baja (el número de nivel más alto), puede generar demasiadas entradas y llenar los registros con información innecesaria.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router R1

```
R1#show run
Building configuration...

Current configuration : 1572 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
```



```
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
```



```
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^CUnauthorized access is prohibited.^C
!
line con 0
 password 7 110A1016141D
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 01100F175804
 login
 transport input all
!
scheduler allocate 20000 1000
ntp master 5
```



```
!
end
```

R2 del router

```
Building configuration...

Current configuration : 1742 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
```



```
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
logging host 172.16.2.3
!
!
!
control-plane
!
!
banner motd ^CUnauthorized access is prohibited.^C
!
line con 0
 password 7 121A0C041104
 logging synchronous
```



```
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 01100F175804
 login
 transport input all
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.1.1.1
!
end
```


Práctica de laboratorio: Investigación del software de supervisión de 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.

Objetivos

Parte 1: Evaluar su comprensión del monitoreo de red

Parte 2: Investigar las herramientas de monitoreo de red

Parte 3: Seleccionar una herramienta de monitoreo de red

Información básica/situación

El monitoreo de red es necesario para las redes de cualquier tamaño. Monitorear proactivamente la infraestructura de red puede ayudar a los administradores de red con sus tareas diarias. La amplia variedad de herramientas de red disponibles varía en costo, según las características, la cantidad de ubicaciones de red y de nodos admitidos.

En esta práctica de laboratorio, investigará sobre el software de supervisión de red disponible. Recopilará información acerca de productos de software y las características de esos productos. Investigará un producto con mayor detalle e indicará algunas de las características clave disponibles.

Recursos necesarios

- Computadora con acceso a Internet

Parte 1: Evaluar su comprensión del monitoreo de red

Nota para el instructor: en la parte 1, el instructor puede desear hacer un análisis con los estudiantes acerca de su comprensión del monitoreo de red y sobre cómo lo utilizan los administradores de red. Esta práctica de laboratorio puede asignarse como tarea para el hogar.

Describa su comprensión del monitoreo de red. Proporcione un ejemplo de cómo se puede utilizar en una red de producción.

_____

_____

_____

_____

_____

_____

El monitoreo de red se realiza mediante software, generalmente una herramienta o un conjunto de herramientas que ayudan a los administradores de red con la resolución de problemas, el monitoreo y la modificación de dispositivos dentro de la red. Los informes, los gráficos de rendimiento, la administración del inventario de hardware y de software, la asignación de topologías de la red, la generación de alertas a través del correo electrónico o el envío de textos a un administrador de red pueden formar parte de la herramienta de software. Un administrador de red puede decidir configurar una alerta por correo electrónico cuando la pérdida de paquetes en un router supera cierto límite.

Parte 2: Investigar herramientas de monitoreo de red

Paso 1: Investigar y buscar tres herramientas de monitoreo de red.

Indique las tres herramientas que encontró.

_____

_____

_____

Las respuestas varían. Solar Winds, PRTG y Nagios son algunos ejemplos.

Paso 2: Completar el formulario siguiente para las herramientas de monitoreo de red seleccionadas.

Fabricante	Nombre del producto	Características
Solar Winds: www.solarwinds.com	Network Performance Monitor	Monitoreo de rendimiento, detección automática de dispositivos de red, alertas de red, compatibilidad con dispositivos de varios proveedores
Paessler: www.paessler.com	PRTG	Registro, monitoreo de ancho de banda, detección de paquetes, compatibilidad con NetFlow
Nagios: www.nagios.org	Nagios XI	Monitoreo de eventos en tiempo real, planificación de rendimiento y capacidad, asistentes de configuración, preferencias de notificación específicas de los usuarios

Parte 3: Seleccionar una herramienta de monitoreo de red

Paso 1: Seleccionar una o más herramientas de monitoreo de la investigación realizada.

A partir de la investigación realizada, identifique una o más herramientas que elegiría para monitorear su red. Indique las herramientas y explique los motivos para elegirlas, incluidas las características específicas que considere importantes.

_____

_____

_____

_____

_____

_____

Las respuestas varían considerablemente. Muchas de las herramientas comerciales ofrecen pruebas gratuitas de 30 días. PRTG es gratuito para hasta 10 sensores de red. La facilidad de uso del producto puede ser un factor importante al seleccionar herramientas. La compatibilidad con varios proveedores también es importante.

Paso 2: Investigar la herramienta de monitoreo de red PRTG.

Navegue hasta www.paessler.com/prtg.

En el espacio proporcionado a continuación, proporcione ejemplos de algunas de las características que encontró para PRTG.

Las respuestas varían. PRTG proporciona monitoreo de red integral con compatibilidad para más de 170 tipos de sensores. También tiene sistemas de alertas flexibles, por ejemplo: correo electrónico, syslog, localizador, archivos de sonido de alarma y alertas de varias condiciones. El monitoreo remoto de red, los mapas de red y las interfaces web personalizables también se encuentran disponibles.

Reflexión

Sobre la base de la investigación realizada, ¿a qué conclusiones llegó sobre el software de supervisión de red?

Las respuestas varían. Dada la gran cantidad de productos disponibles, elegir el producto correcto es crucial. Las versiones de prueba de 30 días pueden ser una buena opción, ya que permiten que el administrador de red trabaje con un producto antes de adquirirlo. Independientemente del producto que se elija, habrá una curva de aprendizaje para utilizarlo.

Práctica de laboratorio: Configuración de SNMP (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

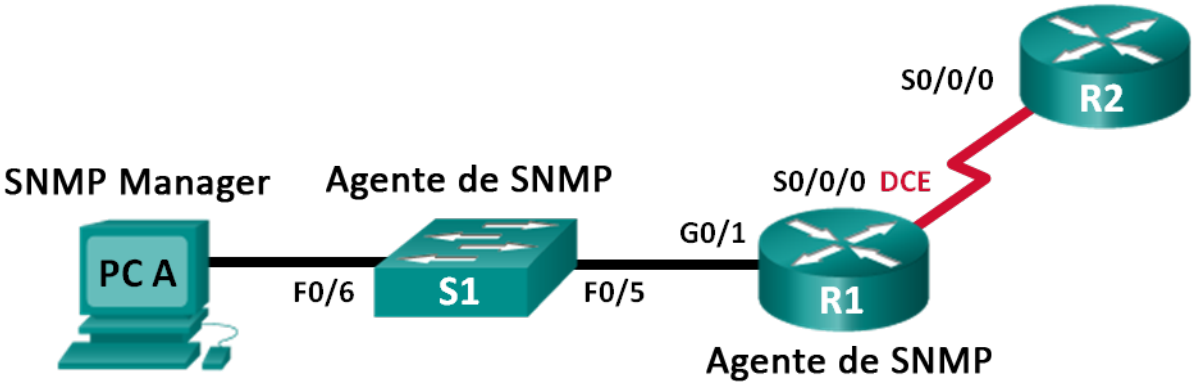


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

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

Parte 2: Configurar un administrador de SNMP y agentes SNMP

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

Información básica/situación

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

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

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

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

```
S1# show sdm prefer
```

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

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

Recursos necesarios

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

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

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

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

Paso 2: Configurar el equipo host.

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

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

a. Desactive la búsqueda del DNS.

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

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

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

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

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

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

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

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

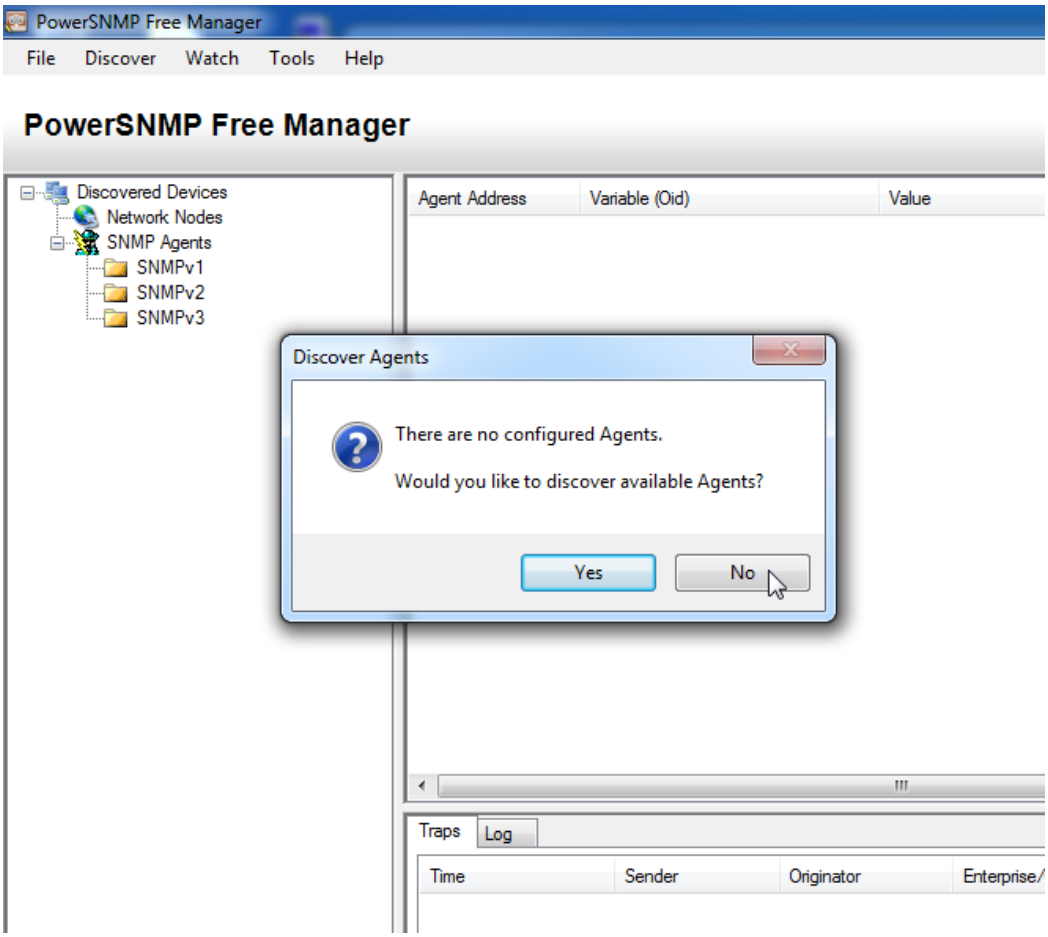
En la parte 2, se instalará y se configurará el software de administración SNMP en la PC-A, y se configurará el R1 y el S1 como agentes SNMP.

Paso 1: Instalar un programa de administración SNMP.

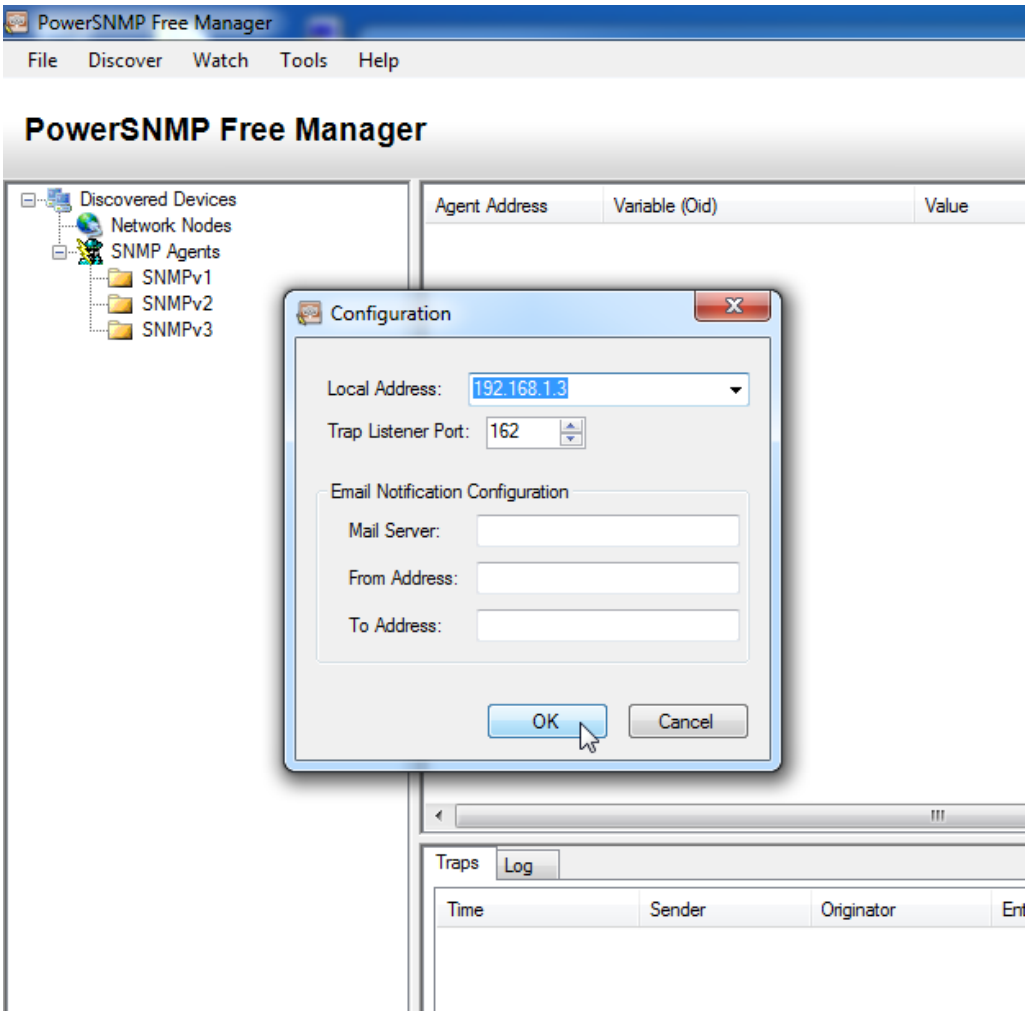
a. Descargue e instale PowerSNMP Free Manager de Dart Communications del siguiente URL: http://www.dart.com/snmp-free-manager.aspx.

b. Inicie el programa PowerSNMP Free Manager.

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



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



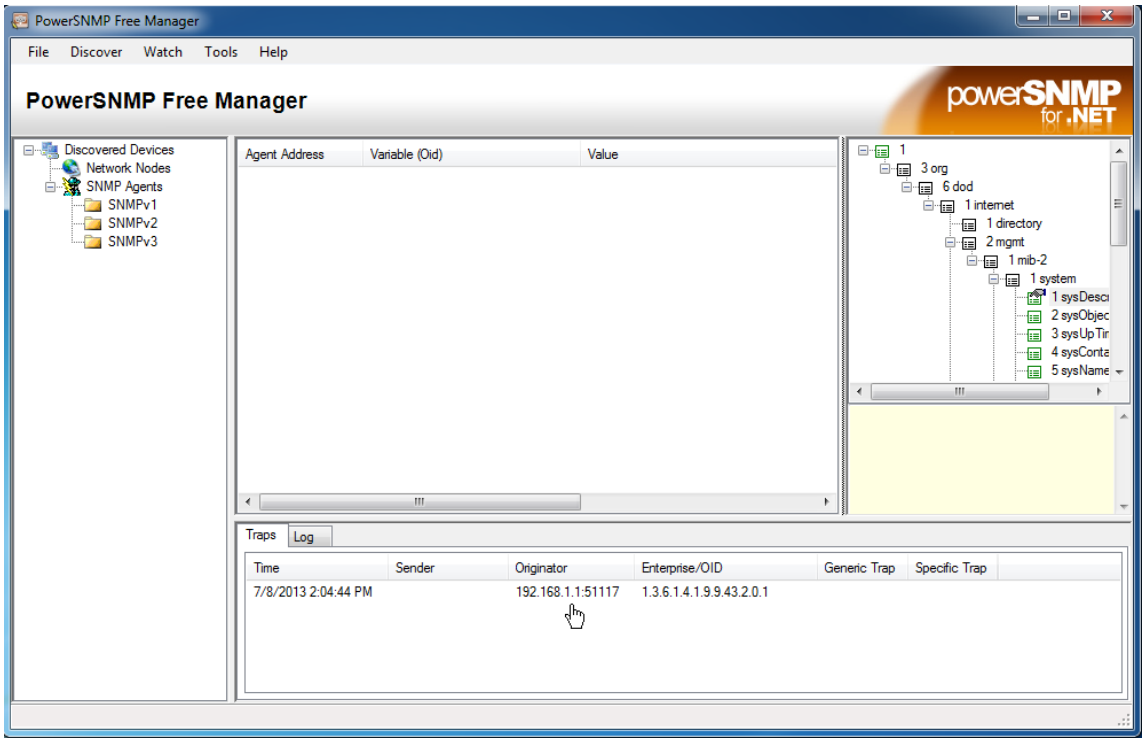
Nota: si se le pide que detecte los agentes SNMP disponibles, haga clic en **No** y continúe con la siguiente parte de la práctica de laboratorio.

Paso 2: Configurar un agente SNMP.

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

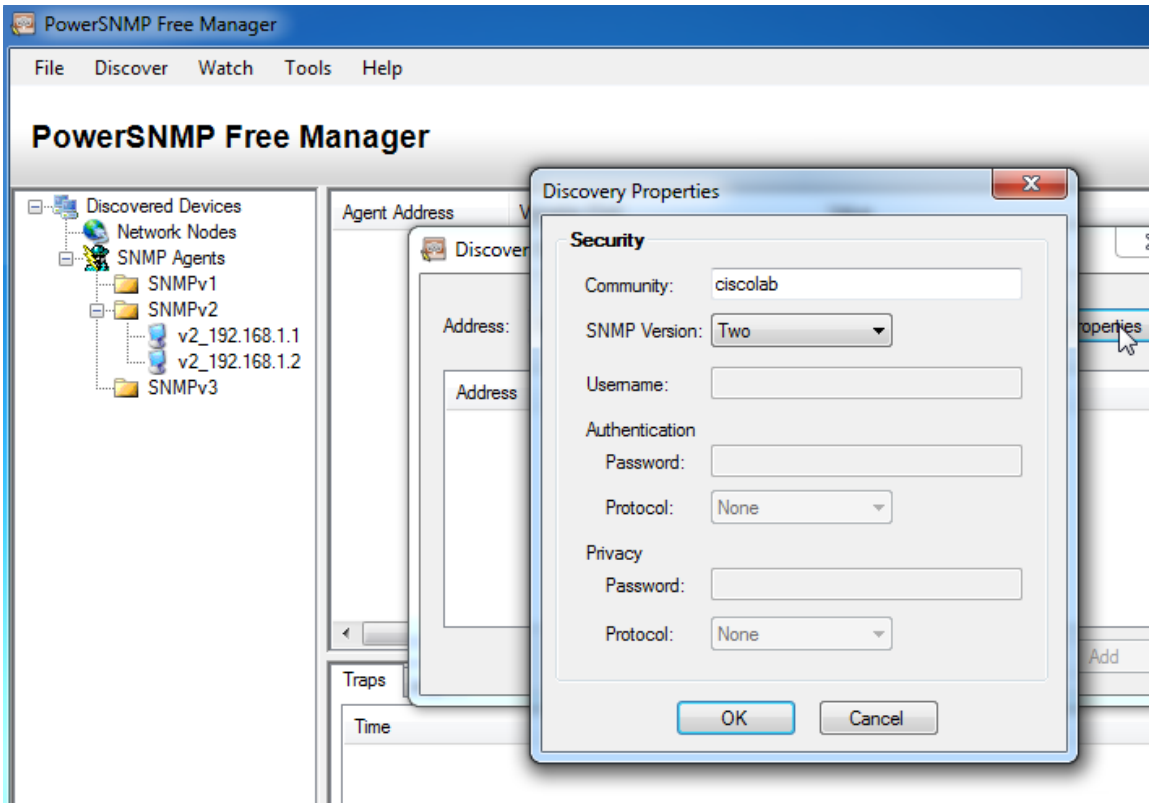
```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

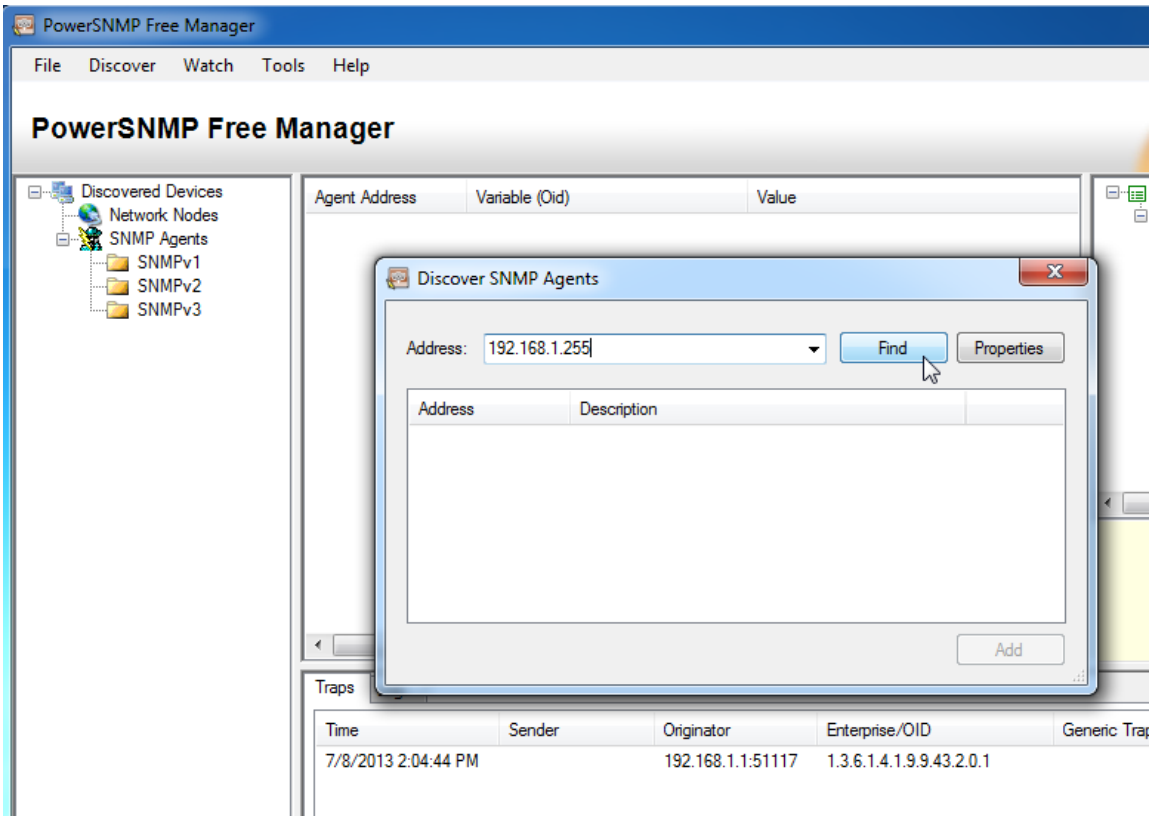

b. En este momento, puede observar que PowerSNMP Free Manager recibe notificaciones del R1. De lo contrario, puede intentar forzar que se envíe una notificación SNMP mediante la introducción del comando **copy run start** en el R1. Continúe con el siguiente paso si no se realiza correctamente.

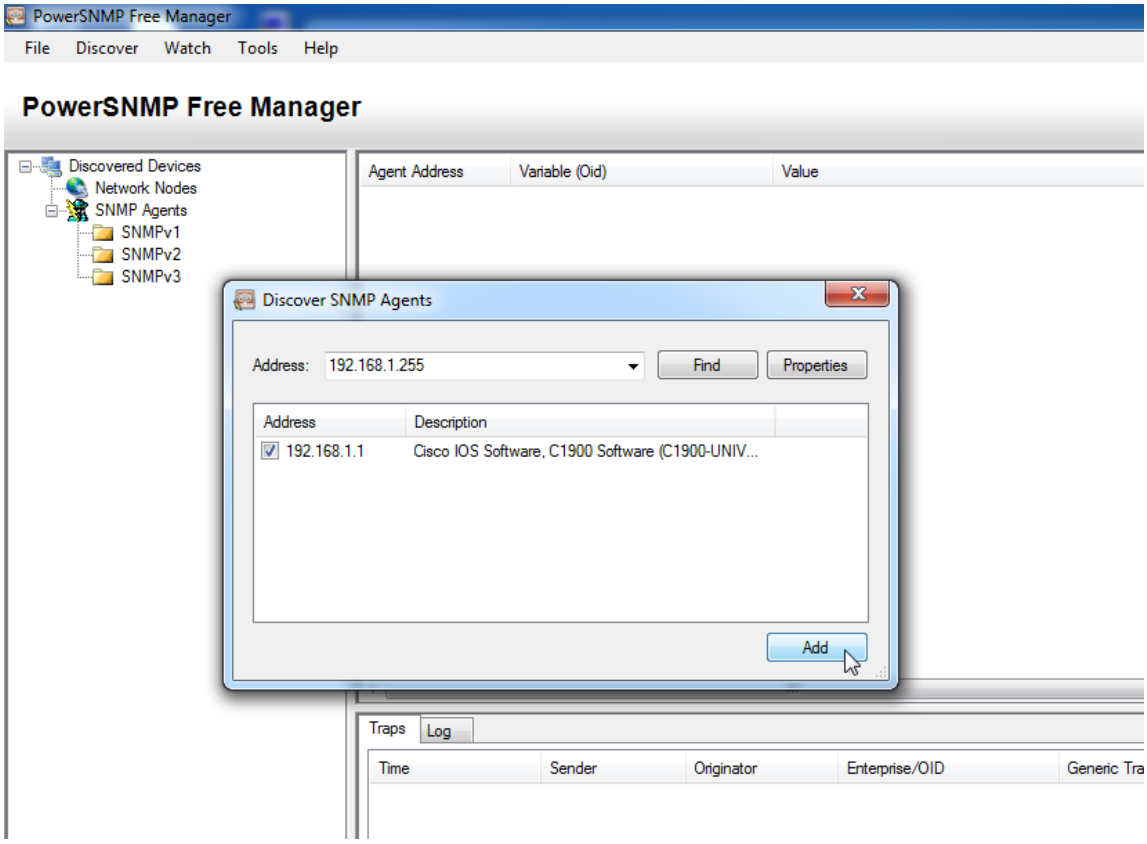


Paso 3: Detectar los agentes SNMP.

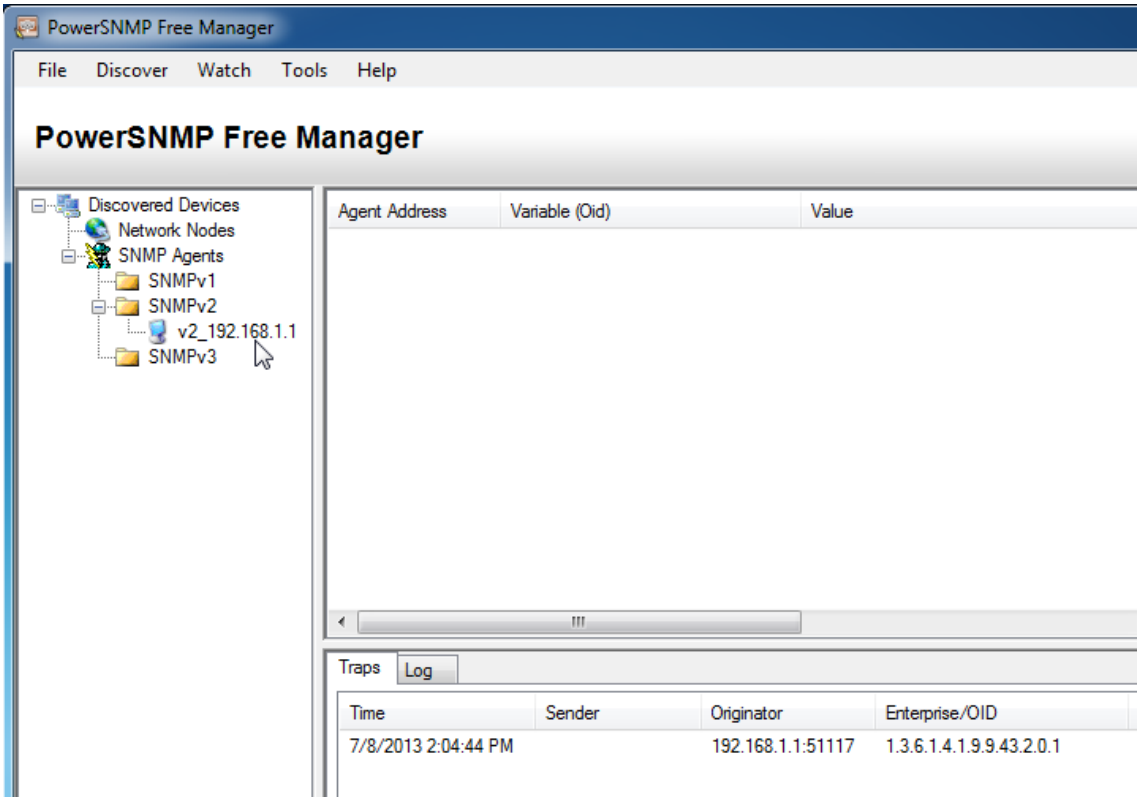
a. Desde PowerSNMP Free Manager en la PC-A, abra la ventana **Discover > SNMP Agents** (Detectar > Agentes SNMP). Introduzca la dirección IP **192.168.1.255**. En la misma ventana, haga clic en **Properties** (Propiedades) y establezca **ciscolab** en Community (Comunidad) y **Two** (Dos) en SNMP Version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







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



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

```
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server location snmp_manager
S1(config)# snmp-server contact ciscolab_admin
S1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
S1(config)# snmp-server enable traps
S1(config)# ip access-list standard SNMP_ACL
S1(config-std-nacl)# permit 192.168.1.3
```

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

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

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

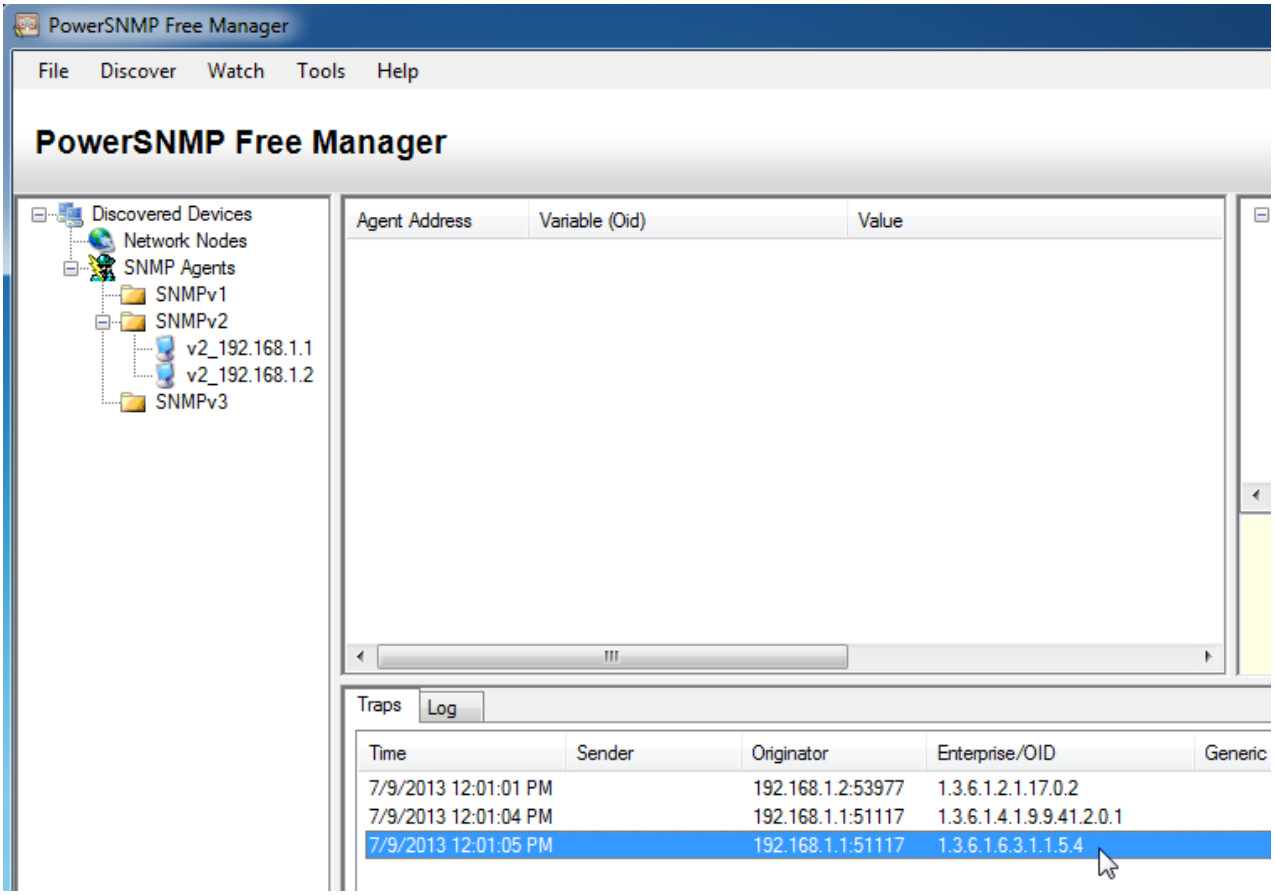
Paso 1: Borrar los mensajes de SNMP actuales.

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

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

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

```
R1(config)# interface s0/0/0
R1(config)# ip address 192.168.2.1 255.255.255.252
R1(config)# clock rate 128000
R1(config)# no shutdown
```

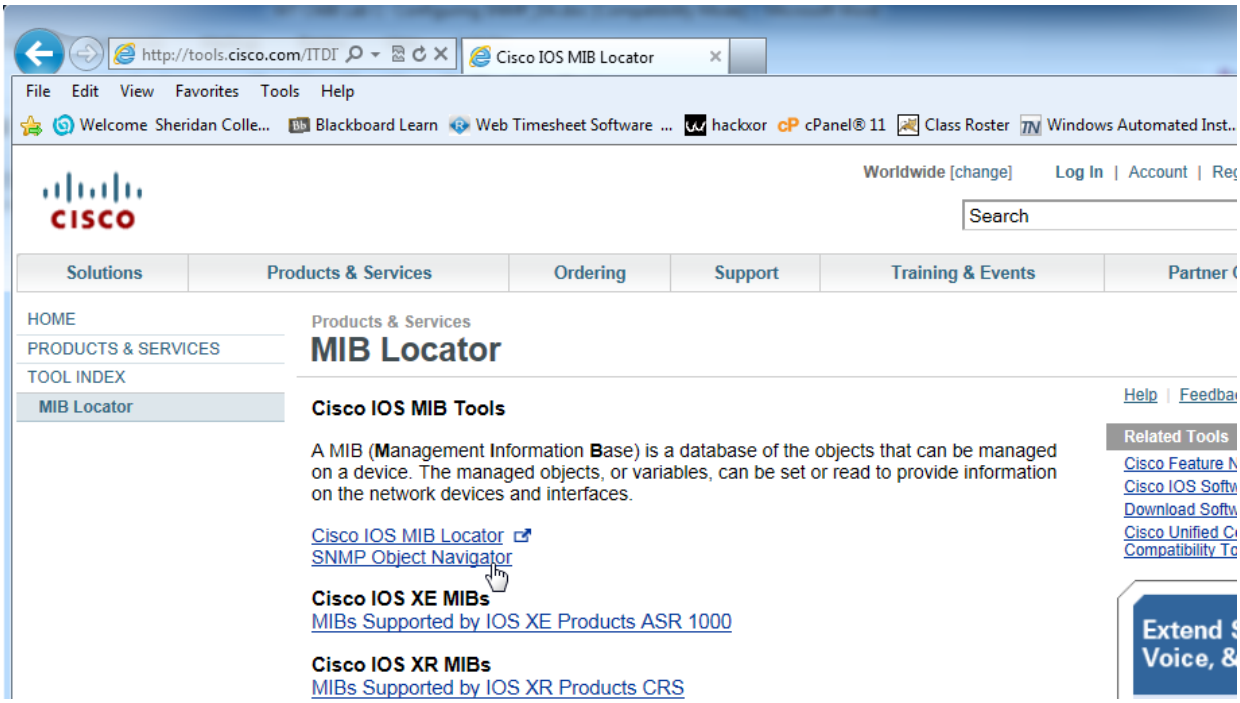
Paso 3: Decodificar los mensajes MIB y OID de SNMP.

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

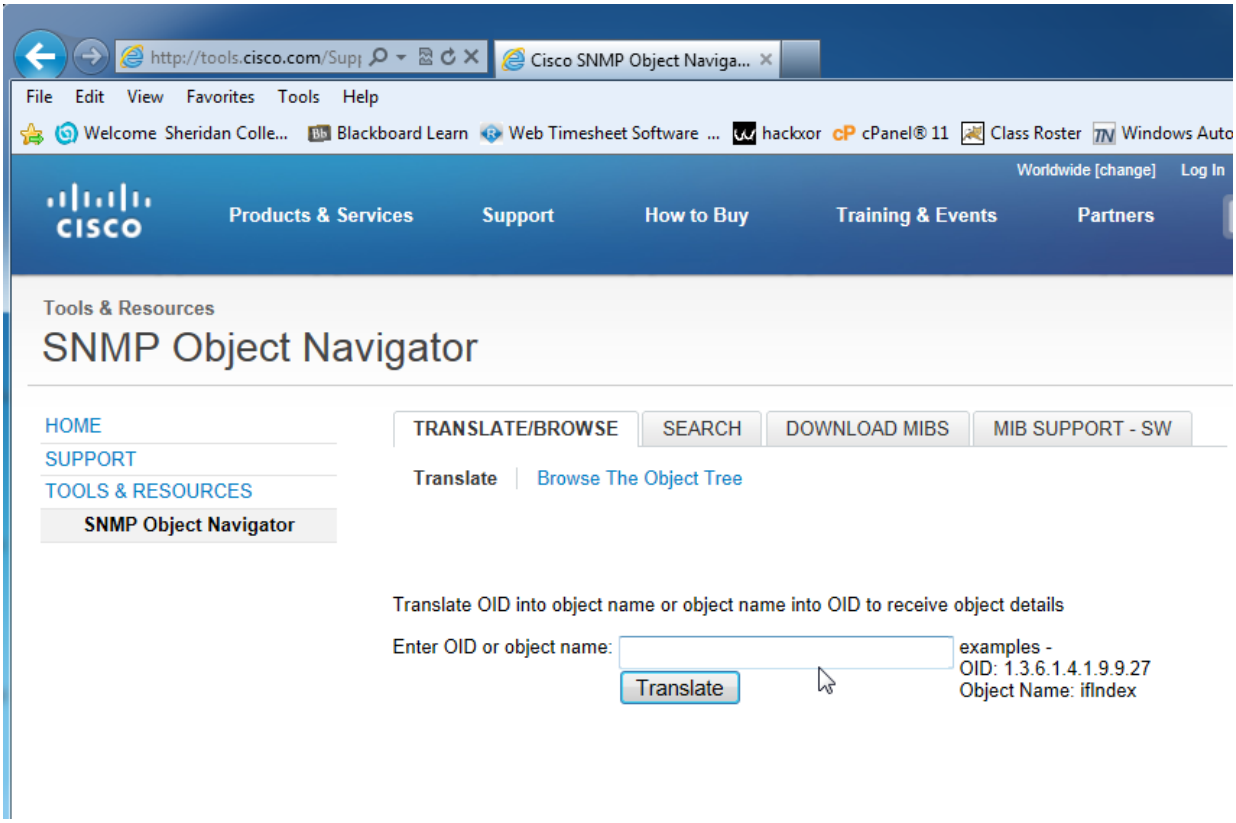
a. Mediante la herramienta de búsqueda en la parte superior de la ventana, busque **SNMP Object Navigator**.

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

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



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



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

Por ejemplo, la descripción del OID 1.3.6.1.6.3.1.1.5.4 es una trap de linkUp que significa que la entidad SNMP, en función de agente, detectó que el objeto ifOperStatus para uno de los enlaces de comunicación dejó el estado inactivo y pasó a otro estado (pero no al estado notPresent). El valor ifOperStatus que se incluye indica este otro estado.

Reflexión

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

Las respuestas varían, pero los estudiantes pueden señalar la capacidad de SNMP como protocolo abierto y multiplataforma para funcionar con diversos dispositivos, incluidos los equipos host en la red. SNMP beneficia a un administrador de red cuyo trabajo es controlar el estado y la configuración de los hosts de red a través toda la red.

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

Dado que SNMPv2 admite solamente cadenas de comunidad sin cifrar, utilizar acceso de lectura y escritura sería un mayor riesgo de seguridad.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos

Router R1

```
R1#show run
Building configuration...

Current configuration : 5969 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
```



```
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
!
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
```



```
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps c3g
snmp-server enable traps entity-sensor threshold
snmp-server enable traps adslline
snmp-server enable traps vdsl2line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp cbgp2
snmp-server enable traps isis
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-
change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
```



```
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps waas
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps firewall serverstatus
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.1.3 version 2c ciscolab
!
control-plane
```



```
!
line con 0
 password cisco
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

R2 del router

```
R2#show run
Building configuration...

Current configuration : 1251 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
 no ip address
```



```
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
```



```
end
```

Switch S1

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

Current configuration : 4618 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
```



```
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
```



```
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-
guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet police
snmp-server enable traps fru-ctrl
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps ipsla
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.1.3 version 2c ciscolab
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```


Práctica de laboratorio: Recopilación y análisis de datos de NetFlow (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

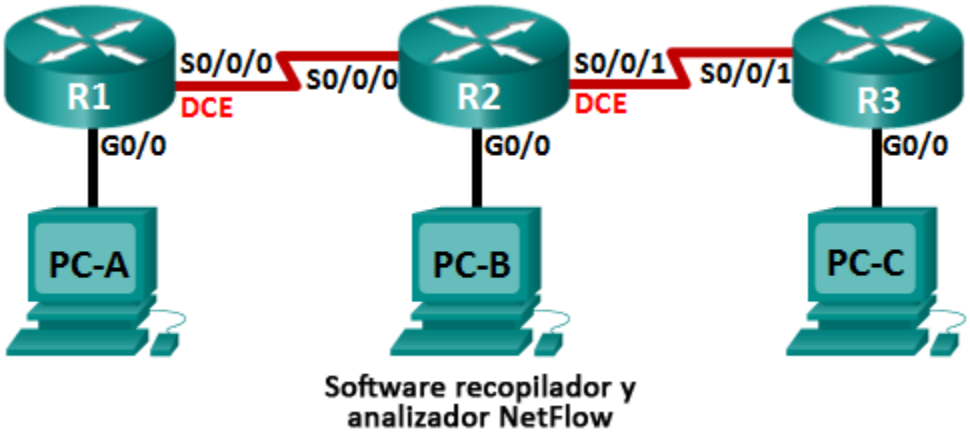


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
R1	G0/0	192.168.1.1/24	N/A
	S0/0/0 (DCE)	192.168.12.1/30	N/A
R2	G0/0	192.168.2.1/24	N/A
	S0/0/0	192.168.12.2/30	N/A
	S0/0/1 (DCE)	192.168.23.1/30	N/A
R3	G0/0	192.168.3.1/24	N/A
	S0/0/1	192.168.23.2/30	N/A
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Objetivos

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

Parte 2: Configurar NetFlow en un router

Parte 3: Analizar NetFlow mediante la CLI

Parte 4: Explorar el software recopilador y analizador NetFlow

Información básica/situación

NetFlow es una tecnología del IOS de Cisco que proporciona estadísticas sobre los paquetes que fluyen a través de un switch multicapa o un router Cisco. NetFlow habilita el monitoreo de red y de seguridad, la planificación de la red, el análisis de tráfico y la contabilidad de IP. Es importante no confundir el propósito y los resultados de NetFlow con los del hardware y el software de captura de paquetes. La captura de paquetes registra toda la información posible que sale de un dispositivo de red o que ingresa a este para un análisis posterior, NetFlow identifica información estadística específica.

Flexible NetFlow es la tecnología de NetFlow más reciente y mejora el NetFlow original al agregar la capacidad de personalizar los parámetros de análisis de tráfico. Flexible Netflow usa el formato de exportación de la versión 9. A partir de la versión 15.1 del IOS de Cisco, se admiten muchos comandos útiles de Flexible NetFlow.

En esta práctica de laboratorio, configurará NetFlow para capturar paquetes entrantes y salientes. Utilizará comandos **show** para verificar que NetFlow funciona y recopila información estadística. También explorará las opciones disponibles para el software de recopilación y de análisis de NetFlow.

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

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

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

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

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

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

Paso 2: inicializar y volver a cargar los routers según sea necesario.

Paso 3: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

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

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

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

e. Cifre las contraseñas de texto no cifrado.

f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

g. Configure **logging synchronous** para la línea de consola.

h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

i. Configure las direcciones IP como se indica en la tabla de direccionamiento.

j. Configure OSPF con la ID de proceso 1 y anuncie todas las redes. Las interfaces Ethernet deben ser pasivas.

k. Cree una base de datos local en el R3 con el nombre de usuario **admin** y la contraseña **cisco** con el nivel de privilegio **15**.

l. En el R3, habilite el servicio HTTP y autentique los usuarios HTTP con la base de datos local.

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

Paso 4: configurar los equipos host.

Paso 5: Verificar la conectividad de extremo a extremo.

Todos los dispositivos deben poder hacer ping a los otros dispositivos en la topología. Resuelva los problemas según sea necesario hasta que se establezca la conectividad de extremo a extremo.

Nota: quizá sea necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

Parte 2: Configurar NetFlow en un router

En la parte 2, configurará NetFlow en el router R2. NetFlow capturará todo el tráfico entrante y saliente en las interfaces seriales del R2 y exportará los datos al recopilador NetFlow, la PC-B. Se utilizará la versión 9 de Flexible NetFlow para realizar la exportación al recopilador NetFlow.

Paso 1: Configurar la captura de NetFlow.

Configure la captura de datos de NetFlow en ambas interfaces seriales. Capture datos de los paquetes entrantes y salientes.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Paso 2: Configure la exportación de datos de NetFlow.

Utilice el comando **ip flow-export destination** para identificar la dirección IP y el puerto UDP del recopilador NetFlow al cual el router debe exportar los datos de NetFlow. Se utilizará el número de puerto UDP 9996 para esta configuración.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```


Paso 3: Configure la versión de exportación de NetFlow.

Los routers Cisco que ejecutan el IOS 15.1 admiten las versiones de NetFlow 1, 5 y 9. La versión 9 es el formato de exportación de datos más versátil, pero no es compatible con las versiones anteriores. Utilice el comando **ip flow-export version** para establecer la versión de NetFlow.

```
R2(config)# ip flow-export version 9
```

Paso 4: Verificar la configuración de NetFlow

a. Emita el comando **show ip flow interface** para revisar la información de la interfaz de captura de NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Emita el comando **show ip flow export** para revisar la información de exportación de datos de NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Parte 3: Analizar NetFlow mediante la CLI

En la parte 3, generará tráfico de datos entre el R1 y el R3 para observar la tecnología NetFlow.

Paso 1: Generar tráfico de datos entre el R1 y el R3.

a. Acceda mediante Telnet del R1 al R3 con la dirección IP 192.168.3.1. Introduzca la contraseña **cisco** para ingresar al modo EXEC del usuario. Introduzca la contraseña **class** para habilitar el modo EXEC global. Emita el comando **show run** para generar tráfico de Telnet. Mantenga activa la sesión de Telnet por ahora.

b. Desde el R3, emita el comando **ping 192.168.1.1 repeat 1000** para hacer ping a la interfaz G0/0 del R1. Esto generará tráfico ICMP a través del R2.

c. Desde la PC-A, acceda al R3 con la dirección IP 192.168.3.1. Inicie sesión como **admin** con la contraseña **cisco**. Mantenga el explorador abierto después de iniciar sesión en el R3.

Nota: asegúrese de que el bloqueador de elementos emergentes esté deshabilitado en el explorador.

Paso 2: Mostrar un resumen de las estadísticas de contabilidad de NetFlow.

En el R2, emita el comando **show ip cache flow** para mostrar los cambios en el resumen de datos de NetFlow, incluso la distribución del tamaño de paquetes, la información del flujo IP, los protocolos capturados y la actividad de interfaz. Observe que ahora se muestran los protocolos en los datos de resumen.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4      0.0        27    43      0.2       5.0      15.7
TCP-WWW            104      0.2        14   275      3.4       2.1       1.5
ICMP                 4      0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:             112      0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Paso 3: Finalizar las sesiones de Telnet y del explorador.

a. Emita el comando **exit** en el R1 para desconectarse de la sesión de Telnet al R3.

b. Cierre la sesión del explorador en la PC-A.

Paso 4: Borrar las estadísticas de contabilidad de NetFlow.

a. En el R2, emita el comando **clear ip flow stats** para borrar las estadísticas de contabilidad de NetFlow.

```
R2# clear ip flow stats
```

b. Vuelva a emitir el comando **show ip cache flow** para verificar que se hayan restablecido las estadísticas de contabilidad de NetFlow. Observe que, aunque ya no genera más datos a través del R2, NetFlow captura datos. En el ejemplo que se muestra a continuación, la dirección de destino para este tráfico es la dirección de multidifusión 224.0.0.5, o los datos de LSA de OSPF.

```
R2# show ip cache flow
```



```
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other             2      0.0       193    79      0.6    1794.8       5.7
Total:               2      0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Parte 4: Explorar el software recopilador y analizador NetFlow

El software recopilador y analizador NetFlow se puede conseguir de muchos proveedores. Algunas opciones de software se proporcionan como freeware, otras no. El siguiente URL proporciona una página web de resumen de algunas opciones de software de NetFlow freeware disponibles: http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html.

Revise esta página web para conocer algunos de los productos de software recopilador y analizador NetFlow disponibles.

Reflexión

1. ¿Cuál es el propósito del software recopilador NetFlow?

_____

_____

_____

El software recopilador NetFlow recibe los datos de NetFlow que se exportan de los routers y los switches en la red. Filtra y agrega los datos según las políticas que establece el administrador de red, y almacena los datos resumidos o agregados, en lugar de los datos de flujo sin procesar, para minimizar el consumo de espacio en disco.

2. ¿Cuál es el propósito del software analizador NetFlow?

   _____

   _____

   _____

   El software analizador NetFlow proporciona medios para visualizar y analizar en tiempo real los datos de flujo registrados y agregados. Le permite especificar el router, el esquema de agregación y el intervalo de tiempo en el cual desea verlos. Después puede clasificar y visualizar los datos de una manera que sea útil para los usuarios (gráficos de barras, gráficos circulares o histogramas de los informes clasificados).

3. ¿Cuáles son los siete campos fundamentales que usa NetFlow original para diferenciar flujos?

   _____

   _____

   Dirección IP de origen, dirección IP de destino, número de puerto de origen, número de puerto de destino, tipo de protocolo de capa 3, marca de tipo de servicio (TOS), interfaz lógica de entrada.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Configuraciones de dispositivos (final)

Router R1

```
R1# show run
Building configuration...

Current configuration : 1592 bytes
```



```
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.1.0 0.0.0.255 area 0
```



```
 network 192.168.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 030752180500
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 02050D480809
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

R2 del router

```
R2# show run
Building configuration...

Current configuration : 1808 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```



```
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 ip flow ingress
 ip flow egress
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 ip flow ingress
 ip flow egress
 clock rate 128000
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip flow-export version 9
ip flow-export destination 192.168.2.3 9996
```



```
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 060506324F41
 login
 transport input all
!
scheduler allocate 20000 1000
!
End
```

R3 del router

```
R3# show run
Building configuration...

Current configuration : 1769 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
```



```
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 192.168.23.2 255.255.255.252
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 exec-timeout 0 0
 password 7 01100F175804
 logging synchronous
```



```
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 0822455D0A16
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```


Caja de herramientas de un administrador de red para el monitoreo (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.

Objetivo

Explicar los diversos recursos que se pueden usar para recibir mensajes de registro del router.

Nota para el instructor: esta actividad se puede completar en forma individual o en grupos pequeños y después se puede compartir con la clase.

Situación

Como administrador de red de una pequeña o mediana empresa, acaba de comenzar con el monitoreo de red mediante CLI en los routers, los switches y los servidores de la empresa.

Decide crear una lista situacional en la que explica cuándo usar cada método. Los métodos de monitoreo de red que se deben incluir son los siguientes:

- Syslog
- SNMP
- NetFlow

Recursos

- Software de procesamiento de texto

Instrucciones

Paso 1: Crear varias situaciones en las que un administrador de red deba usar syslog, SNMP y NetFlow.

Paso 2: Indicar las situaciones en formato de matriz y solicitar a otro estudiante o grupo que identifique qué herramienta de monitoreo mediante CLI se debe usar para recopilar información acerca de los problemas de red descritos.

Paso 3: Compartir la matriz con otro grupo o con la clase.

Ejemplo sugerido de la actividad:

Situaciones para la herramienta de monitoreo mediante CLI

Situación	Herramienta de monitoreo de red mediante CLI que se debe usar
Se instaló un nuevo sistema VoIP en la red. Usted desea conservar registros de la carga de la red durante una semana para ver si se debe redistribuir o equilibrar el tráfico.	NetFlow
Algunos empleados informan disponibilidad de red esporádica a diario. Usted cree que podría ser un problema de router o de switch, pero no está seguro y desea realizar una revisión rápida de los enlaces en los equipos de red.	Syslog
Se debe realizar una revisión del estado de cada interfaz en los routers y los switches de la empresa. La información de estado incluye lo siguiente: • Qué interfaces están activas o inactivas • Qué octetos se enviaron y se recibieron • Errores de ping y tráfico descartado	SNMP

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Herramientas de monitoreo de red
- Syslog
- SNMP
- NetFlow

Falla 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.

Objetivo

Resolver problemas de conectividad IP mediante comandos básicos.

Nota para el instructor: conviene realizar esta actividad en grupos de dos estudiantes; luego, se puede compartir y analizar con otro grupo de estudiantes, con toda la clase o con el instructor.

Situación

Acaba de mudarse a una nueva oficina, y la red es muy pequeña. Después de un largo fin de semana dedicado a configurar la nueva red, advierte que esta no funciona correctamente.

Algunos dispositivos no tienen acceso entre ellos y algunos no pueden acceder al router que se conecta al ISP.

Su responsabilidad consiste en llevar a cabo la resolución y la reparación de problemas. Para identificar las posibles áreas de resolución de problemas, decide comenzar con los comandos básicos.

Recursos

- Software Packet Tracer

Instrucciones

Paso 1: Cree una topología de la red simple mediante el software Packet Tracer, que incluya lo siguiente:

a. Dos routers de la serie 1941 conectados

b. Dos switches Cisco 2960, uno conectado a cada router para formar dos LAN

c. Seis dispositivos para usuarios finales

1) Una impresora y tres computadoras de escritorio o portátiles en la LAN1

2) Dos servidores en la LAN2

Paso 2: Configure la red y los dispositivos de usuario y verifique que todo funcione correctamente. Introduzca uno o dos errores en las configuraciones. Asegúrese de desactivar los parámetros Options (Opciones), Preferences (Preferencias) y Show Link Light (Mostrar luces de enlace) que están disponibles en el software Packet Tracer.

Paso 3: Comparta el archivo guardado de Packet Tracer con otro grupo; haga que encuentren y corrijan los problemas usando solo los comandos siguientes:

- `ping`
- `traceroute`
- `telnet`
- `show interface`
- `show IP interface brief` or `show IPv6 interface brief`

- `show IP route` or `show IPv6 route`
- `show running-config`
- `show protocols`
- `show vlan`

Paso 4: Comparta los resultados de la actividad con la clase o el instructor. ¿Cómo corrigieron los grupos los problemas?

Solución de ejemplo sugerida para la actividad:

Notas para el instructor:

Todos los archivos, problemas y correcciones de los estudiantes variarán. Los alumnos deben poder demostrar cómo usaron los comandos básicos de resolución de problemas para identificar los problemas de la red.

Algunos problemas posibles en la red podrían incluir la configuración incorrecta o la falta de lo siguiente:

Autenticación

Direcciones IP y máscaras de subred (IPv4 o IPv6) en los dispositivos de red o las estaciones de trabajo

Protocolos de routing (capa 2 o 3)

Cableado (tipos o conexiones de cables incorrectos)

Colocación de la frecuencia de reloj (DCE)

Rutas predeterminadas o estáticas

Estados de interfaz (inactivo)

Configuración de la VLAN (nombres, asignaciones de puertos, direccionamiento, desactivación, entre otros)

Asegúrese de que los estudiantes desactiven la preferencia de luz de enlace en el software Packet Tracer; de esa manera, usarán los comandos indicados en esta actividad para buscar y corregir los problemas de red.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Comandos para recolectar síntomas para la resolución de problemas de red
- Procedimientos de resolución de problemas

Elaboración del registro (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.

Objetivo

Resolver los problemas en la red de una pequeña a mediana empresa mediante un enfoque sistemático.

Nota para el instructor: conviene realizar esta actividad en grupos pequeños. Después se puede compartir con otro grupo, la clase o el instructor (como proyecto de grupo).

Situación

Como administrador de red de una pequeña empresa, desea implementar un sistema de registro para usar en la resolución de problemas de red.

Después de pensar mucho, decide recopilar información simple de la documentación de red en un archivo que se utilizará cuando surjan problemas de red. También sabe que si la empresa crece en el futuro, se puede usar este archivo para exportar la información a un sistema de software de red computarizado.

Para comenzar el proceso de documentación de red, usted incluye lo siguiente:

- Un diagrama físico de la red de su pequeña empresa.
- Un diagrama lógico de la red de su pequeña empresa.
- Información de configuración de red para los dispositivos importantes, incluidos routers y switches.

Recursos

- Software Packet Tracer
- Software de procesamiento de texto

Paso 1: Cree un archivo de Packet Tracer para simular una red empresarial muy pequeña. Incluya estos dispositivos:

- Un router con, por lo menos, dos puertos Ethernet
- Dos switches conectados al router (LAN1 y LAN2)
- Cinco dispositivos de usuario, que incluyan computadoras de escritorio o portátiles, servidores e impresoras conectados a cualquiera de las dos LAN.

Paso 2: Cree un archivo de procesamiento de texto en formato de matriz para registrar cada una de las siguientes áreas principales de documentación de red:

a. Topología física e información
   1) Tipo de dispositivo y nombre del modelo
   2) Nombre de host de la red
   3) Ubicación del dispositivo
   4) Tipos y puertos de conexiones de cables

b. Información de topología lógica
   1) Versiones de la imagen del IOS o OS
   2) Direcciones IP (IPv4, IPv6 o ambas)

3) Direcciones de enlace de datos (MAC)

4) Direcciones VLAN

c. Información de configuración del dispositivo de red

1) Ubicación del archivo de copia de seguridad (servidor TFTP, USB, archivo de texto)

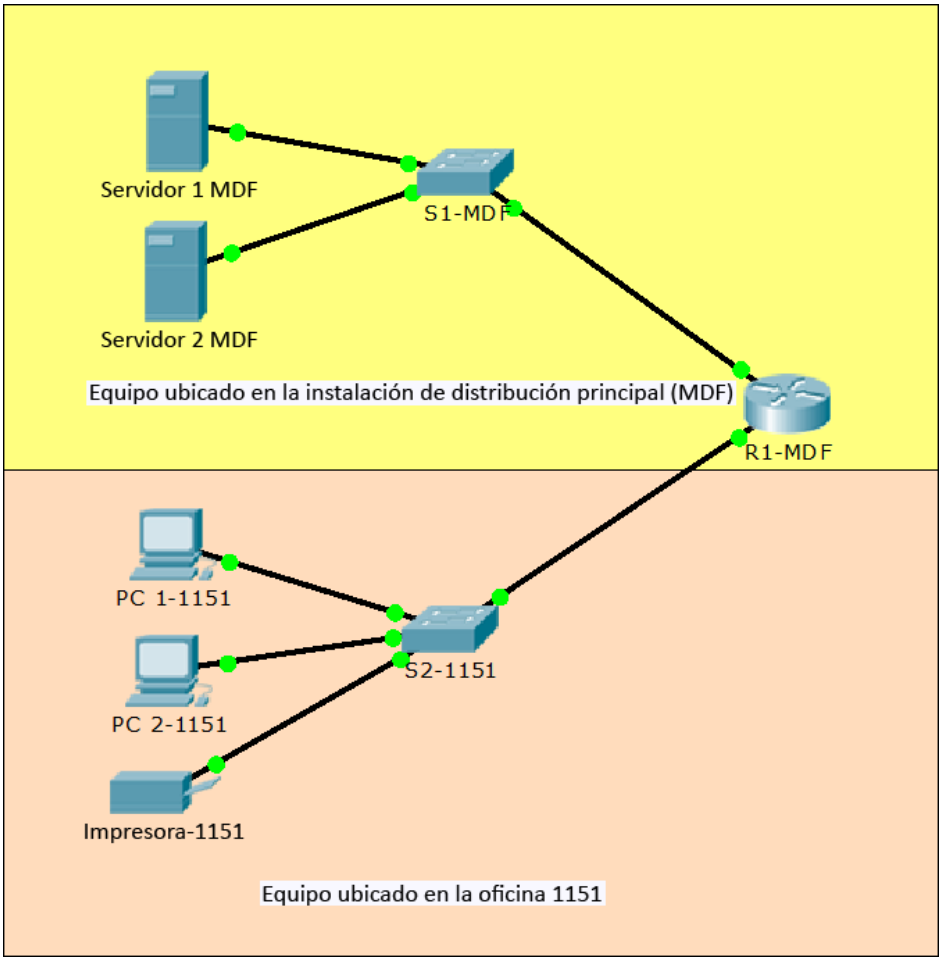
2) Secuencia de comandos de configuración en formato de texto para cada dispositivo de router y switch

Paso 3: Comparta el archivo de Packet Tracer y la documentación de red con un compañero, otro grupo, la clase o el instructor, según las instrucciones proporcionadas. Analice la forma en que esta información puede ser útil para cualquier administrador de red.

Solución de ejemplo sugerida para la actividad: (todas las soluciones de los estudiantes varían)

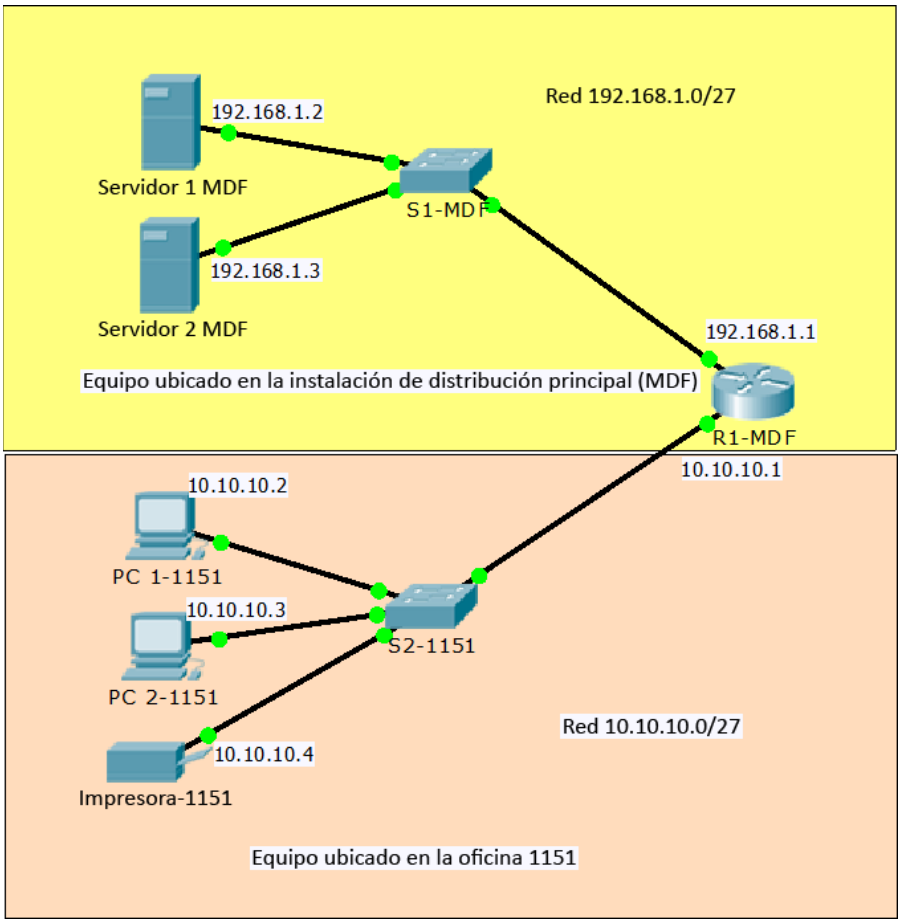
Nota para el instructor: solo se incluye el resultado de la configuración de red para el router.

Diagrama de topología física de la red



Elaboración del registro

Diagrama de topología lógica de la red



Información de la documentación de red

Documentación de red física	
Tipo de dispositivo	**Router**
Nombre del modelo	Cisco 1941 (router modular)
Nombre de host de la red	R1-MDF
Ubicación de la red física	Instalación de distribución principal (MDF, Main Distribution Facility)
Tipos de interfaces y conexiones de enlaces	Enlace GigabitEthernet0/0 a GigabitEthernet1/1 de S1-MDF Enlace GigabitEthernet0/1 a GigabitEthernet0/1 de S2-1151

Elaboración del registro

Topología lógica e información	
Nombre del archivo de imagen de sistema y del IOS o versión del OS de la estación de trabajo	Software C1900 (C1900-UNIVERSALK9-M), versión 15.1(4)M4 flash0:c1900-universalk9-mz.SPA.151-1.M4.bin
dirección IP	192.168.1.1 GigabitEthernet0/0 10.10.10.1 GigabitEthernet0/1
Dirección MAC	0001.63b1.2701 (bia 0001.63b1.2701 GigabitEthernet0/0 0001.63b1.2702 (bia 0001.63b1.2702 GigabitEthernet0/1
Direcciones VLAN	ninguno

Información de configuración del dispositivo de red	
Ubicación del archivo de copia de seguridad	USB externo (consultar al administrador de red) Espacio del servidor TFTP en el servidor 2-MDF
Secuencias de comandos de configuración de red (configuración en ejecución)	R1-MDF# **show running-config** Building configuration... Current configuration : 667 bytes ! version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec no service password-encryption ! hostname R1-MDF ! license udi pid CISCO1941/K9 sn FTX1524CE1T ! spanning-tree mode pvst ! interface GigabitEthernet0/0 ip address 192.168.1.1 255.255.255.224 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 10.10.10.1 255.255.255.224 duplex auto speed auto ! interface Vlan1 no ip address shutdown ! ip classless ! line con 0 ! line aux 0

	`` ! line vty 0 4 login ! end ```

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Documentación de red para la resolución de problemas
- Topología física de la red
- Topología lógica de la red