Cisco | Networking Academy®
Mind Wide Open™

CCNA Exploration 4.0

Aspectos básicos de redes
Manual de prácticas de laboratorio para el estudiante

Actividad 1.1.1: Uso de Google Earth™ para ver el mundo

Objetivos de aprendizaje

Al completar esta actividad, usted podrá:

- Explicar el objetivo de Google Earth.
- Explicar las diferentes versiones de Google Earth.
- Explicar los requisitos de hardware y software necesarios para usar Google Earth (edición gratuita).
- Probar funciones de Google Earth como Ayuda | Tutorial.
- Experimentar con Google Earth la exploración de continentes, países y lugares de interés.

Información básica

Google Earth es una aplicación muy popular que se ejecuta en el escritorio de la mayoría de los sistemas operativos. Requiere una conexión de banda ancha a Internet y muestra la Tierra como una imagen 2D o 3D manipulada. El reconocido canal de noticias internacionales, CNN, usa regularmente Google Earth para resaltar dónde se ha producido una noticia.

Al momento de escribir esta actividad existen tres versiones de Google Earth. La versión que cubre la mayoría de las necesidades es la versión gratuita de Google, Google Earth. Una versión Google Earth Plus incluye compatibilidad con GPS, un importador de hoja de cálculo y otras características de compatibilidad. La versión Google Earth Pro es para uso profesional y comercial. El URL http://earth.google.com/product_comparison.html contiene una descripción de las versiones. Use este enlace para contestar las siguientes preguntas:

¿Qué versión admite inclinación y rotación 3D? _____

¿Qué versión de Google Earth tiene la mayor resolución? _____

Para usar Google Earth, versión 4 es necesario cumplir con requerimientos mínimos de hardware:

Sistema operativo	Microsoft Windows 2000 o Windows XP
CPU	Pentium 3 con 500 MHz
Memoria del sistema (RAM)	128 MB
Disco duro	400 MB de espacio libre
Velocidad de red	128 kbps
Tarjeta gráfica	Compatible con 3D con 16MB de VRAM
Pantalla	Pantalla a color de alta densidad de 1.024x768 píxeles, 16-bit

Escenario

Esta actividad se realizará en una computadora que cuente con acceso a Internet en la cual pueda instalar el software.

El tiempo estimado para finalizarla, según la velocidad de la red, es de 30 minutos.

Tarea 1: Instalación de Google Earth.

Si Google Earth no está instalado en la computadora, se puede descargar la versión gratuita directamente desde http://earth.google.com/download-earth.html. Siga las instrucciones de instalación; la descarga de Google Earth debería iniciarse automáticamente. Recuerde que puede ser necesario desactivar los bloqueadores de elementos emergentes en el explorador.

Figura 1. Pantalla de apertura de Google Earth

Tarea 2: Ejecución de Google Earth.

Paso 1: Consulte la Figura 1, la pantalla de apertura. La barra de Menú está ubicada en la esquina superior izquierda de la pantalla. En el menú **Ayuda**, seleccione **Guía del usuario** para ejecutar un explorador Web predeterminado y ver la Guía del usuario de Google Earth. http://earth.google.com/userguide/v4/. Dedique unos minutos a explorar la Guía del usuario. Antes de salir del sitio Web de la Guía del usuario, conteste las siguientes preguntas:

Enumere tres formas de mover la imagen.

_____

_____

_____

¿Qué control del mouse acerca o aleja la imagen?

_____

¿Cuál es el objetivo del botón izquierdo del mouse?

_____

Tarea 3: Navegación por la interfaz de Google Earth.

Paso 1: Usar la función Vista general del mapa.

En el menú **Ver**, seleccione **Vista general del mapa**. Esta conveniente función proporciona una posición global de la imagen ampliada.

Paso 2: Revisar los controles de navegación.

Los controles de navegación están ubicados en el cuadrante superior derecho y controlan la ampliación y posición de la imagen. El puntero del mouse se debe mover cerca de los controles, de lo contrario sólo se muestra una brújula. Consulte la Figura 2 para obtener una descripción de los controles de navegación.

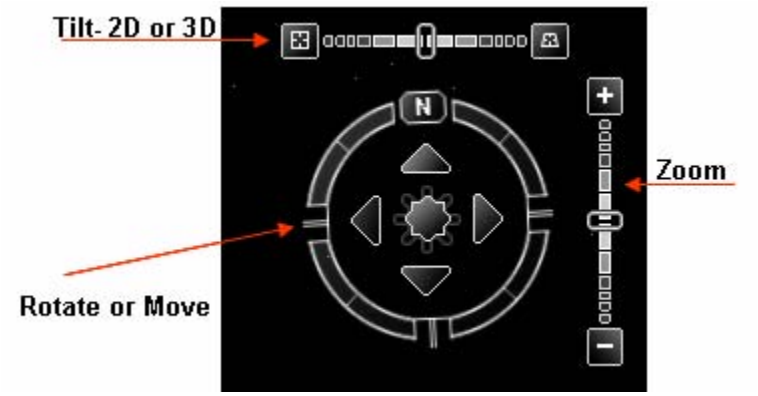


Figura 2. Herramientas de navegación de la pantalla de Google Earth

Paso 3: Usar la función Excursiones.

En la barra de navegación izquierda pruebe con la carpeta **Lugares > Excursiones**. Expanda Excursiones, elija una ubicación que desee visitar y haga doble clic sobre esa ubicación. La imagen lo llevará a ese lugar. Cuando llegue al destino, un indicador de imágenes de transmisión en tiempo real informa cuándo la resolución está completa.

Paso 4: Probar con la carpeta Buscar > Volar a.

Ingrese 95134, un código postal de EE. UU.

¿Qué ciudad y estado de los Estados Unidos se muestra? _____

¿Y si quisiera “Volar a” Londres, Reino Unido? ¿Qué datos se deberían ingresar?

_____

_____

Paso 5: Usar la función Volar a.

Algunas ubicaciones tienen mejor resolución que otras y algunas imágenes son más viejas que otras. Por ejemplo, un usuario comentó que encontró su casa, pero que la nueva casa al lado de la suya todavía no había sido construida. Intente encontrar su casa con la carpeta **Buscar > Volar a**.

¿La resolución para su casa es de la misma calidad que la de Excursiones del Paso 3? _____

Si la resolución para su barrio es suficiente, explore los alrededores para ver si puede determinar aproximadamente cuán vieja es la imagen.

Figura 3. Mapamundi con líneas de latitud y longitud

Paso 6: Ver las coordenadas geográficas.

Las coordinadas geográficas se muestran en el cuadrante inferior izquierdo de la imagen. El primer número se denomina latitud y es el ángulo entre un punto y el Ecuador. Por ejemplo, el Ecuador es una línea imaginaria que divide el globo en hemisferio norte y sur. El segundo número se denomina longitud y es el ángulo este u oeste de un punto arbitrario en la Tierra. El Observatorio Real, en el Reino Unido, es el punto internacional de longitud cero.La combinación de longitud y latitud se denomina gratícula. Las medidas de coordenadas se expresan en grados (°), minutos (‘), segundos y décimas (‘’). Para la latitud, la referencia es al Norte (N) o al Sur (S) del Ecuador. Para la longitud, la referencia es al Este (E) o al Oeste (O) del Observatorio Real. Consulte la Figura 3. Para obtener una definición simple de las coordenadas geográficas, vaya a la URL http://en.wikipedia.org/wiki/Geographic_coordinate_system. En el menú Ver elija Cuadrícula para mostrar las Cuadrículas de Google Earth.

Use el puntero y las coordenadas que se muestran en el cuadrante inferior izquierdo de la imagen, ¿cuáles son las coordenadas de su casa? _____

Tarea 4: Reflexión

Google Earth puede introducir el mundo en la casa o en la oficina. Mientras disfruta las imágenes, piense qué recursos de comunicación digital se usaron. Por ejemplo, la comunicación satelital con una estación terrestre transmitió la imagen de su casa a una ubicación en tierra. Se usaron algunos tipos de bases de datos para guardar la imagen. Una Red de área local (LAN) envió la imagen que usted solicitó a través de Internet, probablemente pasando por varias Redes de área extensa (WAN) y luego a otra LAN con una computadora que le devolvió la imagen. La demora en la recuperación de la imagen puede haber sido corta o larga, según la velocidad más baja de todas las conexiones de red de la ruta entre el registro de base de datos y su computadora.

¿Se podría haber mostrado la imagen más rápido si se hubieran usado técnicas de compresión?

Piense en la seguridad de la red. ¿Es posible que alguien se infiltrara en su conexión de red?

Tarea 5: Desafío

Google Earth muestra las coordenadas de las imágenes en el cuadrante inferior izquierdo de la misma. Use el siguiente URL para consultar diferentes sistemas de coordenadas: http://www.colorado.edu/geography/gcraft/notes/coordsys/coordsys.html Wikipedia tiene una definición útil de términos geográficos comunes.

Use el sistema de coordinación geográfica para describir su casa con la mayor exactitud y detalle posibles.

Tarea 6: Limpieza

Es posible que se le solicite que elimine Google Earth de la computadora. Si es así, realice los siguientes pasos:

1. Haga clic en **Inicio** > **Configuración** > **Panel de control**.
2. Haga doble clic en **Agregar o quitar programas**.
3. Ubique **Google Earth** y haga clic sobre éste.
4. Haga clic en **Eliminar** y siga las indicaciones.

Hay disponible información adicional sobre la eliminación en el URL http://earth.google.com/support/bin/answer.py?answer=20738&ctx=sibling.

A menos que se le indique otra cosa, apague la computadora.

Actividad 1.4.5: Identificación de las vulnerabilidades de seguridad más importantes

Objetivos de aprendizaje

Al completar esta actividad, usted podrá:

- Usar el sitio SANS para identificar rápidamente las amenazas de seguridad de Internet.
- Explicar cómo se organizan las amenazas.
- Enumerar varias vulnerabilidades de seguridad recientes.
- Usar los vínculos de SANS para acceder a información adicional relacionada con la seguridad.

Información básica

Uno de los sitios más conocidos y confiables relacionados con la defensa contra las amenazas de seguridad de computadoras y de redes es SANS. SANS proviene de SysAdmin, Audit, Network, Security (Administración del sistema, Auditoría, Red, Seguridad). SANS está formado por varios componentes, cada uno de los cuales contribuye en gran medida con la seguridad de la información. Para obtener información adicional sobre el sitio SANS, consulte http://www.sans.org/ y seleccione los temas en el menú Recursos.

¿Cómo puede un administrador de seguridad corporativa identificar rápidamente las amenazas de seguridad? SANS y el FBI han recopilado una lista de los 20 principales objetivos de ataques de seguridad en Internet en http://www.sans.org/top20/. Esta lista se actualiza periódicamente con información formateada por:

- Sistemas operativos: Windows, Unix/Linux, MAC
- Aplicaciones: interplataforma, incluyendo la Web, base de datos, punto a punto, mensajería instantánea, reproductores de medios, servidores DNS, software para copias de seguridad y servidores de administración
- Dispositivos de red: dispositivos de infraestructura de red (routers, switches, etc.), dispositivos VoIP
- Elementos humanos: políticas de seguridad, conducta humana, temas personales.
- Sección especial: temas de seguridad no relacionados con ninguna de las categorías anteriores.

Escenario

Esta práctica de laboratorio presentará a los estudiantes las vulnerabilidades en los asuntos de seguridad informática. Se usará el sitio Web de SANS como una herramienta para la identificación, comprensión y defensa de las amenazas de vulnerabilidad.

Esta práctica de laboratorio debe completarse fuera del laboratorio de Cisco, desde una computadora con acceso a Internet.

El tiempo estimado para completarla es de una hora.

Tarea 1: Ubicación de los Recursos SANS.

Paso 1: Abrir la Lista SANS de los 20 principales.

Con un navegador Web, vaya al URL http://www.sans.org. En el menú **Recursos**, elija **Lista de los 20 principales**, como se muestra en la Figura 1.

Figura 1. Menú SANS

La lista SANS de los 20 principales objetivos de ataques de seguridad en Internet está organizada por categorías. Una letra indica el tipo de categoría y los números separan los temas de la categoría. Los temas sobre router y switch se encuentran dentro de la categoría Dispositivos de red (Network Devices) **N**. Hay dos temas principales con hipervínculos:

N1. Servidores y teléfonos VoIP
N2. Debilidades comunes de configuración de dispositivos de red y de otro tipo

Paso 2: Hacer clic en el hipervínculo N2. Debilidades comunes de configuración de dispositivos de red y de otro tipo, para ingresar en este tema.

Tarea 2: Repaso sobre los Recursos SANS.

Paso 1: Repasar el contenido de N2.2 Temas comunes de configuración predeterminada.

Por ejemplo, N2.2.2 (en enero de 2007) contenía información sobre amenazas relacionadas con cuentas y valores predeterminados. Una búsqueda en Google sobre “contraseñas de router inalámbrico” arroja vínculos a diversos sitios que publican una lista de nombres de cuenta de administrador y contraseñas predeterminadas de routers inalámbricos. La imposibilidad de cambiar la contraseña predeterminada en estos dispositivos puede generar compromiso y vulnerabilidad hacia los atacantes.

Paso 2: Observar las referencias CVE.

La última línea debajo de varios temas se refiere a la Exposición común a la vulnerabilidad (CVE). El nombre CVE está relacionado con la Base de datos Nacional de Vulnerabilidad (NVD) del Instituto Nacional de Normas y Tecnología (NIST), patrocinado por la División de Seguridad Cibernética Nacional del Departamento de Seguridad Nacional (DHS) y por US-CERT, que contiene información sobre la vulnerabilidad.

Tarea 3: Recolección de datos.

El resto de esta práctica de laboratorio lo guiará a través de la investigación y solución de una vulnerabilidad.

Paso 1: Seleccionar un tema para investigar y hacer clic en un hipervínculo CVE de ejemplo.

Nota: Debido a que la lista CVE cambia, la lista actual puede no contener las mismas vulnerabilidades que en enero de 2007.

El vínculo debe abrir un nuevo explorador Web conectado a http://nvd.nist.gov/ y la página resumen de vulnerabilidades de CVE.

Paso 2: Completar la información sobre la vulnerabilidad:

Fecha de lanzamiento original: _____

Última revisión: _____

Fuente: _____

Descripción general:

_____

_____

_____

_____

_____

En Impacto hay varios valores. Se muestra la severidad del Sistema de puntaje de vulnerabilidades comunes (CVSS), que contiene un valor entre 1 y 10.

Paso 3: Completar la información sobre el impacto de vulnerabilidad:

Severidad CVSS: _____

Rango: _____

Autenticación: _____

Tipo de impacto: _____

El próximo encabezado contiene vínculos con información sobre la vulnerabilidad y las posibles soluciones.

Paso 4: Con la ayuda de los hipervínculos, escribir una breve descripción sobre la solución encontrada en esas páginas.

Tarea 4: Reflexión

La cantidad de vulnerabilidades para las computadoras, redes y datos sigue creciendo. Los gobiernos han dedicado importantes recursos para coordinar y difundir información sobre las vulnerabilidades y las posibles soluciones. Sigue siendo responsabilidad del usuario final la implementación de la solución. Piense de qué manera pueden los usuarios ayudar a fortalecer la seguridad. Piense qué hábitos de los usuarios crean riesgos en la seguridad.

Tarea 5: Desafío

Intente identificar una organización que se pueda reunir con nosotros para explicarnos cómo se rastrean las vulnerabilidades y se aplican las soluciones. Encontrar una organización dispuesta a hacer esto puede ser difícil, por razones de seguridad, pero ayudará a los estudiantes a aprender cómo se logra mitigar las vulnerabilidades en el mundo. También les dará a los representantes de las organizaciones la oportunidad de conocer a los estudiantes y realizar entrevistas informales.

Práctica de laboratorio 1.6.1: Uso de las herramientas de colaboración: IRC e IM

Diagrama de topología

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Definir Internet Relay Chat (IRC) y Mensajería instantánea (IM).
- Enumerar varios usos de colaboración de IM.
- Enumerar varios usos incorrectos y asuntos relacionados con la seguridad de datos que involucran la IM.
- Usar IRC para demostrar colaboración.

Información básica

Los correos electrónicos permiten que muchos usuarios colaboren, compartan ideas y transfieran archivos. Pero, a menos que el usuario controle permanentemente la cuenta de correo electrónico, los correos electrónicos no leídos pueden pasar inadvertidos durante un largo tiempo. El teléfono ha sido la tecnología elegida cuando las personas buscaban contacto inmediato. Desafortunadamente, no se puede usar el teléfono para transferir archivos. Lo que necesitan los colaboradores para la comunicación en la red humana es una herramienta con la flexibilidad del correo electrónico y la capacidad de respuesta del teléfono. Internet Relay Chat (IRC) y la Mensajería instantánea (IM) se ajustan bien a estos requisitos. A través de Internet o de una red corporativa privada, los usuarios pueden intercambiar fácilmente ideas y archivos. IMing y Chatting son dos métodos de comunicación en tiempo real, pero se implementan en forma diferente.

La Mensajería instantánea proporciona comunicación uno a uno entre individuos “aceptados”. Para iniciar un mensaje instantáneo, una persona debe “invitar” a otra. El receptor de la invitación debe conocer, y aceptar, la sesión IM en base al nombre de pantalla del otro usuario. El cliente IM le permite contar con una lista autorizada de usuarios, generalmente denominada Lista de contactos. Si desea comunicarse con más de una persona al mismo tiempo, puede abrir otras ventanas de IM. Cada una de esas ventanas representa una comunicación entre dos personas.

Internet Relay Chat, por otro lado, permite la interacción entre varias personas. También proporciona un grado de anonimato. Para iniciar una conversación, se establece una conexión a un servidor de chat y se une a un debate sobre un tema determinado. Cuando se une, se dice que se “agregó a una sala”. En la sala de chat, usted crea su propia identidad y puede proporcionar tan poca información sobre usted como desee.

A pesar de que el siguiente análisis se centra principalmente en IM, una breve práctica de laboratorio con nuestra “nube modelo de Internet” demostrará la facilidad de IRC.

IM necesita un dispositivo que proporciona servicios que permiten a los usuarios comunicarse. Este dispositivo se conoce como *Servidor de mensajes instantáneos*. Los usuarios de los dispositivos finales, como una computadora, usan un software denominado *Cliente de mensajes instantáneos*. Esta configuración se denomina relación cliente/servidor. Los clientes IM se conectan a un servidor IM y el servidor une a los clientes. Esta relación se denomina red IM. Hay muchas redes IM disponibles, cada una con usuarios dedicados. Entre las redes de IM conocidas se encuentran America On Line (AOL) Instant Messenger (AIM), Windows Live Messenger (MSN), Yahoo! Messenger e ICQ (I Seek You). La Figura 1 muestra la aplicación cliente AIM conectada a la red AIM.

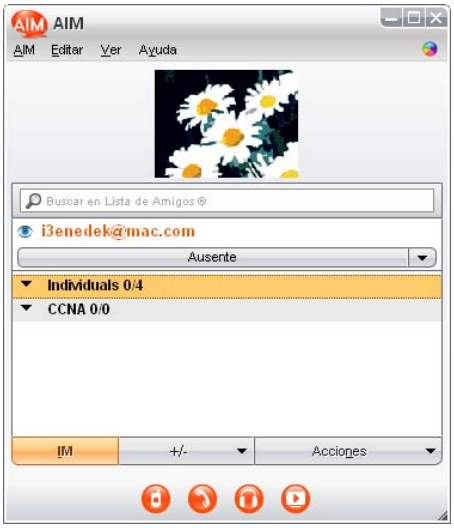


Figura 1. Cliente AIM

Características

Los servicios IM tienen muchas características comunes:

- Cuando un cliente IM se conecta a una red IM, cualquier conexión existente se puede alterar mediante una lista de contactos, una lista de otras personas con las cuales usted se comunica por medio del cliente IM.
- Compartir archivos entre clientes IM permite la colaboración en el trabajo.
- Es posible el envío de mensajes de texto entre clientes, y pueden ser registrados.
- Algunas redes IM ofrecen servicios de audio.
- Los servicios más nuevos que algunas redes IM están comenzando a proporcionar incluyen videoconferencias, Voz sobre IP (VoIP), conferencias Web, intercambio de escritorio e inclusive radio IP e IPTV.

Protocolos

Cada red IM usa un método de comunicación acordado que se denomina protocolo. Muchas de las redes IM usan protocolos propietarios. AIM e ICQ (adquirida por AOL) usan el protocolo propietario Open System for Communication in Realtime (OSCAR). Tanto Microsoft como Yahoo! tienen protocolos propietarios, pero se han asociado a otros servicios para lograr una conectividad conjunta.

A lo largo de este curso aprenderemos acerca de varios protocolos diferentes. El Grupo de trabajo de ingeniería de Internet (IETF) ha intentado estandarizar notablemente los protocolos IM con el Session Initialization Protocol (SIP). SIPv2 fue definido originalmente en RFC 2543 y fue dado por obsoleto por RFC 3261. Como con los protocolos IM propietarios, existe gran cantidad de protocolos de código abierto.

Algunas aplicaciones de cliente IM, como Gaim y Trillian, pueden diferenciar entre los diversos protocolos de red IM. Los servidores IM también pueden incorporar este soporte. El IETF formalizó un estándar abierto, Jabber, basado en el Extensible Messaging and Presence Protocol (EMPP). Las referencias correspondientes a IETF son RFC 3290 y RFC 3291. Admite comunicación encriptada.

El uso social indebido de IM ha sido una preocupación para padres, y muchas redes IM estimulan el control parental. Las restricciones para niños incluyen la limitación de contactos IM y la supervisión cuando están conectados. AIM y Yahoo! Messenger proporcionan herramientas de software gratuitas para supervisión. Algunas herramientas de supervisión incluyen registro de antecedentes, límites de tiempo de conexión, bloqueo de salas de chat, bloqueo de usuarios específicos e inhabilitación de determinadas funciones del cliente.

Seguridad

Se han identificado muchos problemas de seguridad con IM. Como resultado, muchas organizaciones limitan o bloquean completamente el ingreso de IM a la red corporativa. Se han transferido gusanos, virus y troyanos informáticos, categorizados como malware, a equipos cliente de IM. Sin métodos de alta seguridad, la información intercambiada entre los usuarios puede ser capturada y revelada. Los clientes y servidores IM han experimentado vulnerabilidades de aplicaciones, que a su vez afectaron la seguridad de los equipos. Incluso los usuarios legítimos pueden congestionar la velocidad de la red al transferir archivos grandes.

¿Cómo protege su red un administrador de sistemas contra vulnerabilidades y el uso indebido de IM? El instituto SANS (SysAdmin, Audit, Network, Security) recomienda varias medidas preventivas. La siguiente lista es del sitio Web de SANS, `http://www.sans.org/top20/#c4:`

C4.4 Cómo protegerse de vulnerabilidades y el uso no autorizado de IM

- Establecer políticas para el uso aceptable de IM. Asegurarse de que todos los usuarios sean conscientes de esas políticas y que comprendan claramente los posibles riesgos.
- Los usuarios estándar no deben estar autorizados a instalar software. Restringir los privilegios de nivel de usuario administrativo y avanzado al personal de soporte que actúa en calidad de ayuda. Si un usuario debe tener privilegios de nivel de usuario administrativo o avanzado, deberá crearse una cuenta separada para utilizar en sus funciones diarias de oficina, navegación de Internet y comunicaciones en línea.
- Asegurarse de que los parches del fabricante sean aplicados rápidamente al software IM, las aplicaciones interrelacionadas y el sistema operativo subyacente.
- Utilizar productos antivirus y antispyware.
- No confiar en servidores IM externos para el uso interno de IM; tener un servidor proxy IM o servidor interno IM de nivel comercial.
- Crear rutas de comunicación seguras cal utilizar IM con socios comerciales confiables.
- Configurar debidamente los sistemas de detección y prevención de intrusión. Comprender que muchas aplicaciones IM pueden permitir comunicaciones asociadas para hacerse pasar por tráfico legítimo (por ejemplo, http).
- Considerar la implementación de productos diseñados específicamente para la seguridad IM.
- Filtrar todo el tráfico http a través de un servidor proxy de autenticación para proporcionar capacidades adicionales de filtrado y monitoreo de tráfico IM.
- Bloquear el acceso a conocidos servidores públicos IM que no han sido autorizados explícitamente. (Nota: Esto sólo ofrece protección parcial debido a la cantidad de posibles servidores externos).
- Bloquear los puertos IM conocidos. (Nota: Esto sólo ofrece protección parcial debido a la cantidad de posibles protocolos y puertos asociados y a la capacidad de las aplicaciones de burlar las restricciones de puertos).
- Monitorear con un sistema de Detección / Prevención de intrusión para usuarios que crean túneles para IM o que burlan los servidores proxy.

El futuro de IM

El futuro de IM es prometedor, permitiendo a los usuarios adaptar nuevas tecnologías para la colaboración. Por ejemplo, IM móvil admite usuarios móviles, lo cual brinda servicios IM a los teléfonos celulares. Los fabricantes de teléfonos celulares más conocidos tienen su propia forma de IM móvil. Otro conocido aparato portátil es el Blackberry. El Blackberry admite herramientas IM comunes, como mensajería de texto, correo electrónico, telefonía y navegación Web.

Escenario

El diagrama de topología muestra dos equipos conectados a una “nube”. En networking, una nube generalmente se usa para simbolizar una red más compleja, como Internet, lo cual no es el centro de este análisis. En esta práctica de laboratorio usará dos equipos que primero deben obtener software de comunicación de la nube de red. Luego de instalar el software, la nube seguirá siendo necesaria para proporcionar servicios de comunicación. En capítulos subsiguientes, estudiará con más detalle los dispositivos y protocolos dentro de la nube. Dentro de la nube hay un servidor denominado *eagle-server*, como también otros dispositivos de networking. Esta práctica de laboratorio usa eagle-server como servidor IRC, y Gaim como cliente IRC. Gaim se usa para esta práctica de laboratorio, pero se podría usar cualquier cliente IRC que estuviera disponible. Hay un cliente IRC disponible para descargar de eagle-server, URL http://eagle-server.example.com/pub.

El tiempo de finalización estimado es de 45 minutos.

Tarea 1: Configuración del cliente de chat

El protocolo IRC es un estándar abierto, descrito originalmente en RFC 1495, que se comunica a través de enlaces de texto sin formato.

Paso 1: Verifique que el equipo del laboratorio cuente con un cliente IRC.

En caso contrario, descargue e instale gaim-1.5.0.exe (ejecutable para Windows) desde el URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter1`. Acepte la configuración predeterminada durante la instalación. Luego de verificar que se haya instalado el cliente de chat Gaim, realice los siguientes pasos para configurar Gaim.

Paso 2: Abra la ventana Cuentas.

1. Abra Gaim y seleccione la ventana Inicio de sesión, ícono **Cuentas**. En la Figura 2 se muestra la ventana Cuentas.

Figura 2. Ventana Cuentas de Gaim

2. En la ventana Cuentas, haga clic en **Agregar**.

Paso 2: Agregue una nueva cuenta.

1. Consulte la Figura 3. En la ventana Agregar cuenta, amplíe la opción “`Mostrar más opciones`”. Complete la información solicitada:

Protocolo: `IRC`

Nombre de pantalla: `(cómo lo verán otros)`
Servidor: `eagle-server.example.com`
Tipo de proxy: `Sin proxy`

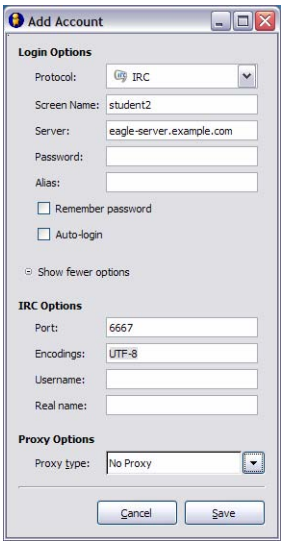


Figura 3. Ventana Agregar cuenta de Gaim

2. Cuando termine, haga clic en **Guardar**.
3. Cierre la ventana Cuentas.

Tarea 2: Conexión con el servidor de chat

Paso 1: Regístrese.

Vuelva a la ventana de Inicio de sesión, donde debe estar visible la nueva cuenta para eagle-server. Haga clic en **Registrarse**. Se abrirán dos ventanas. La Figura 4 muestra la ventana de estado de conexión de IRC. La Figura 5 muestra la ventana principal del cliente IM de Gaim, que se usa para chats o IM.

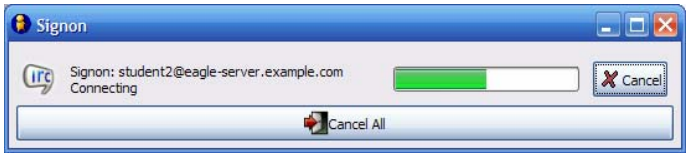


Figura 4. Ventana de estado de conexión de IRC

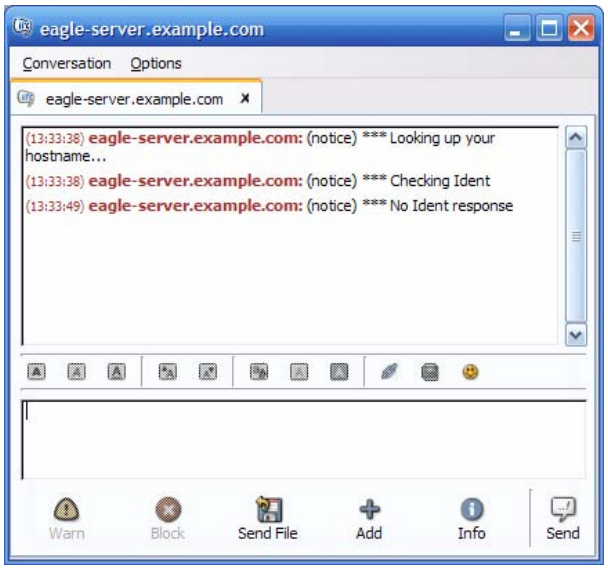


Figura 5. Ventana de cliente IRC de Gaim

Paso 2: Únase al chat.

Cuando el cliente IRC se conecta al servidor IRC, la ventana de estado se cierra y se muestra una ventana de Lista de contactos. Haga clic en **Chat**, como se muestra en la Figura 6.

Nota: Para unirse a un canal de chat, el nombre del canal *debe* comenzar con #. Si el nombre del canal es incorrecto, usted estará solo en una sala de chat (salvo que otro estudiante cometa el mismo error).

Figura 6. Cómo unirse a un chat

Tarea 3: La sesión de chat

La Figura 7 muestra un breve chat entre usuarios *Root* y *student2*. Varios estudiantes pueden unirse e interactuar entre ellos.

Figura 7. Participación en un chat

Durante el chat, piense cómo administraría usted, como padre o administrador de red, este tipo de conexión.

Tarea 4: Reflexión

En una red con conexión a Internet, se puede usar el cliente IM Gaim para conectarse con varios proveedores IM diferentes. La mayoría de los adolescentes y jóvenes adultos actualmente están familiarizados con IMing con amigos y la transferencia de archivos, pero la comunicación entre el cliente y el servidor puede no ser comprendida. Como futuro ingeniero de redes, usted debe comprender los problemas sociales y de seguridad con IM e IRC.

Tarea 5: Desafío

Mientras esté conectado al chat, transfiera archivos entre compañeros. Use un ping continuo desde el host hacia el eagle server para monitorear el rendimiento de la red. Observe el tiempo de respuesta antes y durante la transferencia de archivos. Escriba una breve descripción del tiempo de respuesta de la red durante las transferencias de archivos y sin transferencias.

_____

_____

_____

_____

_____

Tarea 6: Limpieza

Consulte con el instructor antes de eliminar Gaim y de apagar el equipo.

Práctica de laboratorio 1.6.2: Uso de las herramientas de colaboración: Wikis y weblogs

Diagrama de topología

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Definir los términos *wiki* y *blog.*
- Explorar las características de wiki.

Información básica

La topología de la práctica de laboratorio debe estar configurada y lista para su uso. Si existen problemas de conectividad con el equipo del laboratorio al conectarse con Eagle Server, pida ayuda al instructor.

El diagrama de topología muestra dos equipos conectados a una “nube”. En networking, una nube generalmente se usa para simbolizar una red más compleja, lo cual no es el centro de este análisis. En esta práctica de laboratorio se utilizará un equipo host que se conecta a través de la nube para acceder a Twiki. En capítulos subsiguientes, estudiará con más detalle los dispositivos y protocolos dentro de la nube.

Escenario

En esta práctica de laboratorio, tendrá la oportunidad de aprender acerca de las diferentes partes de una wiki. Si alguna vez utilizó *Wikipedia*, probablemente ya está familiarizado con el aspecto general de una wiki. Después de utilizar *Wikipedia*, con sus contenidos ricos y enlaces flexibles, volver a los archivos planos puede ser limitante e insatisfactorio.

Se explorará el servidor wiki TWiki instalado en Eagle Server para obtener experiencia con una wiki.

Tarea 1: Definir los términos wiki y blog.

Wikis
"Wiki" es una palabra del idioma hawaiano que significa *rápido.* En términos de networking, una wiki es una herramienta de colaboración basada en la Web que permite a casi todas las personas publicar información, archivos o gráficos a un sitio común para que otros usuarios lean y modifiquen. Una wiki permite a una persona acceder a una página de inicio (primera página) que provee una herramienta de búsqueda para ayudarlo a localizar artículos de su interés. Puede instalarse una wiki para la comunidad de Internet o detrás de un firewall corporativo para uso de los empleados. El usuario no sólo lee contenidos wiki sino que también participa en la creación de contenidos dentro de un navegador Web.

A pesar de que están disponibles diferentes servidores wiki, las siguientes características comunes se formalizaron en cada wiki:

- Se puede utilizar cualquier navegador Web para editar páginas o crear nuevos contenidos.
- Los enlaces edit y auto están disponibles para editar una página y automáticamente enlazar páginas. El formateo de texto es similar a la creación de un correo electrónico.
- Se utiliza un motor de búsqueda para la ubicación rápida de contenidos.
- Se puede configurar el control de acceso mediante el creador de temas que define quién está autorizado a editar el contenido.
- Una Web wiki es un grupo de páginas con diferentes grupos de colaboración.

Para obtener más información sobre Wiki, visite los siguientes URL fuera del horario de clase:

http://www.wiki.org/wiki.cgi?WhatsWiki
http://www.wikispaces.com/

Blogs

Un weblog, llamado blog, es similar a una wiki porque los usuarios crean y envían contenidos para que otros los lean. Los blogs generalmente son creación de una sola persona y el propietario del blog es quien controla los contenidos del blog. Algunos blogs permiten a los usuarios dejar comentarios y responderle al autor, mientras que otros son más restrictivos. Hay hostings gratis para blogs similares a los sitios Web o a las cuentas de correo electrónico gratuitas. Uno de ellos es www.blogger.com.

Tarea 2: Explorar las características de Wiki con el tutorial Twiki.

El tutorial Twiki consiste en explorar algunas de las características más comunes de una wiki. En la siguiente lista aparecen los temas más importantes que se tratan en el tutorial:

Tutorial Twiki de 20 minutos
1. Prepárese…
2. Dé un paseo rápido...
3. Abra una cuenta privada...
4. Observe los usuarios y grupos Twiki.
5. Pruebe los controles de la página…
6. Modifique una página y cree una nueva…
7. Utilice el navegador para subir archivos como adjuntos de páginas...
8. Reciba alertas de correo electrónico cada vez que las páginas cambien...

Debido a que cada tema del tutorial se investiga, complete las preguntas en esta tarea. La excepción es "3. Abra una cuenta privada...". Twiki requiere una verificación de correo electrónico para las cuentas

nuevas y el correo electrónico no se configuró en los equipos host del laboratorio. En cambio, ya se crearon usuarios para los pasos que requieren privilegios de inicio de sesión.

La potencia de una wiki está en el contenido rico del hipervínculo. Seguir hipervínculos puede causar problemas de continuidad. Se recomienda abrir dos navegadores. Señale un navegador en el URL de Twiki y utilice el otro navegador para páginas “de trabajo”. Ajuste el tamaño de la ventana del navegador para que se puedan ver las instrucciones en uno de los navegadores mientras se realizan las acciones en el otro. Cualquier enlace externo que se seleccione generará un error.

Paso 1: Establezca una conexión de cliente Web con wiki Eagle Server.

Abra un navegador Web y conéctese a TWiki Sabdbox, URL http://eagle-server.example.com/twiki/bin/view/Sandbox/WebHome. El nombre URL distingue mayúsculas de minúsculas y se debe escribir exactamente como se muestra. La Sandbox es un tema Web diseñado para probar las características wiki. Consulte la Figura 1.

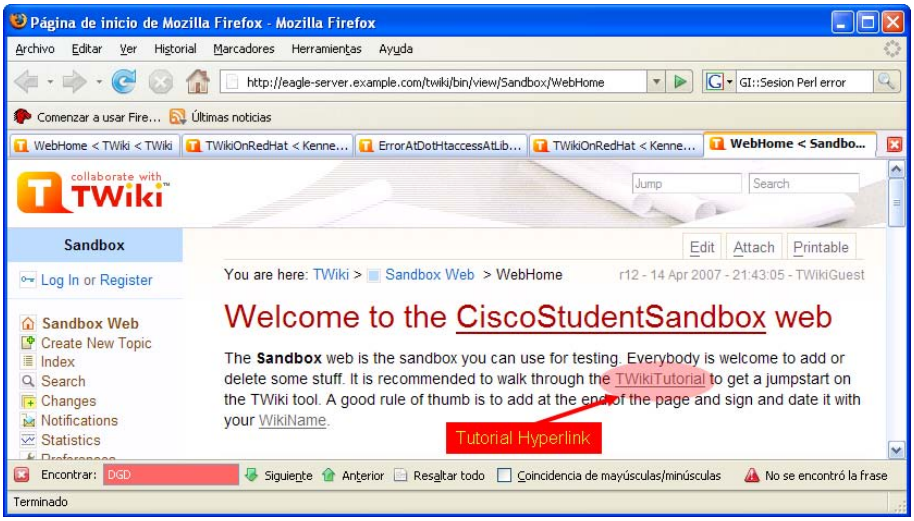


Figura 1. Sitio Web TWiki Sandbox.

Paso 2: Abra el tutorial Twiki.

Haga clic en el enlace del tutorial Twiki resaltado en el óvalo rojo de la Figura 1, para abrir la página del tutorial wiki.

Paso 3: Complete el tutorial wiki.

Consulte el paso 1 del tutorial, “`Prepárese...`”, y el paso 2, “`Dé un paseo rápido...`”. Después de completar las dos primeras secciones del tutorial, responda las siguientes preguntas:

¿Qué es una Wikiword?

_____
_____
_____

¿Cuántos son los resultados de una búsqueda con Websearch? _____

Consulte el paso 3 del tutorial, "`Abra una cuenta privada...`" El correo electrónico no está disponible en este momento, por lo tanto no podrá registrarse. En cambio, se crearon ID de usuario para utilizar más adelante en esta práctica de laboratorio.

El punto clave que hay que entender en este paso es que el registro es un proceso que consta de dos partes. Primero, los usuarios completan la información de registro y envían el formulario a TWiki.

Haga una lista de la información obligatoria necesaria para el registro:

_____
_____
_____
_____
_____
_____
_____

Twiki responde a una solicitud de registro mediante el envío de un correo electrónico al usuario, que contiene un código de activación único.

La segunda parte del proceso de registro es cuando el usuario (1) ingresa el código en la ventana de activación o (2) responde con un correo electrónico al hacer clic en el enlace de respuesta de Twiki. En este momento, la cuenta del usuario se agrega a la base de datos de Twiki.

Consulte el paso 4 del tutorial, "`Observe los usuarios y grupos Twiki...`" Se muestra una lista de usuarios y grupos Twiki. Después de completar esta sección del tutorial, responda las siguientes preguntas relacionadas con problemas de usuarios y grupos:

¿Cómo se restablece una contraseña de usuario?

_____
_____
_____

¿Cómo se pueden solucionar modificaciones incorrectas en un tema wiki?

_____

El paso 5 del Tutorial, "`Pruebe los controles de la página...`", lo familiarizará con los comandos de edición de la página. Después de completar esta sección del tutorial, responda las siguientes preguntas:

¿Cuál es el último número de revisión?

_____

Ubique el enlace de acción correcto al lado de la descripción para los controles de página:
Adjuntar Enlaces recibidos Editar Historial Más Imprimible r3 > r2 > r1 Vista sin modificaciones

Descripción	Enlace de acción
agregar a o editar tema	
mostrar el texto de origen sin la edición del tema	
adjuntar archivos a un tema	

Descripción	Enlace de acción
descubrir qué otros temas tienen un enlace a este tema (enlace inverso)	
controles adicionales, como renombrar / mover, control de versión y configuración del titular del tema.	
los temas están en control de revisión; muestra el historial de cambio completo del tema. Por ejemplo: quién cambió qué y cuándo.	
ver una versión anterior del tema o la diferencia entre las dos versiones.	
ir a una versión desmontada de la página, que se pueda imprimir	

El paso 6 del tutorial "`Cambiar una página y crear una nueva...`" es una oportunidad para agregar contenido a la wiki. Complete este tutorial utilizando la siguiente tabla para iniciar sesión en el servidor wiki.

Se ha creado un grupo con cuentas privadas en Eagle Server para permitir la participación en un tema Twiki privado. Estas cuentas van de **StudentCcna1** a **StudentCcna22**. Todas las cuentas tienen la misma contraseña: **`cisco`**. El usuario debe utilizar la cuenta que refleje el número de equipo host y módulo. Consulte la siguiente tabla:

N.º de pod/host de práctica de laboratorio	ID de inicio de sesión de la cuenta (distingue minúsculas de minúsculas)
Pod1host1	**`StudentCcna1`**
Pod1host2	**`StudentCcna2`**
Pod2host1	**`StudentCcna3`**
Pod2host2	**`StudentCcna4`**
Pod3host1	**`StudentCcna5`**
Pod3host2	**`StudentCcna6`**
Pod4host1	**`StudentCcna7`**
Pod4host2	**`StudentCcna8`**
Pod5host1	**`StudentCcna9`**
Pod5host2	**`StudentCcna10`**
Pod6host1	**`StudentCcna11`**
Pod6host2	**`StudentCcna12`**
Pod7host1	**`StudentCcna13`**
Pod7host2	**`StudentCcna14`**
Pod8host1	**`StudentCcna15`**
Pod8host2	**`StudentCcna16`**
Pod9host1	**`StudentCcna17`**
Pod9host2	**`StudentCcna18`**
Pod10host1	**`StudentCcna19`**
Pod10host2	**`StudentCcna20`**
Pod11host1	**`StudentCcna21`**
Pod11host2	**`StudentCcna22`**

Desde la pantalla de Bienvenida de wiki de la práctica de laboratorio, haga clic en el enlace **Iniciar sesión** en la esquina superior izquierda de la página. Vea la Figura 2.

Figura 2. Enlace Iniciar sesión.

Aparecerá un cuadro de inicio de sesión similar a la que se muestra en la Figura 3. Ingrese el nombre de usuario válido Twiki y la contraseña **`cisco`.** Tanto el nombre de usuario como la contraseña distinguen mayúsculas de minúsculas.

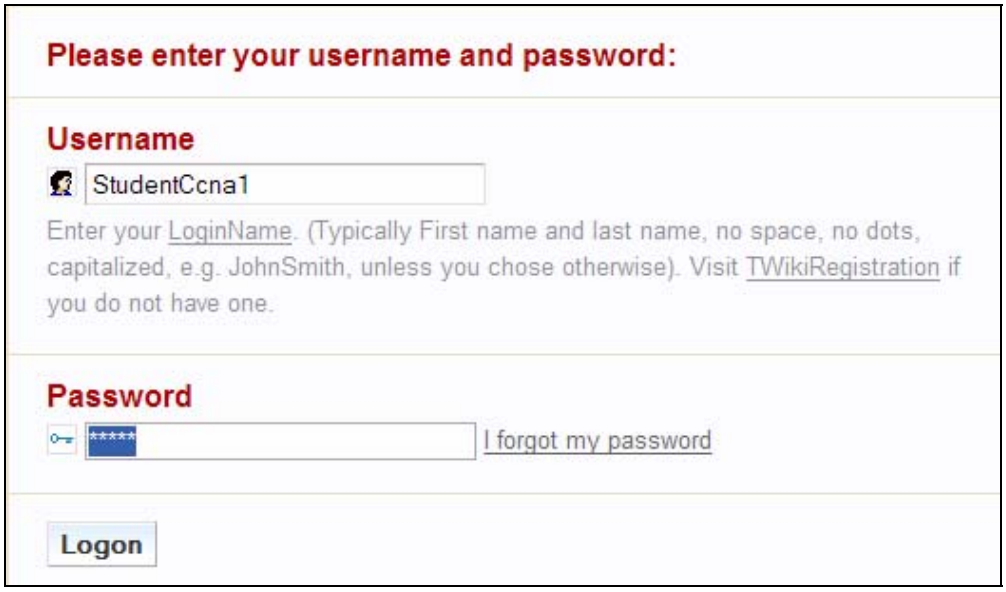


Figura 3. Cuadro de Inicio de sesión.

Esto debe mostrar su página de tema wiki similar a la que se muestra en la Figura 4.

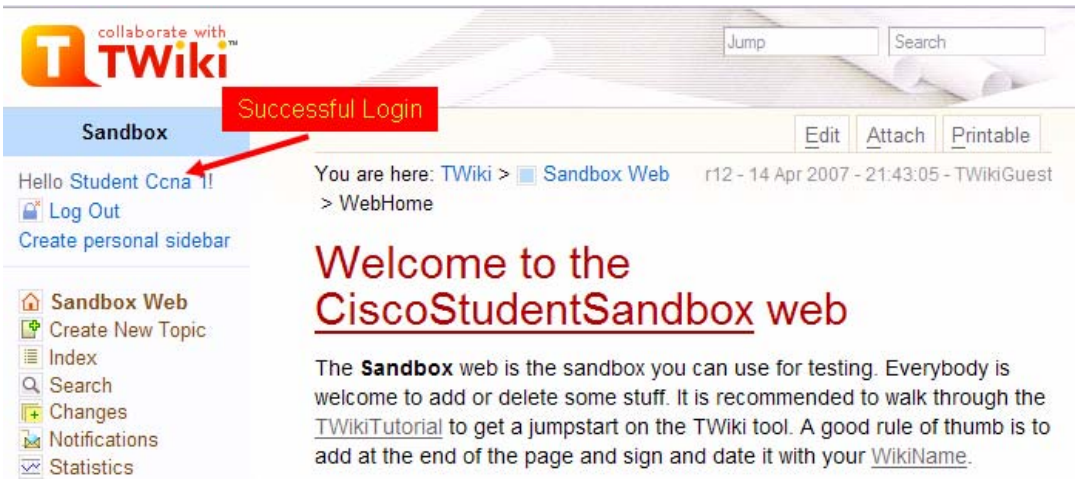


Figura 4. Página de tema wiki.

El paso 7 del Tutorial, "`Utilice el navegador para subir archivos como adjuntos de páginas...`", describe el proceso para cargar archivos en la wiki. Para completar este tutorial, cree un documento utilizando el bloc de notas y cárguelo al servidor wiki.

¿Cuál el tamaño máximo de archivo predeterminado que se puede transferir? ___10 MB_____

El paso 8 del Tutorial, "`Reciba alertas de correo electrónico cada vez que las páginas cambien...`", detalla cómo recibir alertas de correo electrónico cada vez que una página específica fue actualizada. A veces no es conveniente regresar regularmente a una wiki nada más que para verificar actualizaciones. Debido a que el correo electrónico no está configurado en el equipo host, no se enviarán las alertas.

Describa cómo puede recibir notificaciones por correo electrónico cada vez que cambia un tema.

_____

_____

_____

Tarea 3: Reflexión

En esta práctica de laboratorio se presentaron los mecanismos de una wiki. El usuario no se dará cuenta de la utilidad y la colaboración de éstos hasta que realmente participe en una wiki. Las wikis que podrían interesarle son:

- CCNA – http://en.wikibooks.org/wiki/CCNA_Certification
- Historial de sistemas Cisco – http://en.wikipedia.org/wiki/Cisco_Systems
- Web Wiki acerca del equipamiento y tecnología Cisco – http://www.nyetwork.org/wiki/Cisco
- Red+ – http://en.wikibooks.org/wiki/Network_Plus_Certification/Study_Guide
- Diccionario de la red – http://wiki.networkdictionary.com/index.php/Main_Page
- Analizador del protocolo de red Wireshark – http://wiki.wireshark.org/

Tarea 4: Desafío

Según el tipo de instalación de Eagle Server, la clase podría utilizar el servidor wiki Twiki para publicar temas interesantes relacionados a la teoría de red de equipos y el progreso de la clase.

Cree un blog personal de su experiencia educacional con la red. Necesitará acceso a Internet.

Tarea 5: Limpieza

Cierre todos los navegadores Web y apague el equipo a menos que se le indique lo contrario.

1.7.1: Desafío de integración de habilidades: Introducción a Packet Tracer

Diagrama de topología

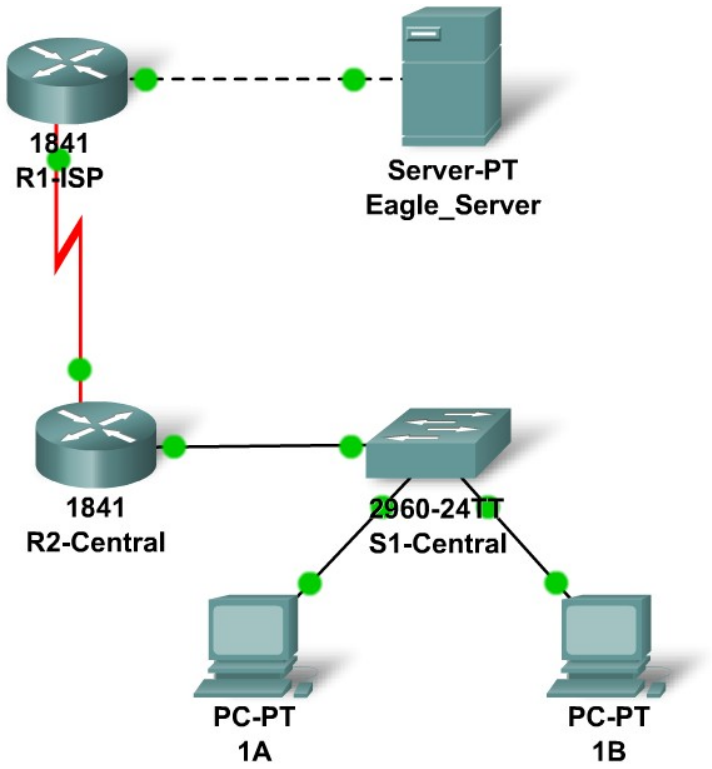


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Explorar el modo de tiempo real del Packet Tracer
- Explorar el área lógica de trabajo
- Explorar la operación del Packet Tracer
- Conectar dispositivos
- Examinar la configuración de un dispositivo
- Repasar la configuración estándar del laboratorio
- Obtener una visión general de los dispositivos

Información básica

A lo largo del curso, utilizará una configuración de laboratorio estándar creada a partir de PC, servidores, routers y switches reales para aprender los conceptos sobre redes. El método proporciona la gama más amplia de funciones y la experiencia más realista. Debido a que el equipo y el tiempo son limitados, esta experiencia puede complementarse con un ambiente simulado. El simulador que se usa en este curso es el Packet Tracer. El Packet Tracer ofrece un grupo rico de protocolos, equipos y funciones, pero sólo una fracción de lo que es posible con un equipo real. El Packet Tracer es un suplemento, no un reemplazo de la experiencia con un equipo real. Se lo invita a comparar los resultados obtenidos con los modelos de red del Packet Tracer con el comportamiento del equipo real. También se lo invita a examinar los archivos de Ayuda integrados en el Packet Tracer, que incluyen un extenso “Mi primer laboratorio de Packet Tracer”, tutoriales e información sobre las fortalezas y limitaciones al usar el Packet Tracer para los modelos de red.

Esta actividad le brindará una oportunidad para explorar la configuración de laboratorio estándar usando el simulador del Packet Tracer. El Packet Tracer posee dos formatos de archivo que puede crear: archivos .pkt (archivos modelos de simulación de red) y archivos .pka (archivos de actividad para práctica). Cuando cree sus propias redes en el Packet Tracer o modifique los archivos existentes de su instructor o de sus pares, generalmente usará el formato de archivo .pkt. Cuando inició esta actividad del plan de estudios, aparecieron estas instrucciones. Son el resultado del .pka, el formato de archivo de actividad del Packet Tracer. En la parte inferior de estas instrucciones hay dos botones: Verificar resultados (que le indica qué porcentaje de la actividad ha realizado) y Restablecer actividad (que inicia la actividad nuevamente, si quiere borrar su trabajo o adquirir más experiencia).

Tarea 1: Explorar la interfaz del Packet Tracer (PT).

Paso 1: Examinar el área lógica de trabajo.

Cuando se inicia el Packet Tracer, éste presenta una vista lógica de la red en el modo de tiempo real. La parte principal de la interfaz del PT es el **Área lógica de trabajo.** Ésta es el área principal donde se colocan y conectan los dispositivos.

Paso 2: Recorrido por los símbolos.

La porción inferior izquierda de la interfaz del PT, debajo de la barra amarilla, es la porción de la interfaz que se usa para seleccionar y ubicar los dispositivos en el área de trabajo lógica. El primer cuadro en la parte inferior, a la izquierda, contiene símbolos que representan grupos de dispositivos. Cuando mueve el puntero del mouse sobre estos símbolos, aparece el nombre del grupo en el cuadro de texto del centro. Cuando usted hace clic en uno de esto símbolos, aparecen los dispositivos específicos del grupo en el cuadro de la derecha. Cuando señala los dispositivos específicos, aparece una descripción del dispositivo en el cuadro de texto que se encuentra debajo de los dispositivos específicos. Haga clic en cada uno de los grupos y estudie los distintos dispositivos que se encuentran disponibles y sus símbolos.

Tarea 2: Exploración de las operaciones del PT

Paso 1: Conectar los dispositivos con la opción conexión automática.

Haga clic en el símbolo de conexiones del grupo. Los símbolos de conexión específicos proporcionan distintos tipos de cables que pueden usarse para conectar los dispositivos. El primer tipo específico, el rayo dorado, selecciona automáticamente el tipo de conexión que se basa en las interfaces disponibles en los dispositivos. Cuando hace clic en el símbolo, el puntero se asemeja a un conector de cable.
Para conectar dos dispositivos haga clic en el símbolo de conexión automática, haga clic en el primer dispositivo y luego en el segundo dispositivo. Con el símbolo de conexión automática, haga la siguiente conexión:

- Conecte el Eagle Server al router R1-ISP.
- Conecte la PC-PT 1A al switch S1-Central.

Paso 2: Examinar la configuración del dispositivo con el mouse.

Pase el cursor del mouse sobre los dispositivos que se encuentran en el área lógica de trabajo. A medida que mueve el puntero del mouse sobre estos símbolos, aparecen las configuraciones de los dispositivos en un cuadro de texto.

- Un **router** muestra la información de configuración del puerto, incluida la dirección IP, el estado del puerto y la dirección MAC.
- Un **servidor** muestra la dirección IP, la dirección MAC y la información del gateway.
- Un **switch** muestra la información de configuración del puerto, incluida la dirección IP, el estado del puerto y la membresía de VLAN.
- Una **PC** muestra la dirección IP, la dirección MAC y la información del gateway.

Paso 3: Examinar la configuración del dispositivo.

Haga clic con el botón izquierdo del mouse en cada tipo de dispositivo que se encuentre en el área lógica de trabajo para observar la configuración.

- **Los dispositivos como el router y el switch** contienen tres fichas. Estas fichas son: Física, Configuración y CLI (Interfaz de la línea de comando).
  - La ficha Física muestra los componentes físicos del dispositivo, como los módulos. Con esta ficha, también se pueden agregar nuevos módulos.
  - La ficha Configuración muestra la información de configuración general, como por ejemplo el nombre del dispositivo.
  - La ficha CLI permite al usuario configurar el dispositivo con una interfaz de línea de comando.
- **Los dispositivos como el servidor y el hub** contienen dos fichas. Estas fichas son Física y Configuración.
  - La ficha Física muestra los componentes del dispositivo, como por ejemplo los puertos. Con esta ficha, también se pueden agregar nuevos módulos.
  - La ficha Configuración muestra la información general, como por ejemplo el nombre del dispositivo.
- **Los dispositivos de PC** contienen tres fichas. Estas fichas son Física, Configuración y Escritorio.
  - La ficha Física muestra los componentes del dispositivo. Con esta ficha, también se pueden agregar nuevos módulos.
  - La ficha Configuración muestra el nombre del dispositivo, la dirección IP, la máscara de subred, el DNS y la información del gateway.
  - La ficha Escritorio permite al usuario configurar la dirección IP, la máscara de subred, el gateway por defecto, el servidor DNS, dial-up e inalámbrico. Con la ficha Escritorio también se puede acceder a un emulador de terminal, a la petición de entrada de comandos y a un navegador Web simulado.

Tarea 3: Repaso de la configuración estándar del laboratorio.

Paso 1: Obtener una visión general de los dispositivos.

La configuración estándar de laboratorio consistirá de dos routers, un switch, un servidor y dos PC. Cada uno de estos dispositivos está preconfigurado con información, como nombres de dispositivos, direcciones IP, gateways y conexiones.

Reflexión:

Se lo invita a solicitarle a su instructor el Packet Tracer y a completar Mi primer laboratorio de Packet Tracer.

Actividad 2.2.5: Uso de NeoTrace™ para ver Internetworks

Objetivos de aprendizaje

- Explicar el uso de programas de rastreo de rutas, como tracert y NeoTrace.
- Usar tracert y NeoTrace para rastrear una ruta desde la PC hasta un servidor remoto.
- Describir la naturaleza interconectada y global de Internet respecto del flujo de datos.

Información básica

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

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

`traceroute` `<destination network name or end device address>`

(Unix y sistemas similares)

o

`tracert` `<destination network name or end device address>`

(sistemas MS Windows)

y determina la ruta que tomaron los paquetes a través de una red IP.

La herramienta **`traceroute`** (o **`tracert`**) se usa generalmente para resolver problemas de redes. Al mostrar una lista de los routers atravesados, permite al usuario identificar la ruta tomada para llegar a un destino determinado de la red o a través de internetworks. Cada router representa un punto donde una red se conecta con otra y por donde se envió el paquete. La cantidad de routers se conoce como la cantidad de “saltos” que viajaron los datos desde el origen hasta el destino.

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

De todos modos, hay que tener en cuenta que, debido a la naturaleza “de malla” de las redes interconectadas que forman Internet y a la capacidad del Protocolo de Internet para seleccionar diferentes rutas sobre las cuales enviar los paquetes, dos rutas de rastreo entre el mismo origen y destino realizadas con una diferencia de tiempo pueden producir resultados diferentes.

Este tipo de herramientas generalmente está incluido en el sistema operativo del dispositivo final.

Otras, como NeoTrace™, son programas patentados que proporcionan información adicional. NeoTrace, por ejemplo, usa información en línea disponible para mostrar gráficamente la ruta rastreada en un mapa global.

Escenario

Con una conexión a Internet, usará dos programas de rastreo de enrutamiento para examinar la ruta de Internet hacia las redes de destino.

Esta actividad debe realizarse en una computadora que tenga acceso a Internet y acceso a una línea de comando. Primero se utilizará la utilidad **tracert** incorporada en Windows y luego el programa NeoTrace con mejoras adicionales. Esta práctica de laboratorio incluye la instalación de NeoTrace.

Tarea 1: Rastreo de ruta hacia el servidor remoto.

Paso 1: Rastrear la ruta hacia una red remota.

Para rastrear la ruta hacia la red remota, la PC que se use debe tener una conexión con la red de la clase o laboratorio.

1. En la petición de entrada de línea de comandos, escriba: **`tracert www.cisco.com`**

   La primera línea de resultado debe mostrar el Nombre de dominio plenamente calificado (FQDN), seguido de la dirección IP. El Servicio de nombres de dominios (DNS) del servidor del laboratorio pudo resolver el nombre en una dirección IP. Sin esta resolución de nombre, **`tracert`** habría fallado porque esta herramienta funciona en las capas TCP/IP que solamente interpretan direcciones IP válidas.

   Si DNS no se encuentra disponible, la dirección IP del dispositivo de destino debe ser ingresada luego del comando **`tracert`**, en lugar del nombre del servidor.

2. Examine el resultado mostrado.

   ¿Cuántos saltos hay entre el origen y el destino? _____

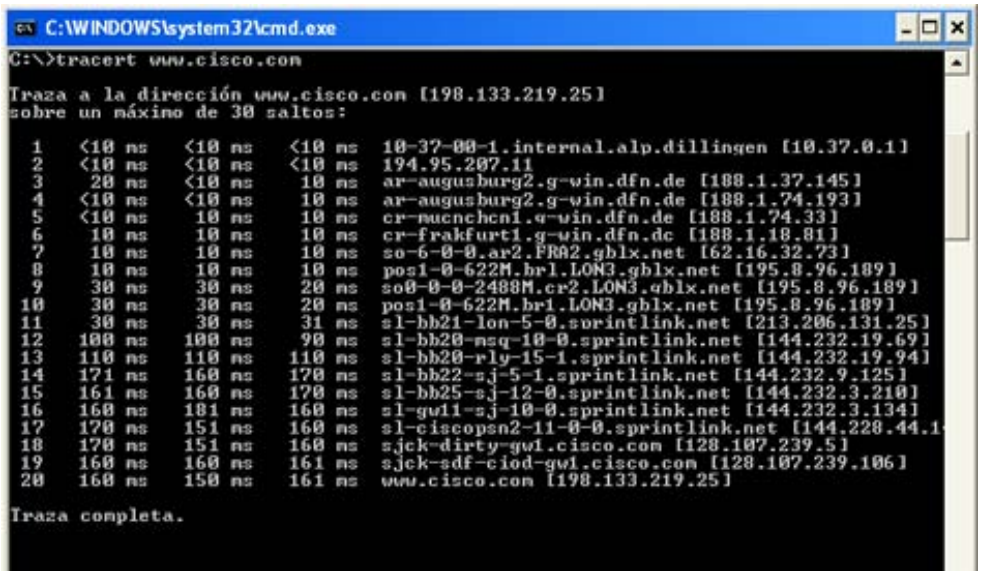


Figura 1. Comando `tracert`

La Figura 1 muestra el resultado exitoso luego de ejecutar:

`tracert www.cisco.com`

desde una ubicación en Baviera, Alemania.

La primera línea de resultado muestra FQDN seguido de la dirección IP. Por lo tanto, un servidor DNS pudo resolver el nombre a una dirección IP. Hay listas de todos los routers que las peticiones **`tracert`** deben atravesar para llegar a destino.

3. Intente el mismo rastreo de ruta desde una PC conectada a Internet y vea el resultado.

   Cantidad de saltos hasta www.cisco.com: _____

Paso 2: Intentar con otro rastreo de ruta en la misma PC y examinar el resultado.

URL de destino: _____

Dirección IP destino: _____

Tarea 2: Rastreo de ruta con NeoTrace.

1. Ejecute el programa NeoTrace.
2. En el menú **Ver**, seleccione **Opciones**. Haga clic en la ficha **Mapa** y, en la sección **Ubicación local**, haga clic en el botón **Establecer ubicación local**.
3. Siga las instrucciones para seleccionar el país y la ubicación en el país. Alternativamente, puede hacer clic en el botón **Avanzado**, que le permite ingresar la latitud y longitud exactas de su ubicación. Consulte la sección Desafío de la Actividad 1.2.5(1).
4. Ingrese “www.cisco.com” en el campo **Destino** y haga clic en **Ir**.
5. Desde el menú **Ver**, **Ver lista** muestra la lista de routers, similar a **`tracert.`**

   Ver nodo del menú **Ver** muestra gráficamente las conexiones, con símbolos.

   Ver mapa del menú **Ver** muestra los vínculos y los routers en su ubicación geográfica en un mapa global.
6. Seleccione una vista por vez y observe las diferencias y similitudes.
7. Pruebe una cantidad diferente de URL y vea las rutas hacia esos destinos.

Tarea 3: Reflexión

Repasar el objetivo y la utilidad de los programas de rastreo de rutas.

Relacione los resultados de NeoTrace con el concepto de redes interconectadas y de la naturaleza global de Internet.

Tarea 4: Desafío

Considere y analice posibles temas de seguridad de redes que puedan surgir a partir del uso de programas como traceroute y Neotrace. Considere qué detalles técnicos son revelados y cómo tal vez esta información puede ser usada incorrectamente.

Tarea 5: Limpieza

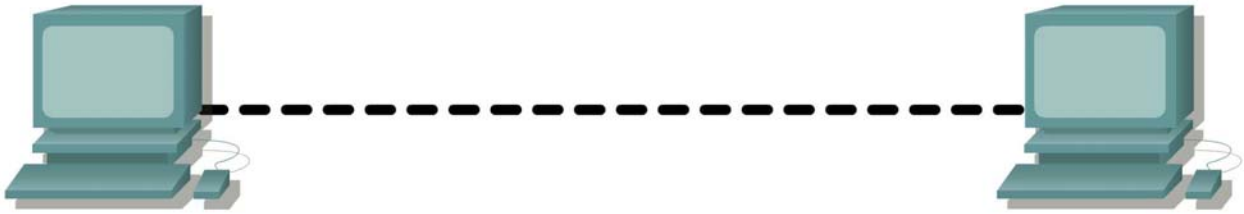
Salga del programa NeoTrace.

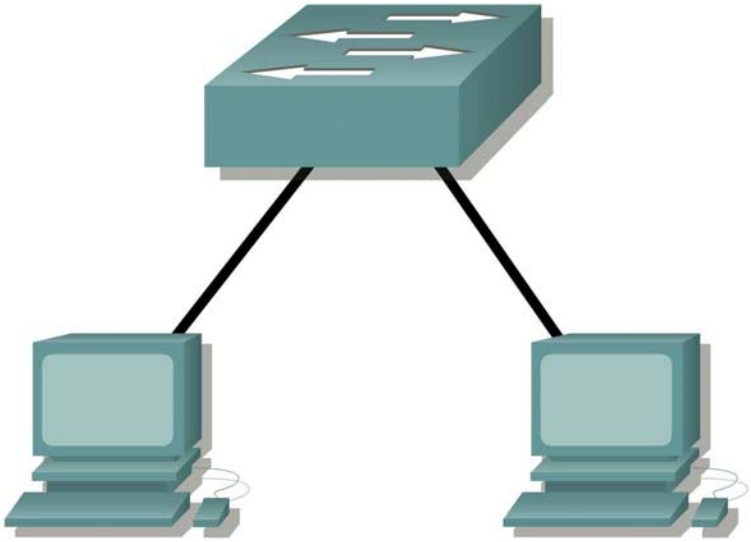
A menos que el instructor indique lo contrario, apague la computadora como corresponde.

Práctica de laboratorio 2.6.1: Orientación de topología y construcción de una red pequeña

Diagrama de topología

Red punto a punto





Redes conmutadas

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Identificar correctamente los cables que se utilizan en la red.
- Cablear físicamente una red conmutada punto a punto.
- Verificar la conectividad básica en cada red.

Información básica

Varios de los problemas de red se pueden solucionar en la capa Física de una red. Por esta razón, es importante saber exactamente cuáles son los cables que se utilizan para las conexiones de red.

En la capa Física (Capa 1) del modelo OSI, los dispositivos finales se deben conectar por medios (cables). Los tipos de medios requeridos dependen de los tipos de dispositivos que se conecten.

En la porción básica de esta práctica de laboratorio se utilizarán cables de conexión directa o patch cables para conectar estaciones de trabajo y switches.

Además, dos o más dispositivos se comunican a través de una dirección. La capa de Red (Capa 3) requiere una dirección única (que se conoce también como una dirección lógica o Direcciones IP), que permite que los datos alcancen el dispositivo destino correcto.

En esta práctica de laboratorio se aplicará el direccionamiento a las estaciones de trabajo y se utilizará para permitir la comunicación entre los dispositivos.

Escenario

Esta práctica de laboratorio comienza con la conexión de red más simple (punto a punto) y finaliza con la práctica de conexión a través de un switch.

Tarea 1: Creación de una red punto a punto.

Paso 1: Seleccione un compañero de laboratorio.

Paso 2: Obtenga el equipo y los recursos para la práctica de laboratorio.

Equipo necesario:

- 2 estaciones de trabajo
- 2 cables de conexión directa (patch).
- 1 cable de conexión cruzada
- 1 switch (o hub)

Tarea 2: Identificar los cables que se utilizan en una red.

Antes de que los dispositivos puedan conectarse, se necesitará identificar los tipos de medios que se utilizarán. Los cables que se utilizarán en esta práctica de laboratorio son de conexión cruzada y de conexión directa.

Utilice un **cable de conexión** cruzada para conectar dos estaciones de trabajo entre sí a través de los puertos Ethernet de su NIC. Éste es un cable Ethernet. Cuando mire el conector notará que los cables naranja y verde están en posiciones opuestas al final de cada cable.

Utilice un **cable de conexión directa** para conectar el puerto Ethernet del router a un puerto del switch o una estación de trabajo a un puerto del switch. Éste, también, es un cable Ethernet. Cuando mire el conector notará que ambos extremos del cable son exactamente iguales en cada posición del pin.

Tarea 3: Conectar una red punto a punto.

Paso 1: Conecte dos estaciones de trabajo.

Con el cable Ethernet correcto, conecte dos estaciones de trabajo. Conecte un extremo del cable al puerto de la NIC en la PC1 y el otro extremo del cable a la PC2.

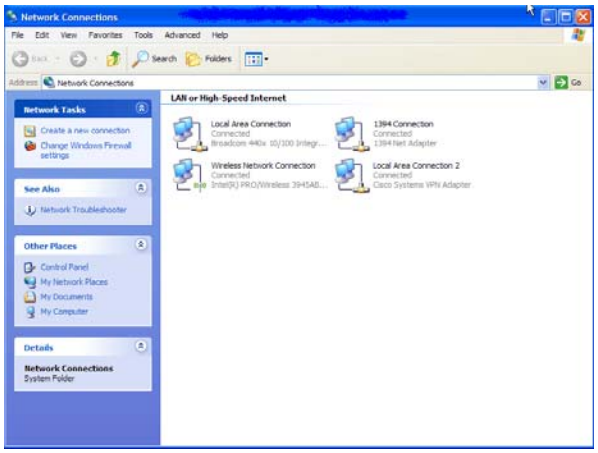
¿Qué cable usó? _____

Paso 2: Aplique una dirección de Capa 3 a las estaciones de trabajo.

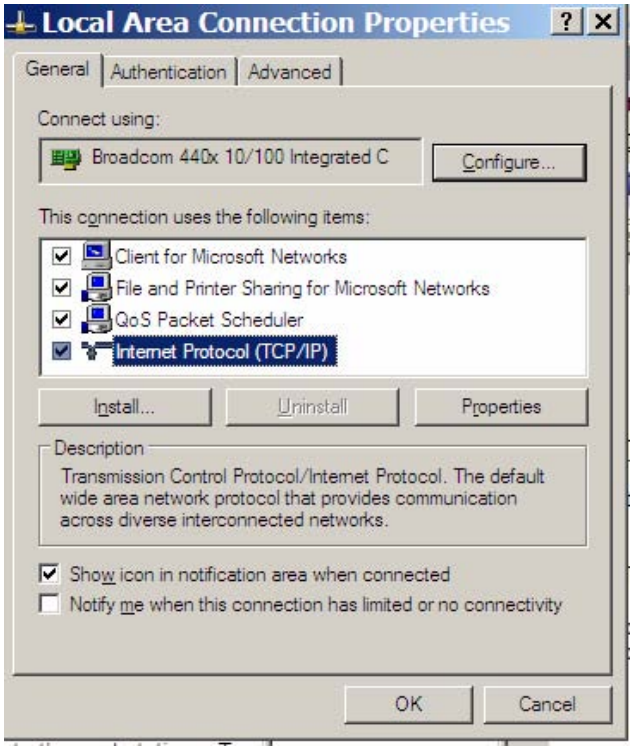
Para completar esta tarea, deberá seguir las siguientes instrucciones paso a paso.

Nota: Estos pasos se deben completar en *cada* estación de trabajo. Las instrucciones son para Windows XP. Los pasos pueden diferir si se utiliza otro sistema operativo.

1. En su computadora, haga clic en **Inicio**, haga clic con el botón derecho en **Mis sitios de red** y luego un último clic en **Propiedades.** Debe mostrarse la ventana Conexiones de red, con íconos que muestren las diferentes conexiones de red.

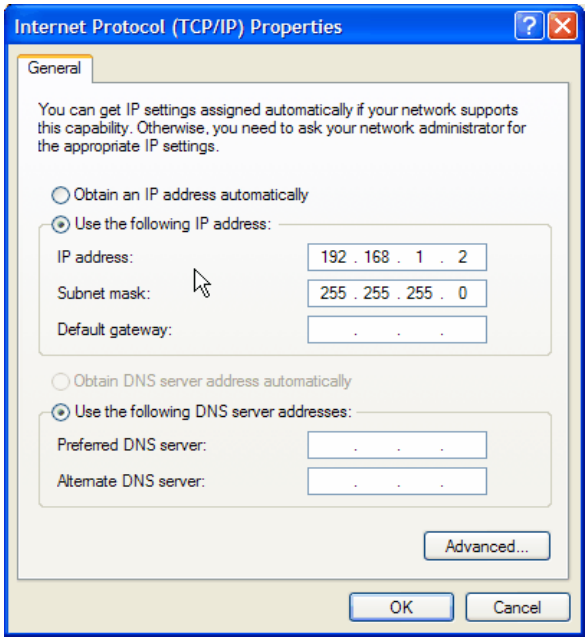


2. Haga clic con el botón derecho en **Conexión de área local** y haga clic en **Propiedades**.
3. Seleccione el **Protocolo de Internet (TCP/IP)** y haga clic en el botón **Propiedades**.



4. En la ficha General de la ventana Propiedades del Protocolo de Internet (TCP/IP), seleccione la opción **Usar la siguiente dirección IP.**

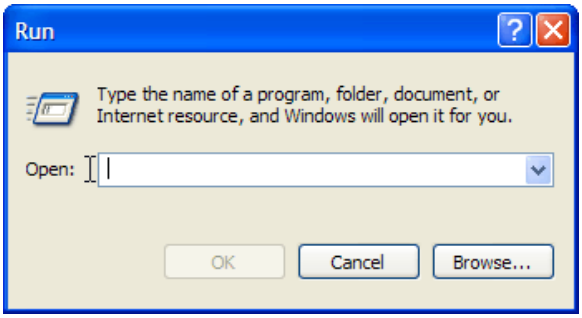
5. En la casilla **Dirección IP**, ingrese la dirección IP 192.168.1.2 para PC1. (Ingrese la dirección IP 192.168.1.3 para PC2.)
6. Presione la tecla de tabulación y la máscara de subred se ingresará automáticamente. La dirección de subred debe ser 255.255.255.0. Si esa dirección no ingresa automáticamente, ingrésela de manera manual.
7. Haga clic en **Aceptar**.



8. Cierre la ventana Propiedades de Conexión de área local.

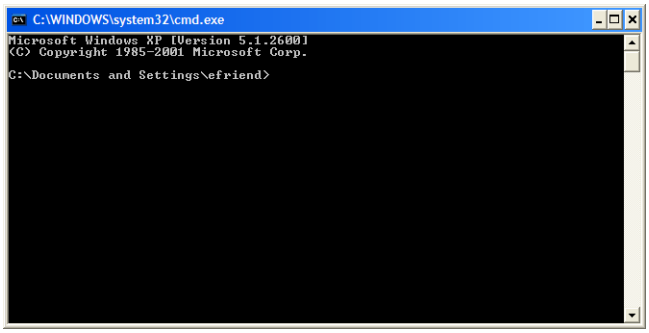
Paso 3: verifique la conectividad.

1. En su computadora, haga clic en **Inicio** y después en **Ejecutar.**



2. Escriba **cmd** en la casilla Abrir y haga clic en **Aceptar.**

   Se mostrará la ventana de comando DOS (cmd.exe). Se pueden ingresar comandos DOS mediante esta ventana. Para ayudar al propósito de esta práctica de laboratorio, se ingresarán comandos de red básicos para permitirle probar conexiones de computadoras.



El comando **ping** es una herramienta de red de computadoras que se utiliza para probar si un host (estación de trabajo, router, servidor, etc.) es alcanzable a través de una red IP.

3. Utilice el comando **ping** para verificar que PC1 puede alcanzar PC2 y que PC2 puede alcanzar PC1. Desde la petición de entrada de comandos PC1 DOS, escriba **ping 192.168.1.3.** Desde la petición de entrada de comandos PC2 DOS, escriba **ping 192.168.1.2.**

   ¿Cuál es el resultado del comando **ping**?

   _____

   _____

   _____

   _____

   Si el comando **ping** muestra un mensaje de error o no recibe una respuesta de la otra estación de trabajo, realice un diagnóstico de fallas. Las áreas que pueden fallar incluyen:

   - Verificación de la dirección IP correcta en ambas estaciones de trabajo
   - Comprobación de que se utilizó el tipo de cable correcto entre las estaciones de trabajo

   ¿Cuál es el resultado del comando **ping** si se desconecta el cable de red y hace ping en la otra estación de trabajo?

   _____

   _____

   _____

   _____

Tarea 4: Conectar las estaciones de trabajo al switch de laboratorio de la clase.

Paso 1: Conecte la estación de trabajo al switch.

Tome el cable correcto y conecte uno de los extremos del mismo al puerto NIC de la estación de trabajo y el otro extremo al puerto del switch.

Paso 2: Repita este proceso con cada estación de trabajo de la red.

¿Qué cable usó? _____

Paso 3: Verifique la conectividad.

Verifique la conectividad de la red utilizando el comando **ping** para alcanzar las otras estaciones de trabajo conectadas al switch.

¿Cuál es el resultado del comando **ping**?

_____

_____

_____

_____

¿Cuál es el resultado del comando **ping** si se hace ping en una dirección que no está conectada a esta red?

_____

_____

_____

_____

Paso 4: Comparta un documento con otras PC.

1. En el escritorio, cree una carpeta nueva y denomínela **prueba**.
2. Haga clic con el botón derecho en la carpeta y haga clic en Compartir archivos. **Nota:** Su ubicará una mano debajo del ícono.
3. Ubique un archivo en la carpeta.
4. En el escritorio, haga doble clic en **Mis sitios de red** y luego en **Computadoras cercanas**.
5. Haga doble clic en el ícono estación de trabajo. Debe mostrarse la carpeta **prueba.** Podrá tener acceso a esta carpeta a través de la red. Una vez que pueda verla y trabajar con el archivo, tendrá acceso a través de las 7 capas del modelo OSI.

Tarea 5: Reflexión

¿Qué podría evitar que un ping se envié entre las estaciones de trabajo cuando éstas están directamente conectadas?

_____

_____

_____

_____

¿Qué podría evitar que un ping se envié a las estaciones de trabajo cuando éstas están conectadas a través del switch?

_____

_____

_____

_____

Práctica de laboratorio 2.6.2: Uso de Wireshark™ para ver las unidades de datos del protocolo

Objetivos de aprendizaje

- Poder explicar el propósito de un analizador de protocolos (Wireshark).
- Poder realizar capturas básicas de la unidad de datos del protocolo (PDU) mediante el uso de Wireshark.
- Poder realizar un análisis básico de la PDU en un tráfico de datos de red simple.
- Experimentar con las características y opciones de Wireshark, como captura de PDU y visualización de filtrado.

Información básica

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Antes de junio de 2006, Wireshark se conocía como Ethereal.

Un husmeador de paquetes (también conocido como un analizador de red o analizador de protocolos) es un software informático que puede interceptar y registrar tráfico de datos pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Wireshark está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado.

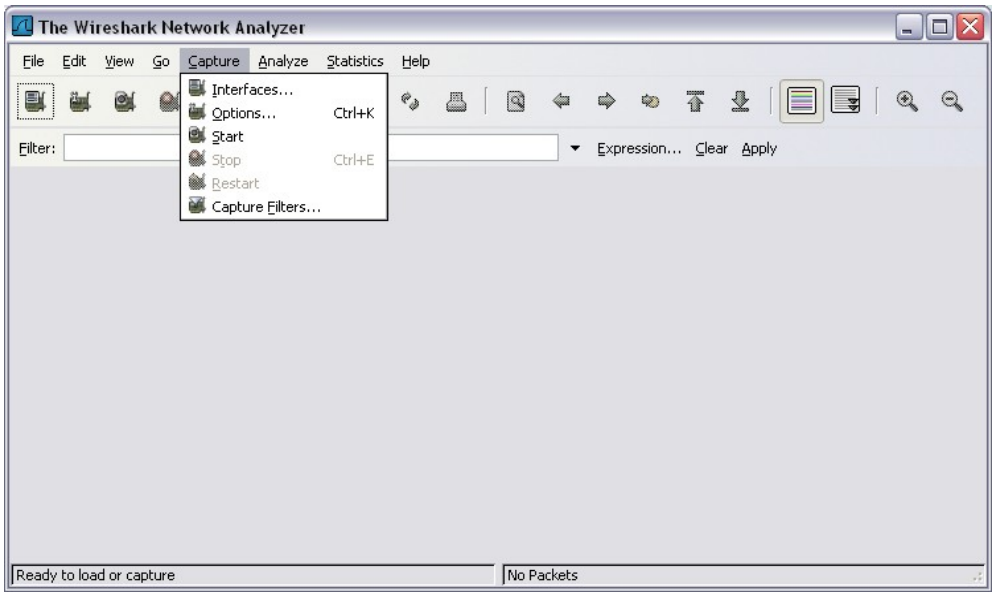
Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos CCNA para el análisis de datos y el diagnóstico de fallas.

Para obtener más información y para descargar el programa visite: http://www.Wireshark.org

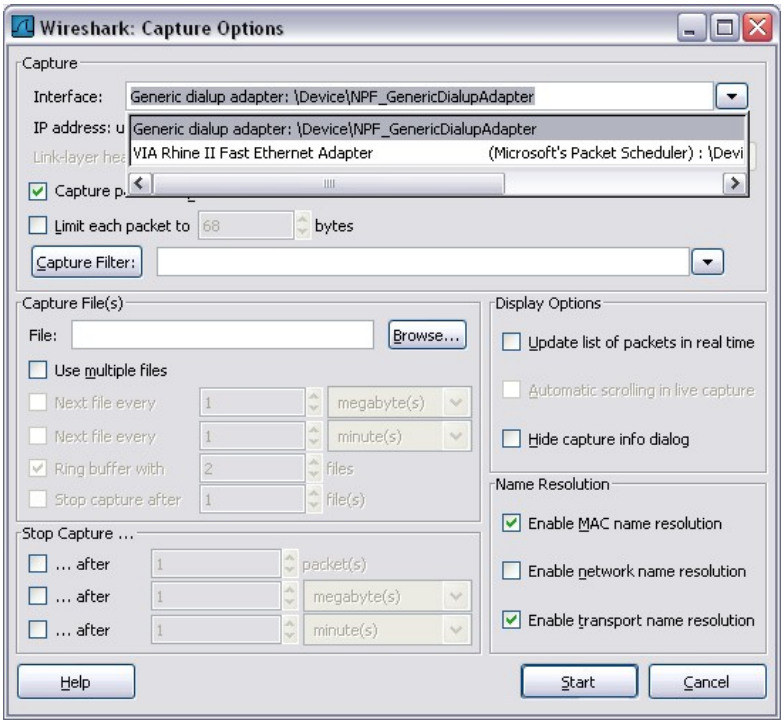
Escenario

Para capturar las PDU, la computadora donde está instalado Wireshark debe tener una conexión activa a la red y Wireshark debe estar activo antes de que se pueda capturar cualquier dato.

Cuando se inicia Wireshark, se muestra la siguiente pantalla.

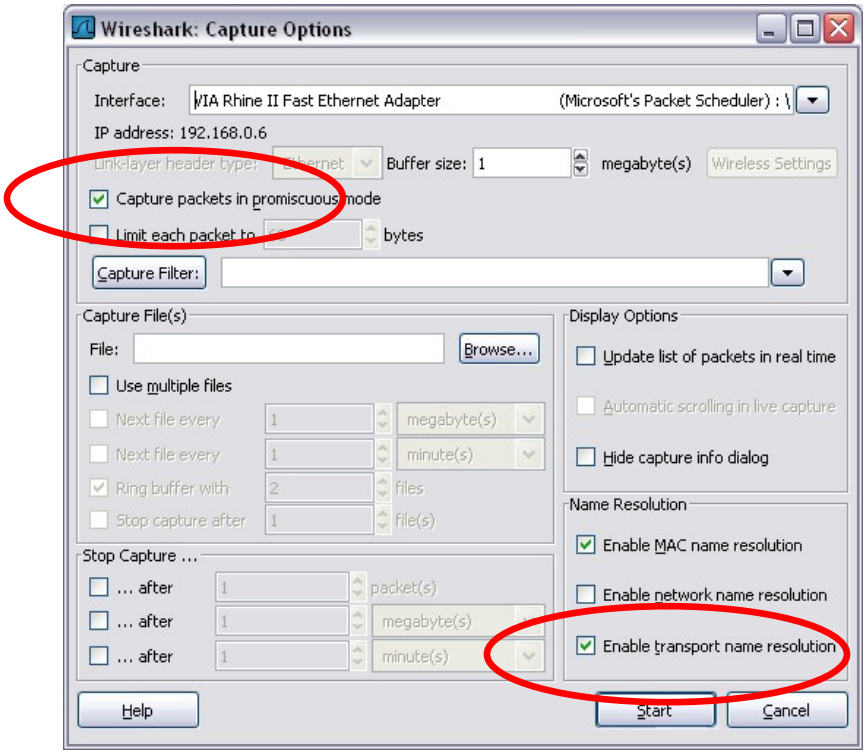


Para empezar con la captura de datos es necesario ir al menú **Captura** y seleccionar **Opciones**. El cuadro de diálogo **Opciones** provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura.



Primero, es necesario asegurarse de que Wireshark está configurado para monitorear la interfaz correcta. Desde la lista desplegable **Interfaz**, seleccione el adaptador de red que se utiliza. Generalmente, para una computadora, será el adaptador Ethernet conectado.

Luego se pueden configurar otras opciones. Entre las que están disponibles en **Opciones de captura,** merecen examinarse las siguientes dos opciones resaltadas.



Configurar Wireshark para capturar paquetes en un modo promiscuo.

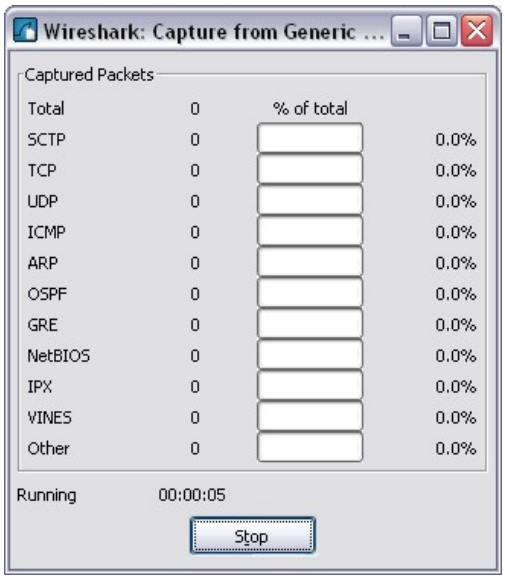
Si esta característica NO está verificada, sólo se capturarán las PDU destinadas a esta computadora. Si esta característica está verificada, se capturarán todas las PDU destinadas a esta computadora Y todas aquellas detectadas por la NIC de la computadora en el mismo segmento de red (es decir, aquellas que “pasan por” la NIC pero que no están destinadas para la computadora).
Nota: La captura de las otras PDU depende del dispositivo intermediario que conecta las computadoras del dispositivo final en esta red. Si utiliza diferentes dispositivos intermediarios (hubs, switches, routers) durante estos cursos, experimentará los diferentes resultados de Wireshark.

Configurar Wireshark para la resolución del nombre de red

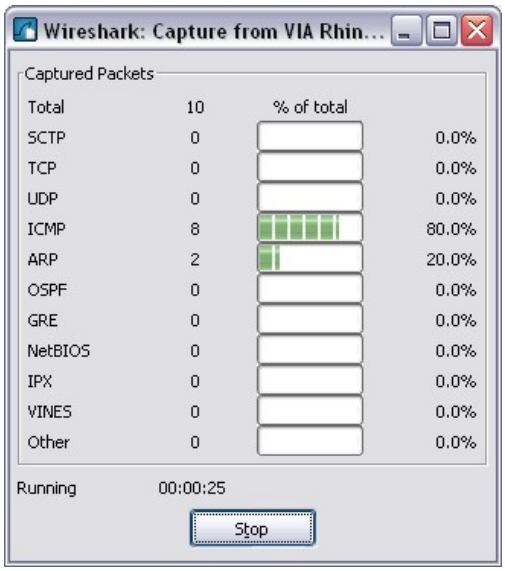
Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis.

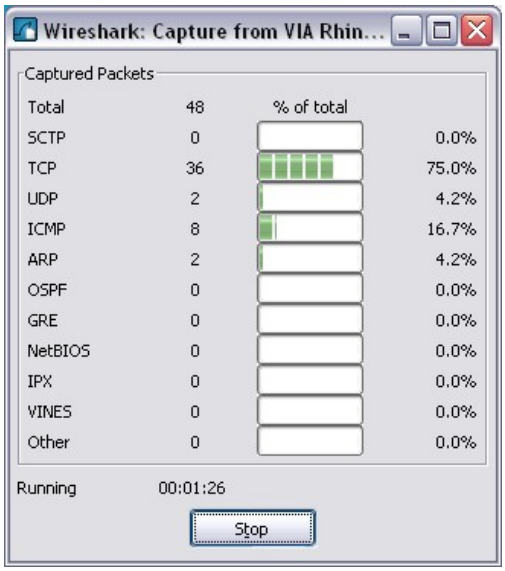
También hay otras configuraciones de proceso y filtrado de captura disponibles.

Haga clic en el botón **Iniciar** para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso.



Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes.

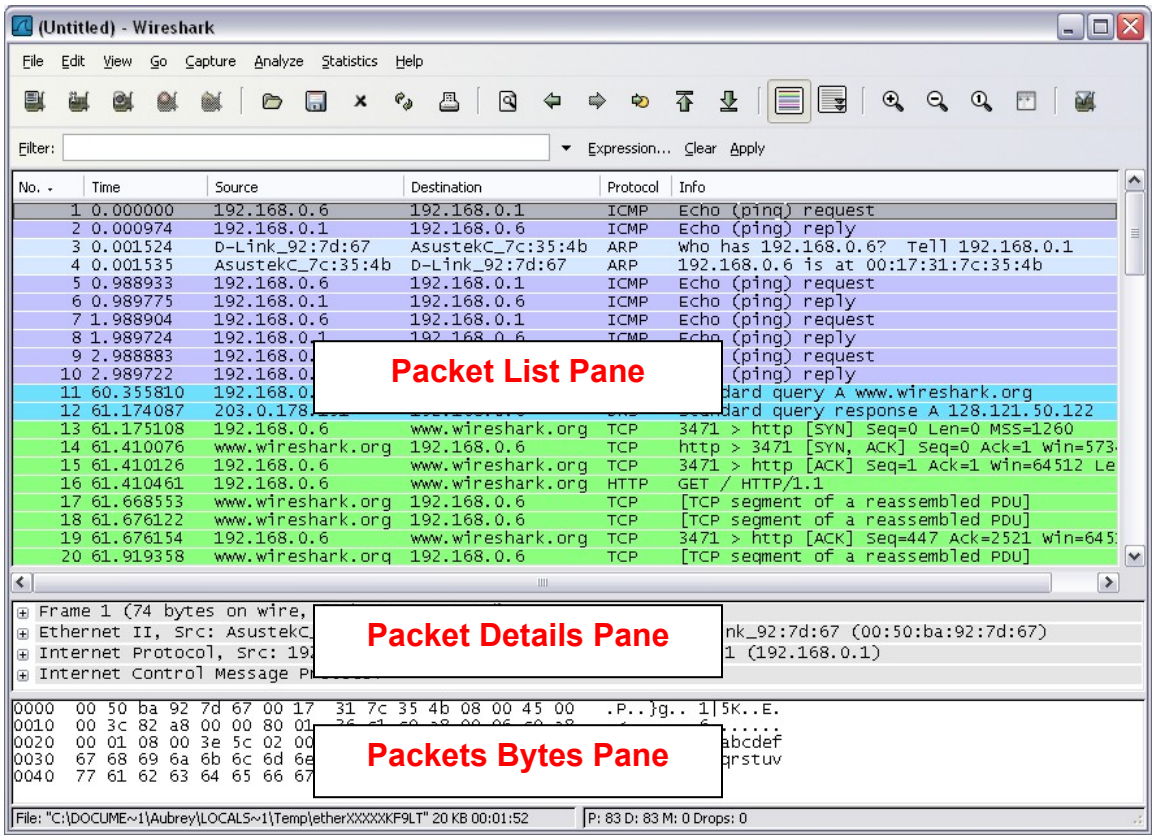




Los ejemplos de arriba muestran la captura de un proceso ping y luego el acceso a una página Web.

Si hace clic en el botón **Detener**, el proceso de captura termina y se muestra la pantalla principal.

La ventana de visualización principal de Wireshark tiene tres paneles.



El panel de Lista de PDU (o Paquete) ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado. Si hace clic en los paquetes de este panel, controla lo que se muestra en los otros dos paneles.

El panel de detalles de PDU (o Paquete) ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete) ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete.

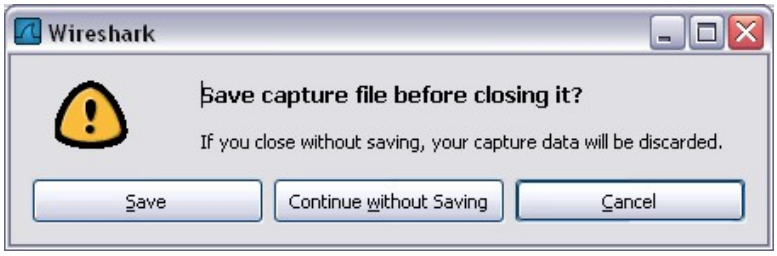
Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados.
Si seleccionó una línea en este panel, se mostrarán más detalles en los paneles “Detalles del paquete” y “Bytes del paquete”. El ejemplo de arriba muestra las PDU capturadas cuando se utilizó la utilidad ping y cuando se accedió a http://www.Wireshark.org. Se seleccionó el paquete número 1 en este panel.

El panel Detalles del paquete muestra al paquete actual (seleccionado en el panel “Lista de paquetes”) de manera más detallada. Este panel muestra los protocolos y los campos de protocolo de los paquetes seleccionados. Los protocolos y los campos del paquete se muestran con un árbol que se puede expandir y colapsar.

El panel Bytes del paquete muestra los datos del paquete actual (seleccionado en el panel “Lista de paquetes”) en lo que se conoce como estilo “hexdump”. En esta práctica de laboratorio no se examinará en detalle este panel. Sin embargo, cuando se requiere un análisis más profundo, esta información que se muestra es útil para examinar los valores binarios y el contenido de las PDU.

La información capturada para las PDU de datos se puede guardar en un archivo. Ese archivo se puede abrir en Wireshark para un futuro análisis sin la necesidad de volver a capturar el mismo tráfico de datos. La información que se muestra cuando se abre un archivo de captura es la misma de la captura original.

Cuando se cierra una pantalla de captura de datos o se sale de Wireshark se le pide que guarde las PDU capturadas.



Si hace clic en **Continuar sin guardar** se cierra el archivo o se sale de Wireshark sin guardar los datos capturados que se muestran.

Tarea 1: Captura de PDU mediante ping

Paso 1: Después de asegurarse de que la topología y configuración de laboratorio estándar son correctas, inicie Wireshark en un equipo en un módulo de laboratorio.

Configure las opciones de captura como se describe arriba en la descripción general e inicie el proceso de captura.

Desde la línea de comando del equipo, haga ping en la dirección IP de otra red conectada y encienda el dispositivo final en la topología de laboratorio. En este caso, haga ping en Eagle Server utilizando el comando ping **192.168.254.254**.

Después de recibir las respuestas exitosas al ping en la ventana de línea de comandos, detenga la captura del paquete.

Paso 2: Examine el panel Lista de paquetes.

El panel Lista de paquetes en Wireshark debe verse ahora parecido a éste:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Observe los paquetes de la lista de arriba. Nos interesan los números de paquetes 6, 7, 8, 9, 11, 12, 14 y 15. Localice los paquetes equivalentes en la lista de paquetes de su equipo.

Si el usuario realizó el Paso 1 A de arriba, haga coincidir los mensajes que se muestran en la ventana de línea de comandos cuando el ping se ejecutó con los seis paquetes capturados por Wireshark.

Responda lo siguiente desde la lista de paquetes Wireshark:

¿Qué protocolo se utiliza por ping? _____

¿Cuál es el nombre completo del protocolo? _____

¿Cuáles son los nombres de los dos mensajes ping? _____

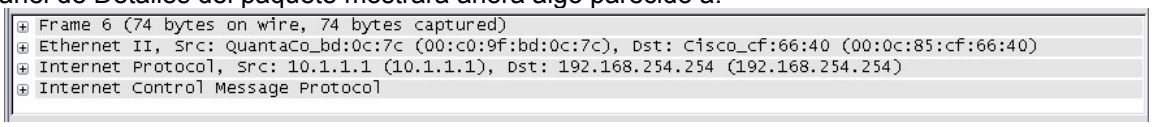
_____

¿Las direcciones IP de origen y destino que se encuentran en la lista son las que esperaba? Sí / No

¿Por qué? _____

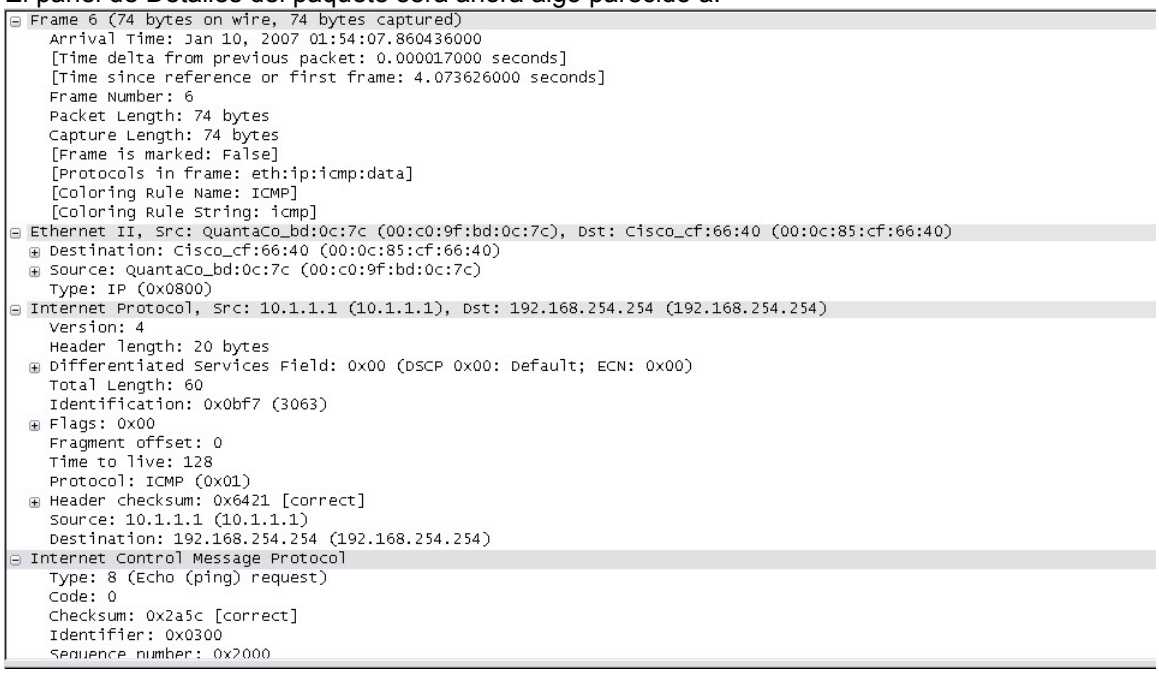
Paso 3: Seleccione (resalte) con el mouse el primer paquete de solicitud de eco en la lista.

El panel de Detalles del paquete mostrará ahora algo parecido a:



Haga clic en cada uno de los cuatro “+” para expandir la información.

El panel de Detalles del paquete será ahora algo parecido a:



Como puede ver, los detalles de cada sección y protocolo se pueden expandir más. Tómese el tiempo para leer esta información. En esta etapa del curso, puede ser que no entienda completamente la información que se muestra, pero tome nota de la que sí reconozca.

Localice los dos tipos diferentes de “Origen” y “Destino”. ¿Por qué hay dos tipos?

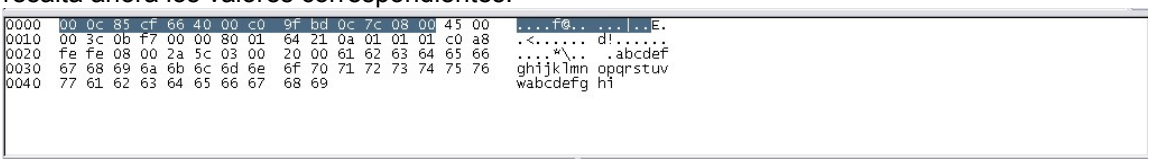
_____

¿Cuáles son los protocolos que están en la trama de Ethernet?

_____

Si selecciona una línea en el panel de Detalles del paquete, toda o parte de la información en el panel de Bytes del paquete también quedará resaltada.

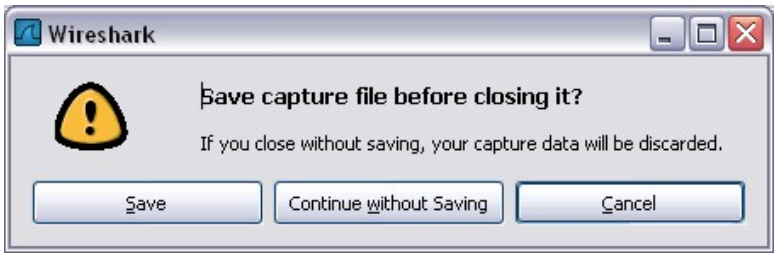
Por ejemplo, si la segunda línea (+ Ethernet II) está resaltada en el panel de detalles, el panel de Bytes resalta ahora los valores correspondientes.



Esto muestra los valores binarios particulares que representan la información de la PDU. En esta etapa del curso no es necesario entender esta información en detalle.

Paso 4: Vaya al menú Archivo y seleccione Cerrar.

Haga clic en **Continuar sin guardar** cuando se muestre esta casilla de mensaje.



Tarea 2: Captura de FTP PDU

Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú **Captura** de Wireshark.

Ingrese **ftp 192.168.254.254** en la línea de comandos del equipo donde se ejecuta Wireshark.

Cuando se establezca la conexión, ingrese **anónimo** como usuario, sin ninguna contraseña.
ID del usuario: **anónimo**
Password: <INTRO>
También se puede iniciar sesión con id de usuario **cisco** y contraseña **cisco.**

Una vez que inició sesión con éxito, ingrese get **/pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe** y presione la tecla ingresar <INTRO>. Con esa operación comenzará la descarga del archivo desde el servidor ftp. El resultado será similar a:

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

Una vez que la descarga del archivo se haya completado, ingrese **quit**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
```

Una vez que los archivos se hayan descargado exitosamente, detenga la captura PDU en Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice y tome nota de las PDU asociadas con la descarga del archivo.
Éstas serán las PDU del protocolo TCP de Capa 4 y del protocolo FTP de Capa 7.

Identifique los tres grupos de PDU asociados con la transferencia del archivo.

Si realizó el paso de arriba, haga coincidir los paquetes con los mensajes y las indicaciones en la ventana de línea de comandos FTP.

El primer grupo está asociado con la fase “conexión” y el inicio de sesión en el servidor.
Haga una lista de ejemplos de mensajes intercambiados en esta fase.

_____

Localice y haga una lista de ejemplos de mensajes intercambiados en la segunda fase, que es el pedido de descarga real y la transferencia de datos.

_____

_____

El tercer grupo de PDU está relacionado con el cierre de sesión y la “desconexión”.
Haga una lista de ejemplos de mensajes intercambiados durante este proceso.

_____

_____

Localice los intercambios TCP recurrentes a través del proceso FTP. ¿Qué característica de TCP indica esto?

_____

_____

Paso 3: Examine los Detalles del paquete.

Seleccione (resalte) un paquete de la lista asociada con la primera fase del proceso FTP.
Observe los detalles del paquete en el panel de Detalles.

¿Cuáles son los protocolos encapsulados en la trama?

_____

Resalte los paquetes que contengan el nombre de usuario y contraseña.
Examine la porción resaltada en el panel Byte del paquete.

¿Qué dice esto sobre la seguridad de este proceso de inicio de sesión FTP?

_____

Resalte un paquete asociado con la segunda fase.
Desde cualquier panel, localice el paquete que contenga el nombre del archivo.

El nombre del archivo es: _____

Resalte un paquete que contenga el contenido real del archivo. Observe el texto simple visible en el panel Byte.

Resalte y examine en los paneles Detalles y Byte; algunos de los paquetes intercambiados en la tercera fase de la descarga del archivo.
¿Qué características distinguen al contenido de estos paquetes?

_____

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 3: Captura de HTTP PDU

Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú Captura de Wireshark.

Nota: Si se continúa desde pasos anteriores de esta práctica de laboratorio, no es necesario configurar las opciones de captura.

Inicie un navegador Web en el equipo donde ejecuta Wireshark.
Ingrese el URL de Eagle Server ejemplo.com o ingrese la dirección IP-192.168.254.254. Una vez que la página Web se haya descargado por completo, detenga la captura del paquete Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice e identifique los paquetes TCP y HTTP asociados con la descarga de la página Web.

Observe el parecido entre este intercambio de mensajes y el intercambio FTP.

Paso 3: En el panel Lista de paquetes, resalte un paquete HTTP que tenga la notación "(text/html)" en la columna Información.

En el panel Detalles del paquete, haga clic en "+" al lado de "Datos de texto basado en línea: html"
¿Cuándo esta información expande lo que se muestra?

_____

Examine la porción que resaltó en el panel Byte.
Esto muestra los datos HTML que contiene el paquete.

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 4: Reflexión

Considere lo que puede proveer Wireshark sobre la información de encapsulación referida a los datos de red capturados. Relacione esto a los modelos de la capa OSI y TCP/IP. Es importante que el usuario pueda reconocer y relacionar tanto los protocolos representados como la capa de protocolo y los tipos de encapsulación de los modelos con la información provista por Wireshark.

Tarea 5: Desafío

Analice cómo podría utilizar un analizador de protocolos como Wireshark para:

(1) diagnosticar fallas de una página Web para descargar con éxito un navegador en un equipo

e

(2) identificar el tráfico de datos en una red requerida por los usuarios.

_____

_____

_____

_____

_____

_____

_____

Tarea 6: Limpieza

A menos que el instructor le indique lo contrario, salga de Wireshark y apague el equipo correctamente.

2.7.1: Desafío de integración de habilidades: Examen de paquetes

Diagrama de topología

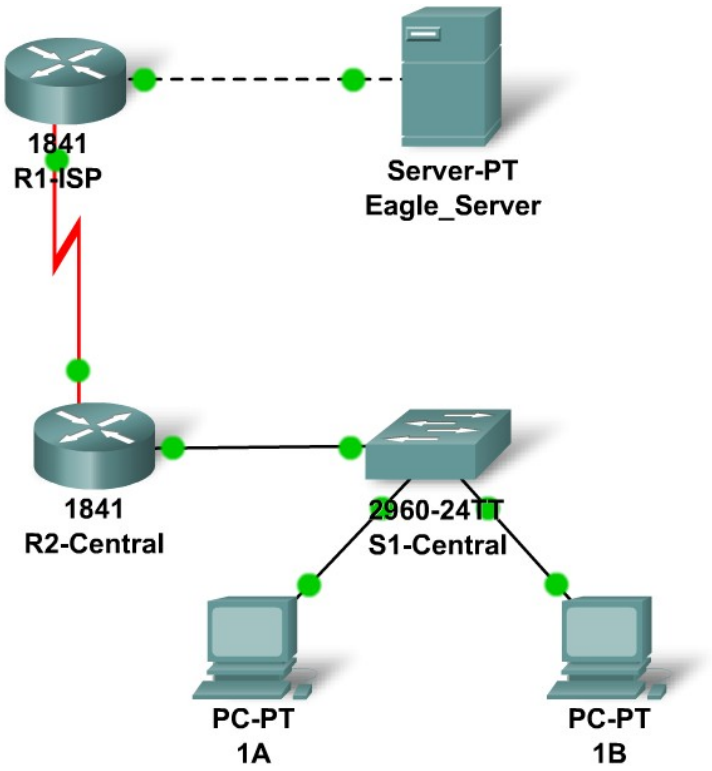


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Completar la topología
- Agregar PDU simples en modo de tiempo real
- Analizar los PDU en modo de simulación
- Experimentar con el modelo de configuración estándar del laboratorio

Información básica

A lo largo del curso, utilizará una configuración de laboratorio estándar creada a partir de PC, servidores, routers y switches reales para aprender los conceptos sobre redes. En esta actividad, seguirá aprendiendo cómo construir y analizar la topología de laboratorio estándar. Si aún no lo ha hecho, se lo invita a examinar los archivos de Ayuda disponibles en el menú desplegable de Ayuda en la parte superior del GUI del Packet Tracer. Los recursos incluyen “Mi primer laboratorio de PT” para ayudarle a aprender el funcionamiento básico del Packet Tracer, tutoriales para guiarlo en las distintas tareas e información sobre las fortalezas y limitaciones de usar el Packet Tracer para modelar redes.

Esta actividad le brindará una oportunidad para explorar la configuración de laboratorio estándar usando el simulador del Packet Tracer. El Packet Tracer posee dos formatos de archivo que puede crear: archivos .pkt (archivos modelos de simulación de red) y archivos .pka (archivos de actividad para práctica). Cuando cree sus propias redes en el Packet Tracer o modifique los archivos existentes de su instructor o de sus pares, generalmente usará el formato de archivo .pkt. Cuando inició esta actividad del plan de estudios, aparecieron estas instrucciones. Son el resultado del .pka, el formato de archivo de actividad del Packet Tracer. En la parte inferior de estas instrucciones hay dos botones: Verificar resultados (que le indica qué porcentaje de la actividad ha realizado) y Restablecer actividad (que inicia la actividad nuevamente, si quiere borrar su trabajo o adquirir más experiencia).

Tarea 1: Realización de la topología.

Agregue una PC al área de trabajo. Configúrela con los siguientes parámetros: Dirección IP 172.16.1.2, máscara de subred 255.255.0.0, gateway por defecto 172.16.255.254, Servidor DNS 192.168.254.254, nombre exhibido “1B” (no incluya las comillas). Conecte la PC 1B al puerto Fa0/2 del switch S1-Central y verifique su trabajo con el botón **Verificar resultados** para determinar que la topología esté completa.

Tarea 2: Aumento de PDU simples en modo de tiempo real.

Mediante Agregar PDU simple, envíe un mensaje de prueba: un mensaje entre la PC 1B y el Eagle Server. Observe que este paquete aparecerá en la lista de eventos como algo que se “detectó” en la red y en la esquina inferior derecha como una PDU creada por el usuario que puede manipularse con fines de verificación.

Tarea 3: Análisis de las PDU en modo de simulación (rastreo de paquetes).

Cambie a modo de simulación. Haga doble clic en el botón “Fire” (fuego) en la ventana de la PDU creada por el usuario. Utilice el botón **Capturar/Adelantar** para mover el paquete por la red. Haga clic en el sobre del paquete o en el cuadrado de color de la columna Información de la Lista de eventos para examinar el paquete en cada paso de su viaje.

Tarea 4: Experimentación con el modelo de configuración estándar del laboratorio

La configuración estándar del laboratorio consiste de dos routers, un servidor y dos PC. Cada uno de estos dispositivos está preconfigurado. Intente crear distintas combinaciones de paquetes de prueba y analizar su viaje por la red.

Reflexión

Si aún no lo ha hecho, se lo alienta a obtener el Packet Tracer de su instructor y completar Mi primer laboratorio de Packet Tracer (disponible a través del menú desplegable AYUDA, en CONTENIDOS).

Actividad 3.4.1: captura del flujo de datos

Objetivos de aprendizaje

Al completar esta actividad, usted podrá:

- Capturar o descargar un stream de audio
- Registrar las características del archivo
- Examinar la velocidad de transferencia de datos asociada al archivo

Información básica

Cuando una aplicación crea un archivo, los datos que contiene ese archivo deben ser guardados en algún lado. Estos datos se pueden guardar en el dispositivo final en el que fueron creados o pueden ser transferidos para ser almacenados en otro dispositivo.

En esta actividad, usará un micrófono y un grabador de sonido de Microsoft para capturar un stream de audio. El grabador de sonido de Microsoft es un accesorio de Windows que se puede encontrar en XP en **Inicio > Programas >Accesorios > Entretenimiento > Grabador de sonido**. Si no tiene disponibles un micrófono ni el grabador de sonido de Microsoft, puede descargar un archivo de audio para usar en esta actividad en http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html.

Escenario

Esta actividad se realizará en una computadora que tenga un micrófono y un grabador de sonido de Microsoft o acceso a Internet para poder descargar un archivo de audio.

El tiempo estimado para finalizarla, según la velocidad de la red, es de 30 minutos.

Tarea 1: Creación de un archivo de sonido

Paso 1: Abrir la aplicación grabador de sonido de Windows.

La aplicación se puede encontrar en Windows XP en **Inicio > Programas > Accesorios > Entretenimiento > Grabador de sonido**. En la Figura 1 se muestra la interfaz del grabador de sonido.

Figura 1. Interfaz del grabador de sonido

Paso 2: Grabar un archivo de audio.

1. Para comenzar a grabar, haga clic en el botón Grabar de la interfaz del grabador de sonido.
2. Hable al micrófono o cree sonidos que puedan ser capturados por el micrófono. Mientras se graba el audio, deberá aparecer una representación en forma de onda de sonido en la interfaz del grabador de sonido, como se muestra en la Figura 2.

Figura 2. Grabación en progreso

3. Haga clic en el botón Detener cuando haya terminado.

Paso 3: Verificar que se haya grabado el archivo de sonido.

1. Presione el botón Reproducir para escuchar la grabación. Se debería reproducir la grabación realizada, como se muestra en la Figura 3.

Figura 3. Reproducción

Si no puede escuchar la grabación, verifique la configuración del micrófono, de los altavoces y del volumen e intente crear la grabación nuevamente.

Si no puede crear una grabación, descargue un archivo de audio de News@Cisco en el siguiente URL: http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html.

2. Guarde el archivo de audio en el escritorio y proceda con la Tarea 2.

Paso 4: Guardar el archivo de audio.

1. Guarde en el escritorio el archivo de audio que creó. Asígnele el nombre **myaudio.wav**.
2. Una vez que el archivo esté guardado, cierre la aplicación del grabador de sonido.

Tarea 2: Observación de las propiedades del archivo de audio

Paso 1: Ver las propiedades del archivo de audio.

Haga clic con el botón derecho del mouse sobre el archivo que guardó en el escritorio y haga clic en **Propiedades** del menú desplegable.

¿Cuál es el tamaño del archivo en kilobytes? _____

¿Cuál es el tamaño del archivo en bytes? _____

¿Cuál es el tamaño del archivo en bits? _____

Paso 2: Abrir el archivo de audio en el reproductor de Windows Media.

1. Haga clic con el botón derecho del Mouse sobre el archivo de audio y seleccione **Abrir con > Reproductor de Windows Media**.
2. Cuando el archivo esté abierto, haga clic con el botón derecho del mouse en la parte superior de la interfaz del reproductor de Windows Media y seleccione **Archivo > Propiedades** en el menú desplegable.

¿Cuál es la duración del archivo de audio en segundos? _____

Calcule la cantidad de datos por segundo en el archivo de audio y guarde el resultado. _____

Tarea 3: Reflexión

Puede que los archivos de datos no permanezcan en los dispositivos en los que fueron creados. Por ejemplo, usted puede querer copiar en otra computadora o en un dispositivo portátil de audio el archivo que creó.

Si el archivo de audio que guardó en el escritorio tuviera que ser transferido a una velocidad de 100 megabits por segundo (Mbps), ¿cuánto tiempo tardaría en completarse la transferencia?

_____

Incluso con una conexión Ethernet que trabaja a 100 Mbps, los datos que forman el archivo no se transfieren a esta velocidad. Todas las tramas de Ethernet contienen otra información, como las direcciones de origen y de destino que son necesarias para entregar la trama.

Si la sobrecarga Ethernet usa el 5% de los 100 Mbps disponibles y el 95% del ancho de banda se reserva para la carga de datos, ¿cuánto tiempo tardaría en completarse la transferencia del archivo?

_____

Tarea 4: Limpieza

Es posible que se le solicite que elimine de la computadora el archivo de audio que había guardado. De ser así, borre el archivo del escritorio.

A menos que se le indique otra cosa, apague la computadora.

Práctica de laboratorio 3.4.2: Administración de un servidor Web

Diagrama de topología

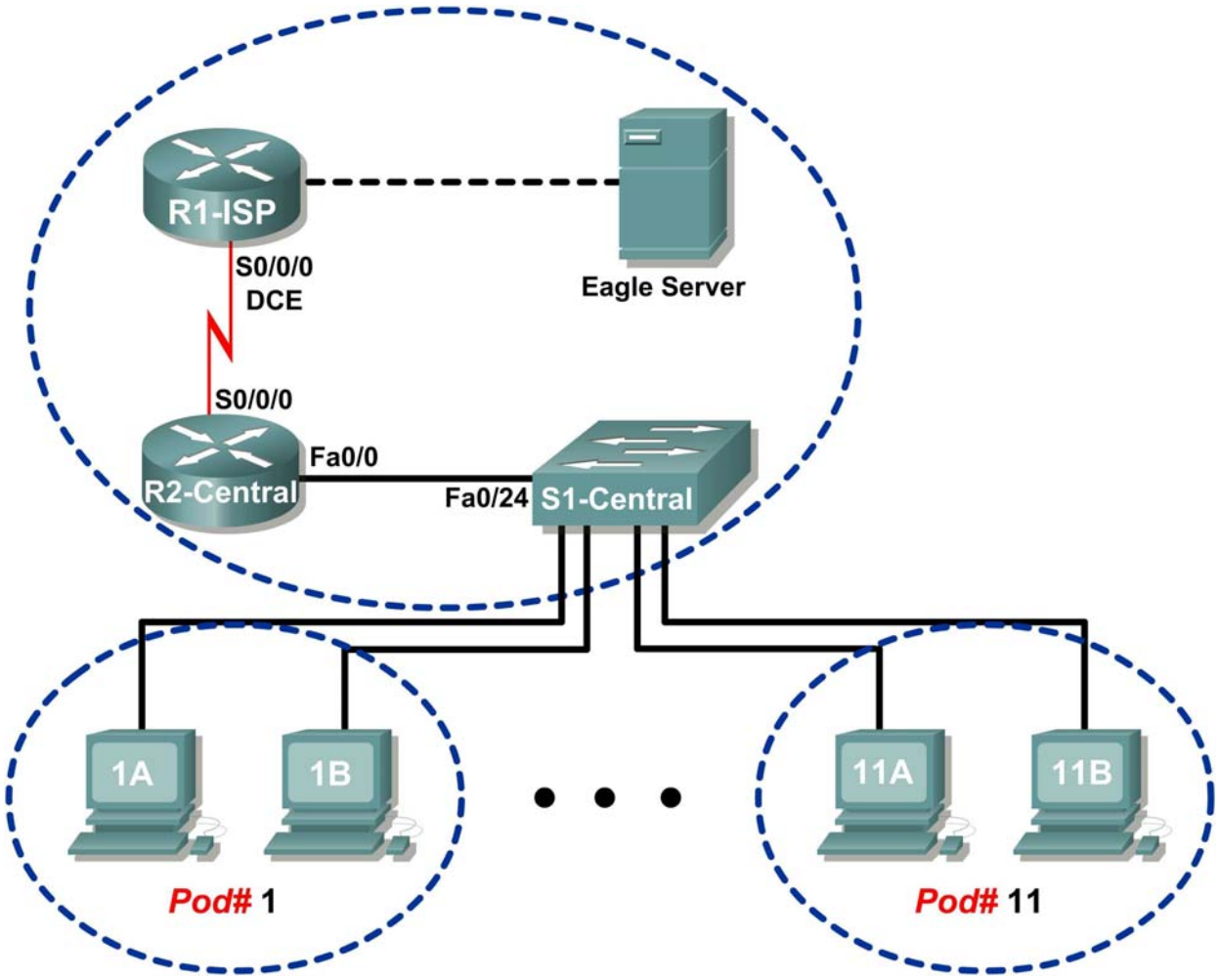


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	**S0/0/0**	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	**S0/0/0**	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	***No aplicable***	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod*#**A**	***No aplicable***	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#**B**	***No aplicable***	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	***No aplicable***	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Descargar, instalar y verificar una aplicación de servidor Web
- Verificar el archivo de configuración de servidor Web predeterminado
- Capturar y analizar tráfico HTTP con Wireshark

Información básica

Los servidores Web son una parte importante del plan de negocios para cualquier organización con presencia en Internet. Los navegadores Web son utilizados por los consumidores para acceder a sitios Web de negocios. Sin embargo, los navegadores Web constituyen sólo la mitad del canal de comunicación. La otra mitad del canal de comunicación es el soporte del servidor Web. El soporte del servidor Web es una ayuda valiosa para los administradores de red. Basada en una encuesta realizada por Netcraft en enero de 2007, la siguiente tabla muestra las aplicaciones de los tres mejores servidores Web según el porcentaje de uso:

Servidor Web	Porcentaje de uso
Apache	60%
Microsoft	31%
Sun	1,6%

Escenario

En este laboratorio descargará, instalará y configurará el conocido servidor Web Apache. Se utilizará un explorador Web para conectar el servidor y un Wireshark para capturar la comunicación. El análisis de la captura lo ayudará a entender el funcionamiento del protocolo HTTP.

Tarea 1: Descargar, instalar y verificar el servidor Web Apache.

La práctica de laboratorio debe estar configurada como se muestra en el Diagrama de topología y en la tabla de dirección lógica. En caso contrario, pídale ayuda al instructor antes de continuar.

Paso 1: Descargue el software desde Eagle Server.

La aplicación del servidor Web Apache está disponible para descargar en Eagle Server.

1. Utilice un navegador Web y el URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3 para acceder y descargar el software. Vea la Figura 1.

Figura 1. Pantalla de descarga FTP para el servidor Web Apache

2. Haga clic con el botón derecho en el archivo y guarde el software en el equipo host del módulo.

Paso 2: Instale el servidor Web Apache en el equipo host del módulo.

1. Abra la carpeta donde guardó el software y haga doble clic en el archivo Apache para comenzar la instalación. Elija valores predeterminados y acepte el acuerdo de licencia. El próximo paso de la instalación requiere una configuración personalizada del servidor Web. Ver Figura 2.

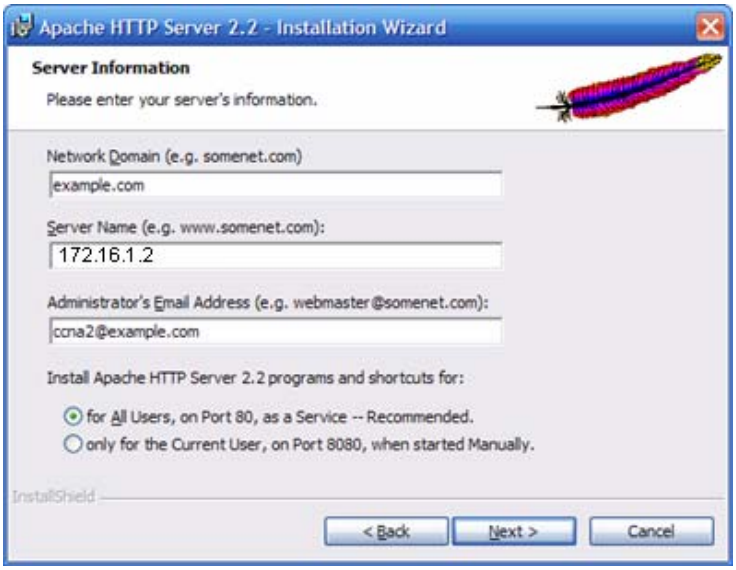


Figura 2. Pantalla de configuración personalizada

Utilice los siguientes valores:

Información	Valor
Dominio de red	example.com
Nombre del servidor	dirección IP del equipo
Dirección de correo electrónico del administrador	ccna*@example.com

* Por ejemplo, para usuarios del 1 al 22, si el equipo está en Pod 5, Host B, el número de correo electrónico del administrador es ccna10@example.com

2. Acepte el puerto y el estado de servicio recomendados. Haga clic en **Siguiente**.
3. Acepte la instalación típica predeterminada y haga clic en **Siguiente**.

¿Cuál es la carpeta de instalación predeterminada?

_____

4. Acepte la carpeta de instalación predeterminada, haga clic en **Siguiente** y luego en **Instalar.** Cuando haya terminado la instalación, cierre la pantalla.

Figura 3. Alerta de seguridad de Windows

Nota: Si aparece una alerta de seguridad de Windows, seleccione desbloquear. Ver Figura 3. Esto permitirá las conexiones con el servidor Web.

Paso 3: Verifique el servidor Web.

El comando **`netstat`** mostrará estadísticas de protocolo e información de conexión para este equipo de laboratorio.

1. Elija **Inicio > Ejecutar** y abra una ventana de línea de comandos. Escriba **cmd** y luego haga clic en **Aceptar**. Utilice el comando **`netstat -a`** para descubrir puertos abiertos y conectados en el equipo.

```
C:\>netstat -a
Conexiones activas

Proto  Dirección local        Dirección remota      Estado
TCP    GW-desktop-hom:http    GW-desktop-hom:0      LISTENING
```

```
TCP      GW-desktop-hom:epmap           GW-desktop-hom:0     LISTENING
TCP      GW-desktop-hom:microsoft-ds    GW-desktop-hom:0     LISTENING
TCP      GW-desktop-hom:3389            GW-desktop-hom:0     LISTENING
<resultado omitido>
C:\>
```

2. Utilice el comando **`netstat -a,`** verifique que el servidor Web funciona correctamente en el equipo host del módulo.

   El ícono de monitor del servidor Web Apache debe estar visible en la parte inferior derecha de la pantalla, cerca de la hora.

3. Abra un navegador Web y conéctese al URL de su equipo. Si el servidor Web está trabajando correctamente, se mostrará una página Web similar a la de la Figura 4.

Figura 4. Página predeterminada del servidor Web

   La dirección de red 127.0.0.0 / 8 está reservada y se utiliza para direcciones IP locales. Debe mostrarse la misma página si el URL cambia a la dirección IP en la interfaz Ethernet o a cualquier dirección IP host en el rango de red 127.0.0.0 / 8.

4. Pruebe el servidor Web en varias direcciones IP diferentes en el rango de red de 127.0.0.0 /8. Complete la siguiente tabla con los resultados:

Dirección IP	Estado	Explicación
127.0.0.1		
127.255.255.254		
127.255.255.255		
127.0.0.0		

Tarea 2: Verificar el archivo de configuración de servidor Web predeterminado.

Paso 1: Acceder al archivo `httpd.conf`.

Puede que un administrador de sistema necesite verificar o modificar el archivo de configuración predeterminado.

Abra el archivo de configuración del servidor Web Apache, C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf. Ver Figura 5.

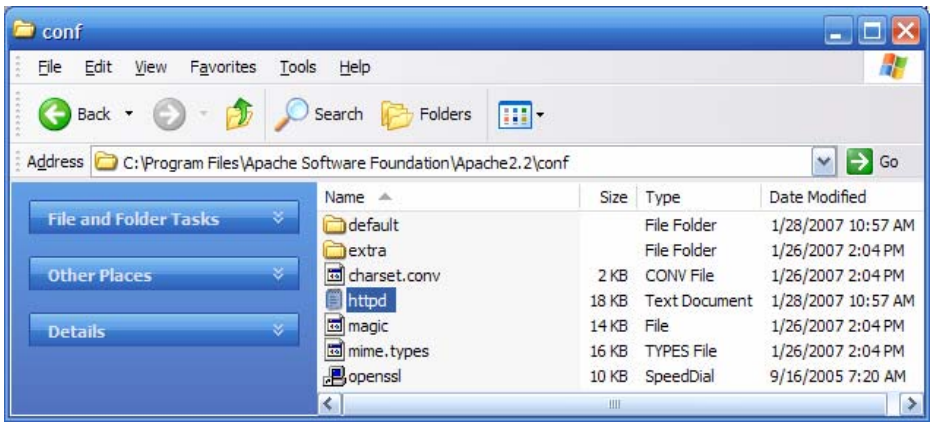


Figura 5. Archivo de configuración del servidor Web Apache

Paso 2: Revise el archivo `httpd.conf`.

Numerosos parámetros de configuración le permiten al servidor Web Apache ser completamente personalizable. El carácter "#" indica un comentario para los administradores del sistema, exento del acceso del servidor Web. Desplácese hacia abajo al archivo de configuración y verifique las siguientes configuraciones:

Valor	Significado
`#Escuchar 12.34.56.78:80` `Escuchar 80`	Escuche el puerto TCP 80 para todas las conexiones entrantes. Para aceptar conexiones sólo de este host, cambie la línea a `Escuchar 127.0.0.1 80`.
`ServerAdmin ccna2@example.com`	Si hay problemas, envíe un correo electrónico al servidor Web a esta dirección de correo electrónico.
`ServerName 172.16.1.2:80`	Para servidores sin nombres DNS, utilice el número de puerto de la dirección IP.
`DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"`	Éste es el directorio raíz para el servidor Web.

`<IfModule dir_module>`
`  DirectoryIndex index.html`
`</IfModule>`
	`DirectoryIndex` establece el archivo que Apache ofrecer requiere un directorio. Si no se requiere ninguna página de ese directorio, muestre `index.html` si está presente.

Paso 3: Modifique la página predeterminada del servidor Web.

La Figura 4 muestra la página Web predeterminada del archivo index.html. A pesar de que esta página es suficiente para la prueba, se debe mostrar algo más personal.

1. Abra la carpeta C:\Program Files\Apache Software Foundation\Apache2.2\htdocs. Debe estar presente el archivo index.html. Haga clic con el botón derecho en el archivo y elija **Abrir con.** Desde la lista desplegable, elija **Bloc de notas.** Cambie el contenido del archivo por algo similar al siguiente ejemplo:

```
<html><body><h1>¡¡¡Bienvenido al servidor Web Pod1HostB!!!</h1>
<center><bold>
¡Operado por mí!
</center></bold>
```

```
Contacte al administrador Web: ccna2@example.com
</body></html>
```

2. Guarde el archivo y actualice el navegador Web. O abra el URL http://127.0.0.1. Debe mostrarse la nueva página predeterminada. Después de realizar y guardar los cambios en index.html, simplemente actualice el navegador Web para ver el nuevo contenido.

Tarea 3: Capturar y analizar tráfico HTTP con Wireshark.

Wireshark no capturará paquetes enviados desde o hacia la red 127.0.0.0 en una computadora Windows. No se mostrará la interfaz. Para completar esta tarea, conéctese a una computadora de un estudiante o a Eagle Server y analice el intercambio de datos.

Paso 1: Analice el tráfico HTTP.

1. Inicie Wireshark y configure la interfaz de captura con la interfaz vinculada con la red 172.16. Abra un navegador Web y conéctese a otra computadora con un servidor Web activo.

¿Por qué *no* hace falta ingresar index.html en el URL para que se muestren los contenidos del archivo?

_____

2. Ingrese deliberadamente una página que no se encuentre en el servidor Web, tal como se muestra en la Figura 6. Observe que apareció un mensaje de error en el navegador Web.

Figura 6. Error 404 No se puede encontrar la página

La Figura 7 contiene una sesión HTTP capturada. El servidor Web requiere el archivo index.html, pero el servidor no tiene el archivo. En cambio, el servidor envía un error **404.** El navegador Web simplemente muestra la respuesta del servidor “No se puede encontrar la página”.

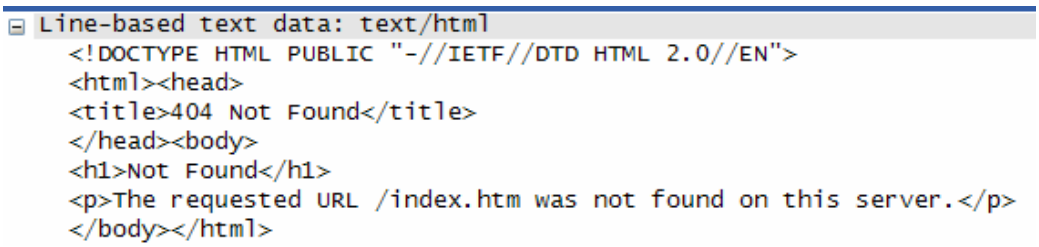
No.	Time	Source	Destination	Protocol	Info
20	14.384747	172.16.1.2	172.16.1.1	TCP	1149 > http [SYN] Seq=0 Len=0 MSS=1460
21	14.384993	172.16.1.1	172.16.1.2	TCP	http > 1149 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
22	14.385030	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	14.388292	172.16.1.2	172.16.1.1	HTTP	GET /index.htm HTTP/1.1
24	14.389299	172.16.1.1	172.16.1.2	HTTP	HTTP/1.1 404 Not Found (text/html)
25	14.541723	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=256 Ack=423 Win=63818 Len=0

Figura 7. Captura Wireshark de tráfico HTTP

3. Resalte la línea de captura que contiene el error 404 y desplácese a la segunda (del medio) ventana Wireshark. Expanda el registro de datos de texto basado en línea.

   ¿Cuáles son los contenidos?

   _____



Tarea 4: Desafío

Modifique el archivo de configuración predeterminado del servidor Web httpd.conf y cambie la línea `Escuchar` a `Escuchar 8080`. Abra un navegador Web y acceda al URL http://127.0.0.1:8080. Con el comando **`netstat,`** verifique que el puerto TCP nuevo del servidor Web sea 8080.

Tarea 5: Reflexión

Los servidores Web son un componente importante de e-commerce. Dependiendo de la organización, el administrador de red o Web tiene la responsabilidad de mantener el servidor Web de la empresa. Esta práctica de laboratorio demostró cómo instalar y configurar el servidor Web Apache, comprobar la operación correcta e identificar varios parámetros clave de configuración.

El estudiante modificó la página Web predeterminada index.html y observó el efecto en el resultado del navegador Web.

Finalmente, se utilizó Wireshark para capturar una sesión HTTP de un archivo no encontrado. El servidor Web respondió con un error HTTP 1.1 404 y devolvió un mensaje de archivo no encontrado al navegador Web.

Tarea 6: Limpieza

Durante esta práctica de laboratorio, se instaló el servidor Web Apache en el equipo host del módulo. Deberá desinstalarse. Para desinstalar el servidor Web, haga clic en **Inicio > Panel de Control > Agregar o quitar programas**. Haga clic en **Apache Web Server** y luego en **Quitar**.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 3.4.3: Protocolos y servicios de correo electrónico

Diagrama de topología

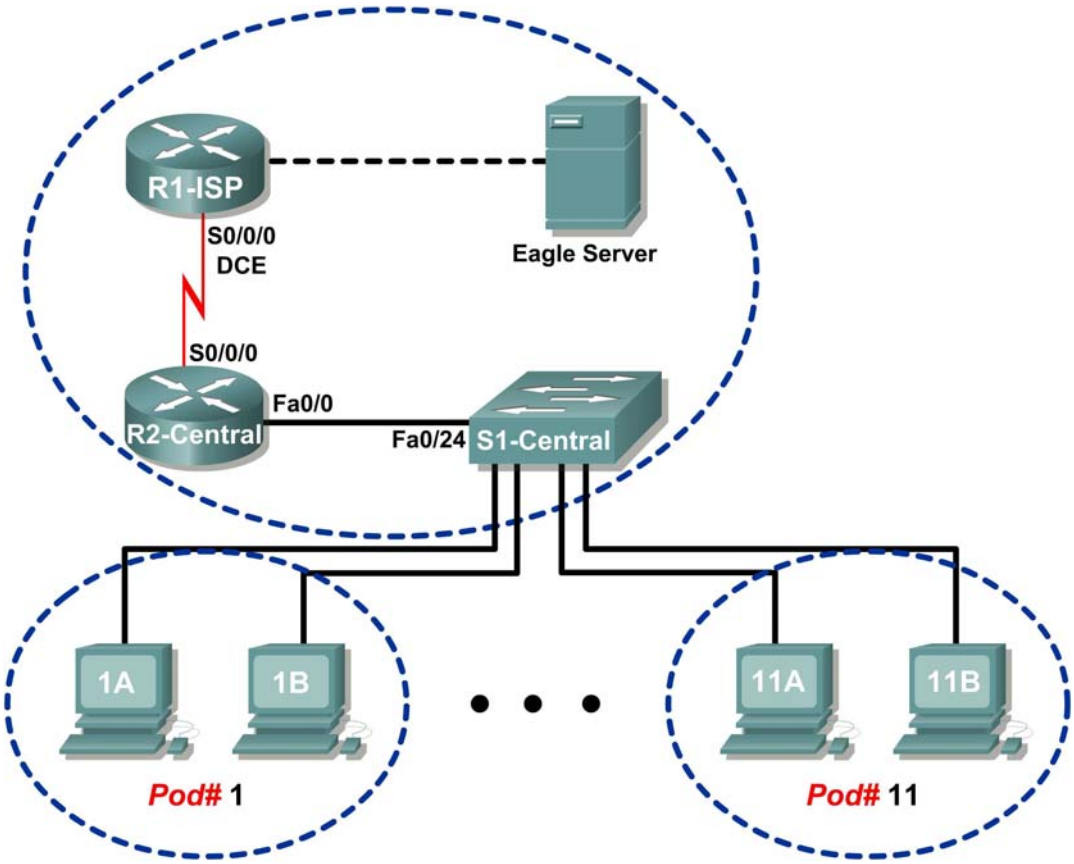


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16. *Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Configurar el equipo host del módulo para el servicio de correo electrónico
- Capturar y analizar comunicaciones por correo electrónico entre el equipo host del módulo y un servidor de mail

Información básica

El correo electrónico es uno de los servicios de red más populares que utiliza un modelo cliente/servidor. El cliente de correo electrónico se configura en una computadora de usuario para conectarse a un servidor de correo electrónico. La mayoría de los proveedores de servicios de Internet (ISP) provee instrucciones paso a paso para el uso de los servicios de correo electrónico. Es por eso que un usuario típico puede desconocer las complejidades del correo electrónico o de los protocolos que se utilizan.

En entornos de red donde el cliente MUA debe conectarse a un servidor de correo electrónico en otra red para enviar y recibir correos electrónicos, se utilizan los siguientes dos protocolos:

- Simple Mail Transfer Protocol (SMTP), que se definió originalmente en RFC 281, agosto de 1982, y ha pasado por varias modificaciones y mejoras. RFC 2821, abril de 2001, que consolida y actualiza RFC relacionados con correos electrónicos anteriores. El servidor SMTP escucha el puerto TCP 25 bien conocido. El SMTP se utiliza para enviar correos electrónicos del cliente externo al servidor de correos electrónico, entregar correos electrónicos a cuentas locales y relay de correos electrónicos entre servidores SMTP.
- Post Office Protocol versión 3 (POPv3) se utiliza cuando un cliente de correo electrónico externo desea recibir correos electrónicos desde el servidor de correo electrónico. El servidor POPv3 escucha el puerto TCP 110 bien conocido.

Las versiones anteriores de ambos protocolos no deben utilizarse. También existen versiones seguras de ambos protocolos que usan capas de socket seguras/seguridad de la capa de transporte (SSL/TSL) para la comunicación.

El correo electrónico está sujeto a múltiples vulnerabilidades de seguridad de equipos. Los ataques de correo no deseado invaden la red con correos electrónicos no solicitados e inútiles que consumen ancho de banda y recursos de red. Los servidores de correo electrónico han tenido numerosas vulnerabilidades que han generado peligro para los equipos.

Escenario

En esta práctica de laboratorio, el usuario configurará y utilizará una aplicación de cliente de correo electrónico para conectarse a los servicios de red de eagle-server. El usuario monitorea la comunicación con Wireshark y analiza los paquetes capturados.

Se utilizará un cliente de correo electrónico, como Outlook Express o Mozilla Thunderbird, para conectarse a un servicio de red de eagle-server. Eagle-server tiene servicios de correo SMTP previamente configurados con cuentas de usuarios que pueden enviar y recibir correos electrónicos externos.

Tarea 1: Configurar el equipo host del módulo para el servicio de correo electrónico.

La práctica de laboratorio debe estar configurada como se muestra en el Diagrama de topología y en la tabla de dirección lógica. En caso contrario, pídale ayuda al instructor antes de continuar.

Paso 1: Descargue e instale Mozilla Thunderbird.

Si Thunderbird no está instalado en el equipo host del módulo, se puede descargar de eagle- server.example.com. Ver Figura 1. El URL para descargarlo es `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3`.

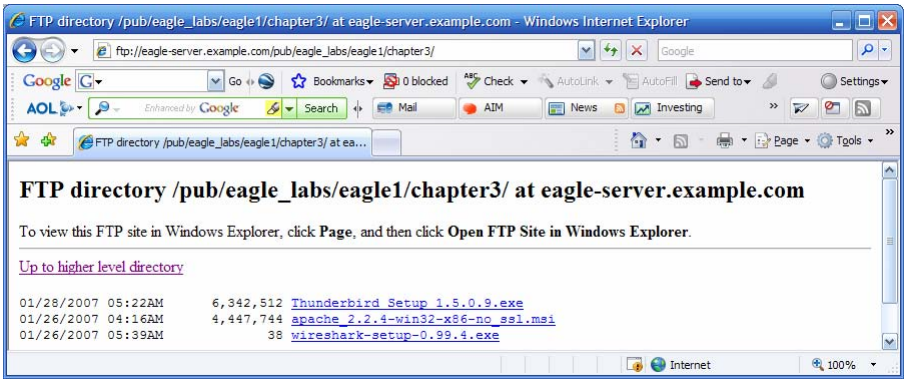


Figura 1. Descarga de FTP para Wireshark

1. Haga clic con el botón derecho en el nombre de archivo Thunderbird y luego guarde el archivo en el equipo host del módulo.
2. Una vez que se descargó el archivo, haga doble clic en el nombre de archivo e instale Thunderbird con las configuraciones predeterminadas.
3. Cuando haya finalizado, inicie Thunderbird.

Paso 2: Configurar Thunderbird para recibir y enviar correos electrónicos.

1. Cuando Thunderbird inicie, se debe configurar la cuenta de correo electrónico. Complete la información de la cuenta tal como se indica a continuación:

Campo	Valor
Nombre de la cuenta	El nombre de la cuenta está basado en el equipo host del módulo. Hay un total de 22 cuentas configuradas en Eagle Server, rotuladas ccna[1.22]. Si este host del módulo está en Pod1, Host A, entonces el nombre de la cuenta es ccna1. Si este host del módulo está en Pod3, Host B, entonces el nombre de la cuenta es ccna6. Y así sucesivamente.
Su nombre	Utilice el mismo nombre que arriba.
Dirección de correo electrónico	*Su_nombre*@eagle-server.example.com
Tipo de servidor de entrada que utiliza	POP
Servidor de entrada (SMTP)	eagle-server.example.com
Servidor de salida (SMTP)	eagle-server.example.com

2. Verifique las configuraciones de la cuenta en **Herramientas > Configuraciones de la cuenta**. Vea la Figura 2.

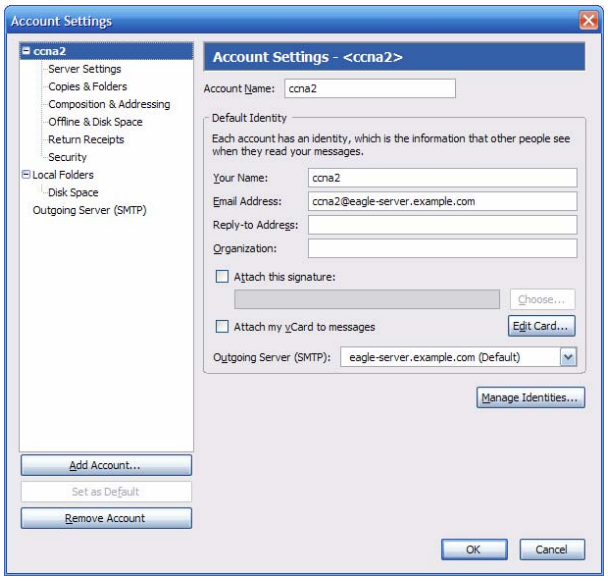


Figura 2. Configuraciones de la cuenta Thunderbird

3. En el panel izquierdo de la pantalla Configuraciones de la cuenta, haga clic en **Configuraciones del servidor**. Se verá una pantalla similar a la que se muestra en la Figura 3.

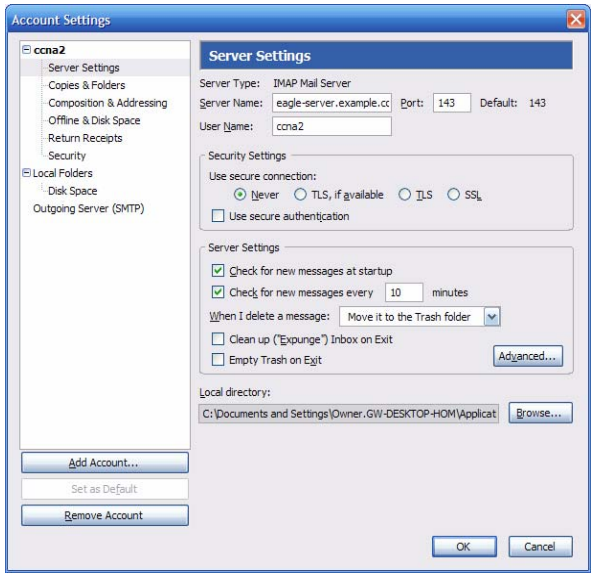


Figura 3. Pantalla Configuraciones del servidor de Thunderbird

La Figura 4 muestra la configuración correcta para el servidor de salida (SMTP).

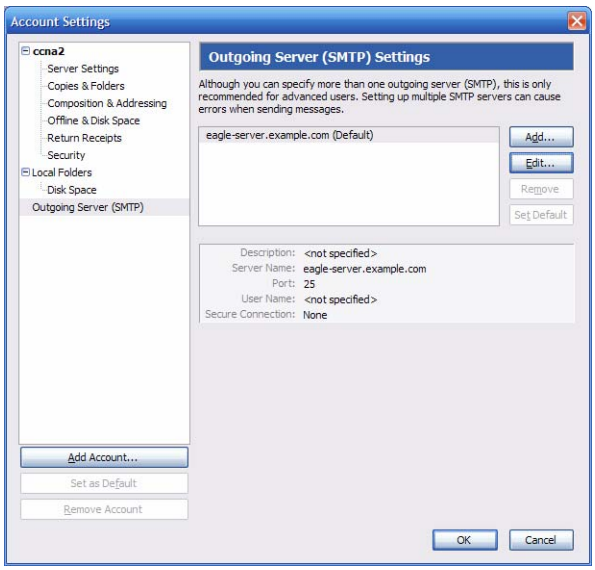


Figura 4. Pantalla Configuraciones del servidor de salida (SMTP)

¿Cuál es el propósito del protocolo SMTP y cuál es el número de puerto TCP bien conocido?

_____

_____

Tarea 2: Capturar y analizar comunicaciones por correo electrónico entre el equipo host del módulo y un servidor de correo electrónico.

Paso 1: Enviar un correo electrónico no capturado.

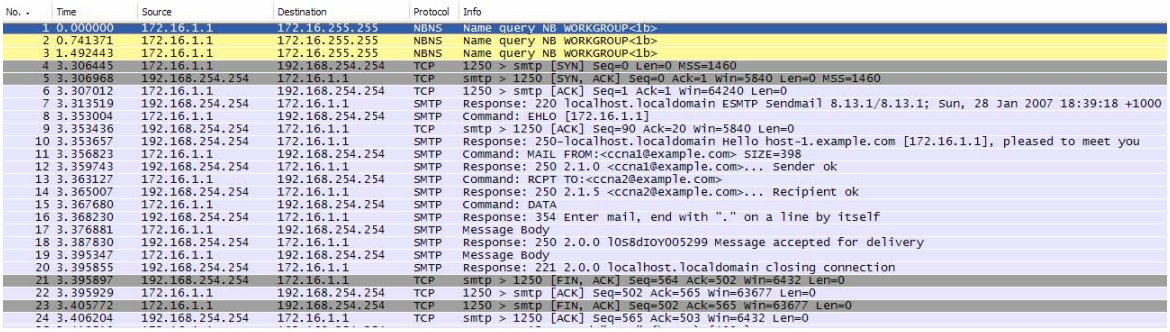
1. Pregúntele a otro estudiante de la clase cuál es su nombre de correo electrónico.
2. Utilice ese nombre para componer y enviar un mensaje amistoso a un estudiante.

Paso 2: Iniciar las capturas de Wireshark.

Una vez que esté seguro de que el funcionamiento del correo electrónico es el correcto tanto para enviar como para recibir, inicie la captura Wireshark. Wireshark mostrará capturas basadas en el tipo de paquete.

Paso 3: Analice una sesión de captura Wireshark de SMTP.

1. Utilice al cliente de correo electrónico y de nuevo, envíe un correo electrónico a un estudiante y reciba otro de él. Esta vez, no obstante, las transacciones del correo electrónico serán capturadas.
2. Después de enviar y recibir un mensaje de correo electrónico, detenga la captura Wireshark. En la Figura 5 se muestra una captura parcial Wireshark de un correo electrónico saliente utilizando SMTP.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
2	0.741371	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
3	1.492443	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
4	3.306445	172.16.1.1	192.168.254.254	TCP	1250 > smtp [SYN] Seq=0 Len=0 MSS=1460
5	3.306968	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
6	3.307012	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	3.313519	192.168.254.254	172.16.1.1	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan 2007 18:39:18 +1000
8	3.353004	172.16.1.1	192.168.254.254	SMTP	Command: EHLO [172.16.1.1]
9	3.353436	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0
10	3.353657	192.168.254.254	172.16.1.1	SMTP	Response: 250-localhost.localdomain Hello host-1.example.com [172.16.1.1], pleased to meet you
11	3.356823	172.16.1.1	192.168.254.254	SMTP	Command: MAIL FROM:<ccna1@example.com> SIZE=398
12	3.359743	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.0 <ccna1@example.com>... Sender ok
13	3.363127	172.16.1.1	192.168.254.254	SMTP	Command: RCPT TO:<ccna2@example.com>
14	3.365007	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.5 <ccna2@example.com>... Recipient ok
15	3.367680	172.16.1.1	192.168.254.254	SMTP	Command: DATA
16	3.368230	192.168.254.254	172.16.1.1	SMTP	Response: 354 Enter mail, end with "." on a line by itself
17	3.376881	172.16.1.1	192.168.254.254	SMTP	Message Body
18	3.387830	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delivery
19	3.395347	172.16.1.1	192.168.254.254	SMTP	Message Body
20	3.395855	192.168.254.254	172.16.1.1	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
21	3.395897	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0
22	3.395929	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0
23	3.405772	172.16.1.1	192.168.254.254	TCP	1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0
24	3.406204	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0

Figura 5. Captura SMTP

3. Resalte la primera captura SMTP en la ventana Wireshark de arriba. En la Figura 5, es la línea número 7.
4. Expanda el registro del Simple Mail Transfer Protocol en la segunda ventana Wireshark.

   Hay varios tipos diferentes de servidores SMTP. Atacantes maliciosos pueden acceder a información valiosa simplemente aprendiendo el tipo y versión del servidor SMTP.

¿Cuál es el nombre y la versión del servidor SMTP?

_____

Las aplicaciones del cliente de correo electrónico envían comandos a los servidores de correo electrónico y los servidores de correo electrónico envían respuestas. En cada primer intercambio SMTP, el cliente de correo electrónico envía el comando **EHLO.** Sin embargo, la sintaxis puede variar entre clientes y el comando ser **HELO** o **HELLO**. El servidor de correo electrónico debe responder al comando.

¿Cuál es la respuesta del servidor SMTP al comando EHLO?

_____

Los próximos intercambios entre cliente y servidor de correo electrónico contienen información de correo electrónico. Utilice la captura Wireshark, complete las respuestas del servidor de correo electrónico a los comandos del cliente de correo electrónico:

Cliente de correo electrónico	Servidor de correo electrónico
MAIL FROM:,ccna1@excmaple.com>	
RCPT TO:<ccna2@example.com>	
DATOS	
(cuerpo de mensaje enviado)	

¿Cuáles son los contenidos del último cuerpo de mensaje de parte del cliente de correo electrónico?

_____

¿Cómo responde el servidor de correo electrónico?

_____

Tarea 3: Desafío

Acceda a un equipo que tenga acceso a Internet. Busque el nombre y la versión del servidor SMTP para conocer las debilidades o compromisos. ¿Hay versiones más nuevas disponibles?

Tarea 4: Reflexión

El correo electrónico es probablemente el servicio de red más comúnmente usado. Entender el flujo de tráfico con el protocolo SMTP lo ayudará a entender cómo el protocolo administra la conexión de datos cliente/servidor. El correo electrónico también puede tener problemas de configuración. ¿El problema es con el cliente de correo electrónico o con el servidor de correo electrónico? Una manera simple de probar el funcionamiento del servidor SMTP es usar la utilidad Telnet de la línea de comandos Windows para telnet dentro del servidor SMTP.

1. Para probar la operación SMTP, abra la ventana de línea de comandos Windows y comience una sesión Telnet con el servidor SMTP.

```
C:\> telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
correo electrónico SMTP server test...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Connection to host lost.
C:\>
```

Tarea 5: Limpieza

Si se instaló Thunderbird en el equipo host del módulo para esta práctica de laboratorio, seguramente el instructor va a querer que se elimine la aplicación. Para eliminar Thunderbird, haga clic en **Inicio > Panel de Control > Agregar o quitar programas.** Desplácese hasta **Thunderbird** y haga clic allí, luego haga clic en **Quitar**.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

3.5.1: Desafío de integración de habilidades: Configuración de hosts y de servicios

Diagrama de topología

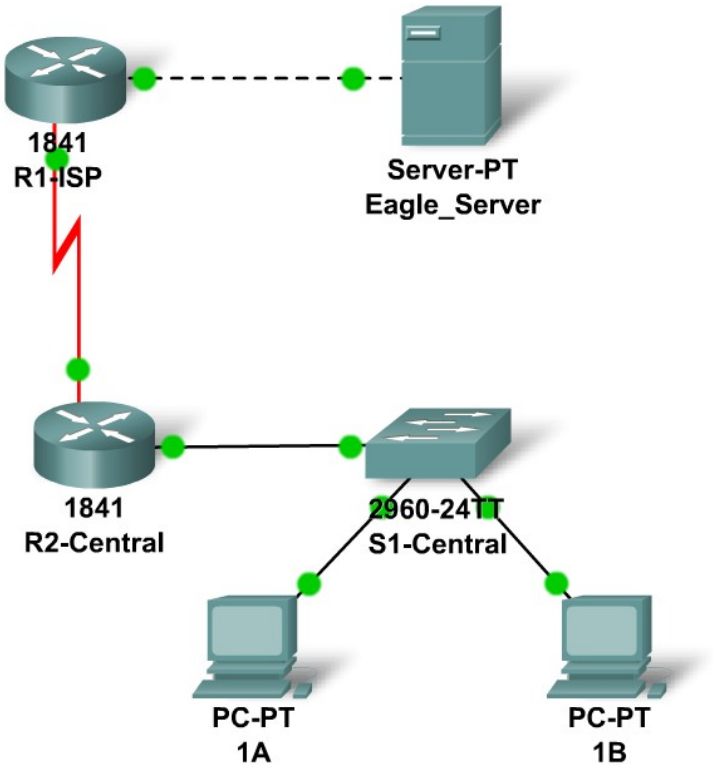


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Configurar hosts y servicios
- Agregar, configurar y conectar hosts y servicios
- Explorar cómo trabajan en forma conjunta DNS y HTTP
- Usar el modo de simulación para visualizar detalles de paquetes generados por DNS y HHTP

Información básica

A lo largo del curso, utilizará una configuración de laboratorio estándar creada a partir de PC, servidores, routers y switches reales para aprender los conceptos sobre redes. Al final de cada capítulo, desarrollará secciones cada vez más largas de esta topología en el Packet Tracer.

Tarea 1: "Reparación" y prueba de la topología.

Agregue una PC con el nombre 1B exhibido en la topología. Configúrela con los siguientes parámetros: Dirección IP 172.16.1.2, Máscara de subred 255.255.0.0, Gateway por defecto 172.16.255.254 y Servidor DNS 192.168.254.254. Conecte la PC 1B al puerto Fa0/2 del switch S1-Central.

Conecte el Eagle Server al puerto Fa0/0 en el router R1-ISP. Encienda los servicios Web en el servidor habilitando HTTP. Habilite los servicios DNS y agregue una entrada DNS que asocie "eagle-server.example.com" (sin comillas) con la dirección IP del servidor. Verifique su trabajo utilizando la evaluación con el botón **Verificar resultados** y la ficha **Puntos de evaluación**. Pruebe la conectividad, en tiempo real, mediante AGREGAR PDU SIMPLE para probar la conectividad entre la PC 1B y el Eagle Server.

Tenga en cuenta que cuando agrega una PDU simple, ésta aparece en la ventana Lista de PDU como parte de "Situación 0". La primera vez que ejecute este mensaje ping para un solo lanzamiento, aparecerá como **Fallido**, esto se debe al proceso ARP que se explicará posteriormente. Al hacer doble clic en el botón "Disparar" en la ventana Lista de PDU, enviará esta prueba de ping simple por segunda vez. Esta vez tendrá éxito. En el Packet Tracer, el término "situación" significa una configuración específica de uno o más paquetes de prueba. Puede crear diferentes situaciones de paquetes de prueba con el botón **Nuevo**; por ejemplo, Situación 0 podría tener un paquete de prueba de la PC 1B al Eagle Server, Situación 1 podría tener paquetes de prueba entre la PC 1A y los routers, y así sucesivamente. Puede retirar todos los paquetes de prueba de una situación en particular al utilizar el botón **Eliminar**. Por ejemplo, si utiliza el botón **Eliminar** para la Situación 0, el paquete de prueba que acaba de crear entre la PC 1B y el Eagle Server se retirará; hágalo antes de pasar a la siguiente tarea.

Tarea 2: Exploración del funcionamiento en conjunto de DNS y HTTP.

Cambie del modo de tiempo real al modo de simulación. Abra un navegador Web desde el escritorio de la PC 1B. Escriba eagle-server.example.com, presione Enter y luego use el botón **Capturar / Reenviar** de la **Lista de eventos** para capturar la interacción de DNS y HTTP. Reproduzca esta animación y examine el contenido del paquete (Ventana de **Información de PDU**, **Detalles de PDU entrantes, Detalles de PDU salientes**) para cada evento de la lista de eventos, especialmente cuando los paquetes están en la PC 1B o en el Eagle Server. Si recibe el mensaje "Búfer lleno", haga clic en el botón **Ver eventos anteriores**. Si bien es posible que aún no comprenda el procesamiento de los paquetes por parte del switch y los routers, debe poder entender cómo trabajan en forma conjunta DNS y HTTP.

Reflexión

¿Puede explicar ahora el proceso que ocurre cuando escribe un URL en un navegador y aparece una página Web? ¿Qué tipo de interacciones cliente-servidor se invocan?
Si aún no lo ha hecho, se lo alienta a obtener el Packet Tracer de su instructor y completar Mi primer laboratorio de Packet Tracer (elija el menú desplegable AYUDA, y luego CONTENIDOS).

Práctica de laboratorio 4.5.1: Observación de TCP y UDP utilizando Netstat

Diagrama de topología

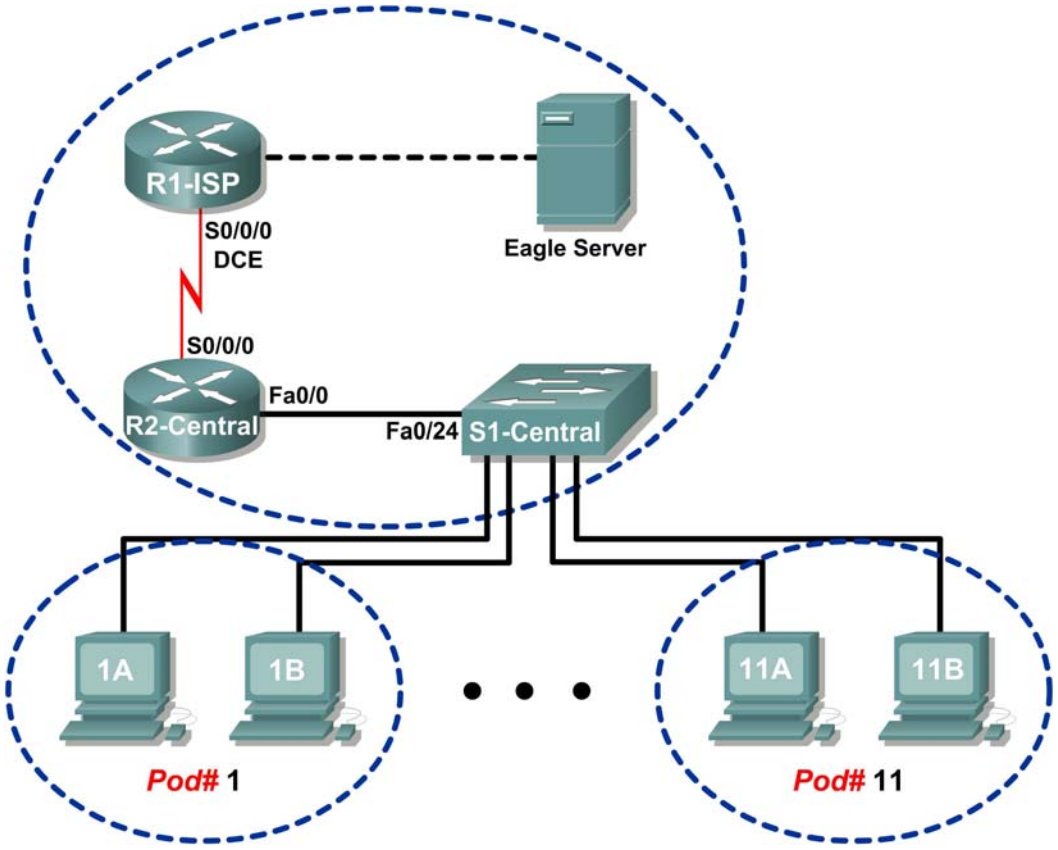


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

- Explicar parámetros y resultados de comandos **netstat** comunes.
- Utilizar **netstat** para examinar la información del protocolo en un equipo host del módulo.

Información básica

netstat es la abreviatura de la utilidad de estadísticas de red que se encuentra disponible tanto en computadoras Windows como en computadoras Unix / Linux. El paso de parámetros opcionales con el comando cambiará la información de resultado. **netstat** muestra conexiones de red entrantes y salientes (TCP y UDP), información de tabla de enrutamiento del equipo host y estadísticas de la interfaz.

Escenario

En esta práctica de laboratorio el estudiante examinará el comando **netstat** en un equipo host del módulo y ajustará las opciones de resultado de **netstat** para analizar y entender el estado del protocolo de la capa de Transporte TCP/IP.

Tarea 1: Explicar parámetros y resultados de comandos netstat comunes.

Abra una ventana terminal haciendo clic en Inicio | Ejecutar. Escriba **cmd** y presione **Aceptar**.

Para mostrar información de ayuda sobre el comando **netstat**, utilice las opciones **/?**, como se muestra:

```
C:\> netstat /? <INTRO>
```

Utilice el comando de salida **netstat** /? como referencia para completar la opción que mejor se ajuste a la descripción:

Opción	Descripción
	Muestra todas las conexiones y puertos que escuchan.
	Muestra direcciones y números de puerto en forma numérica.
	Vuelve a mostrar estadísticas cada cinco segundos. Presione CONTROL+C para detener la nueva visualización de las estadísticas.
	Muestra conexiones para el protocolo especificadas por protocolo. El protocolo puede ser cualquiera de los siguientes: TCP, UDP, TCPv6, o UDPv6. Si se usa con la opción -s para mostrar estadísticas por protocolo, el protocolo puede ser cualquiera de los siguientes: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, o UDPv6.
	Vuelve a mostrar todas las conexiones y puertos que escuchan cada 30 segundos.
	Muestra sólo las conexiones abiertas. Éste es un problema complicado.

Cuando se muestran estadísticas **netstat** para conexiones TCP, también se muestra el estado TCP. Durante la conexión TCP, la conexión atraviesa por una serie de estados. La siguiente tabla es un resumen de los estados TCP desde RFC 793, Transmission Control Protocol, septiembre de 1981, tal como lo informó **netstat**:

Estado	Descripción de la conexión
ESCUCHAR	La conexión local está a la espera de un pedido de conexión de parte de cualquier dispositivo remoto.
ESTABLECIDA	La conexión está abierta y se pueden intercambiar datos a través de la conexión. Éste es el estado normal para la fase de transferencia de datos de la conexión.
TIEMPO-ESPERA	La conexión local está esperando un período de tiempo predeterminado después de enviar un pedido de finalización de conexión antes de cerrar la conexión. Ésta es una condición normal y generalmente dura entre 30 y 120 segundos.
CERRAR-ESPERAR	La conexión se cerró pero sigue esperando un pedido de finalización por parte del usuario local.
SYN-ENVIADA	La conexión local espera una respuesta después de enviar un pedido de conexión. La conexión debe transitar rápidamente por este estado.
SYN_RECIBIDA	La conexión local espera un acuse de recibo que confirme su pedido de conexión. La conexión debe transitar rápidamente por este estado. Conexiones múltiples en el estado SYN_RECIBIDO pueden indicar un ataque TCP SYN.

Las direcciones IP mostradas por **netstat** entran en varias categorías:

Dirección IP	Descripción
127.0.0.1	Esta dirección se refiere al host local o a este equipo.
0.0.0.0	Una dirección global, lo que significa "CUALQUIERA".
Dirección remota	La dirección del dispositivo remoto que tiene una conexión con este equipo.

Tarea 2: Utilizar netstat para examinar la información del protocolo en un equipo host del módulo.

Paso 1: Utilice netstat para ver conexiones existentes.

Desde la ventana Terminal en Tarea 1, arriba, ejecute el comando **netstat –a:**

```
C:\> netstat –a <INTRO>
```

Se mostrará una tabla que lista el protocolo (TCP y UDP), dirección local, dirección remota e información sobre el estado. Allí también figuran las direcciones y los protocolos que se pueden traducir a nombres.

La opción –n obliga a netstat a mostrar el resultado en formato bruto. Desde la ventana Terminal, ejecute el comando **netstat –an:**

```
C:\> netstat –an <INTRO>
```

Utilice la barra de desplazamiento vertical de la ventana para desplazarse hacia atrás y adelante entre los resultados de los dos comandos. Compare los resultados, note cómo los números de puertos bien conocidos cambiaron por nombres.

Anote tres conexiones TCP y tres UDP del resultado de **`netstat -a`** y los números de puertos traducidos correspondientes del resultado de **`netstat -an`**. Si hay menos de tres conexiones que se traducen, anótelo en la tabla.

Conexión	Protocolo	Dirección Local	Dirección extranjera	Estado

Consulte el siguiente resultado **`netstat`**. Un ingeniero de red nuevo sospecha que su equipo host ha sufrido un ataque exterior a los puertos 1070 y 1071. ¿Cómo respondería?

```
C:\> netstat -n
Conexiones activas
Protocolo  Dirección Local        Dirección extranjera    Estado
TCP        127.0.0.1:1070         127.0.0.1:1071          ESTABLISHED
TCP        127.0.0.1:1071         127.0.0.1:1070          ESTABLISHED
C:\>
```

_____

_____

Paso 2: Establezca múltiples conexiones TCP simultáneas y grabe el resultado netstat.

En esta tarea, se realizarán varias conexiones simultáneas con Eagle Server. El comando **`telnet`** autorizado se utilizar para acceder a los servicios de red Eagle Server, además de proveer varios protocolos para examinar con `netstat`.

Abra cuatro ventanas terminales adicionales. Acomode las ventanas de manera tal que estén todas a la vista. Las cuatro ventanas terminales que se utilizarán para las conexiones telnet con Eagle Server pueden ser relativamente pequeñas, más o menos ½ pantalla de ancho por ¼ de pantalla de alto. Las ventanas terminales que se utilizarán para recolectar información de conexión deben ser de ½ pantalla de ancho por la pantalla entera de alto.

Responderán varios servicios de red de Eagle Server a una conexión telnet. Utilizaremos:

- DNS, servidor nombre de dominio, puerto 53
- FTP, servidor FTP, puerto 21
- SMTP, servidor de correo SMTP, puerto 25
- TELNET, servidor Telnet, puerto 23

¿Por qué fallarían los puertos telnet a UDP?

_____

_____

Para cerrar una conexión telnet, presione las teclas <CTRL>] juntas. Eso mostrar el indicador telnet, Microsoft Telnet>. Escriba **quit <INTRO>** para cerrar la sesión.

En la primera ventana terminal telnet, telnet a Eagle Server en puerto 53. En la segunda ventana terminal, telnet en puerto 21. En la tercera ventana terminal, telnet en puerto 25. En la cuarta ventana terminal, telnet en puerto 23. El comando para una conexión telnet en puerto 21 se muestra debajo:

C:\> **telnet eagle-server.example.com 53**

En la ventana terminal más grande, registre las conexiones establecidas con Eagle Server. El resultado debe ser similar a lo siguiente. Si la escritura es lenta, puede que se haya cerrado una conexión antes de que se hayan establecido todas las conexiones. Finalmente, todas las conexiones deben finalizar con la inactividad.

```
Protocolo  Dirección Local        Dirección extranjera    Estado
TCP        192.168.254.1:1688     192.168.254.254:21      ESTABLISHED
TCP        192.168.254.1:1691     192.168.254.254:25      ESTABLISHED
TCP        192.168.254.1:1693     192.168.254.254:53      ESTABLISHED
TCP        192.168.254.1:1694     192.168.254.254:23      ESTABLISHED
```

Tarea 3: Reflexión

La utilidad **netstat** muestra conexiones de red entrantes y salientes (TCP y UDP), información de la tabla de enrutamiento del equipo host y estadísticas de la interfaz.

Tarea 4: Desafío

Cierre bruscamente las sesiones Establecidas (cierre la ventana terminal) y ejecute el comando **netstat -an**. Trate de ver las conexiones en etapas que no sean ESTABLECIDAS.

Tarea 5: Limpieza

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 4.5.2: Protocolos de la capa de Transporte TCP/IP, TCP y UDP

Diagrama de topología

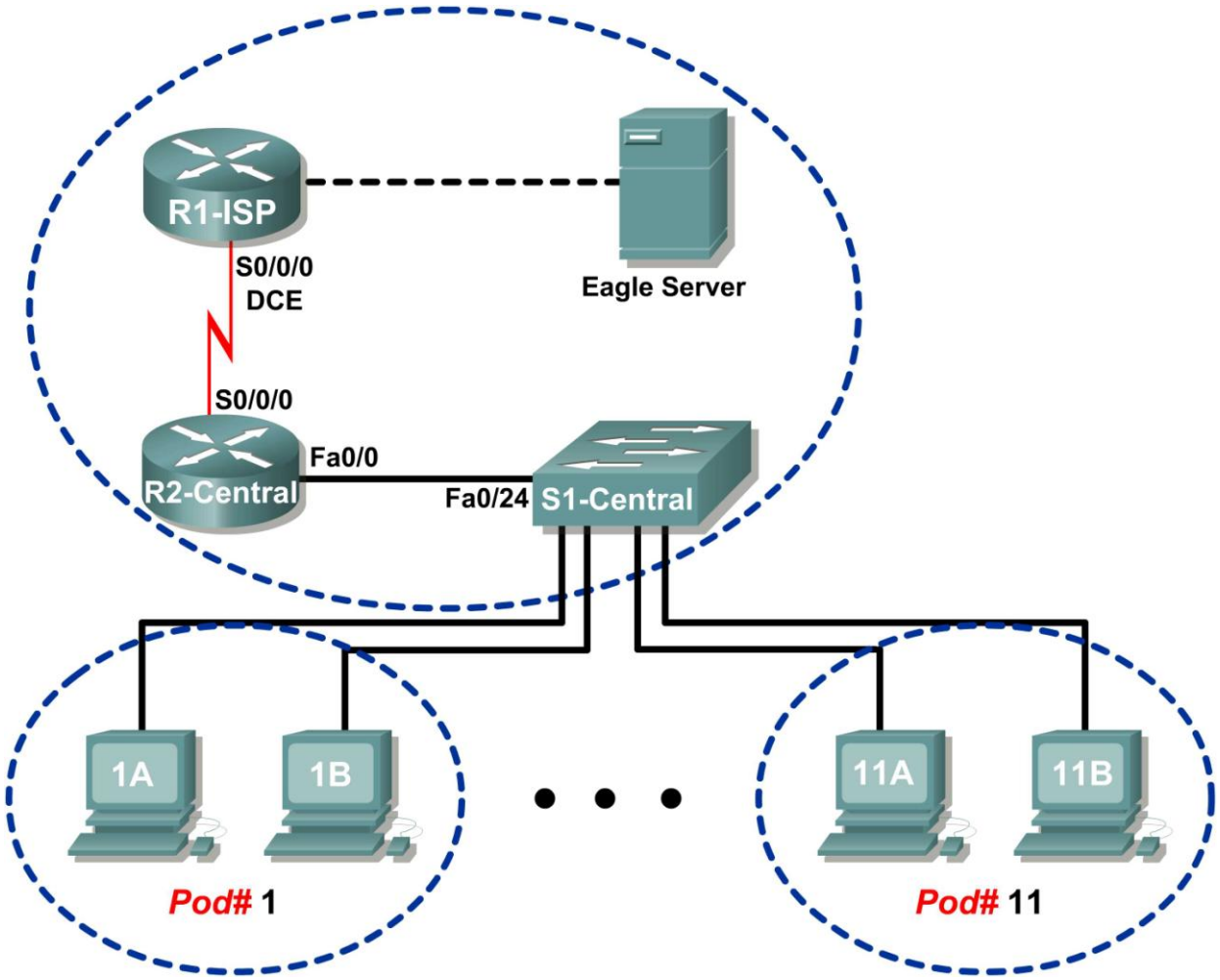


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16.*Pod#.*1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16.*Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

- Identificar campos de encabezado y operación TCP mediante el uso de una captura de sesión FTP Wireshark.
- Identificar campos de encabezado y operación UDP mediante el uso de una captura de sesión TFTP Wireshark.

Información básica

Los dos protocolos en la capa de Transporte TCP/IP son: el Transmission Control Protocol (TCP) definido en RFC 761, en enero de 1980; y el User Datagram Protocol (UDP), definido en RFC 768, en agosto de 1980. Ambos protocolos admiten la comunicación de protocolo de capa superior. Por ejemplo, el TCP se utiliza para proveer soporte de la capa de Transporte para los protocolos HTTP y FTP, entre otros. El UDP provee soporte de la capa de Transporte para servicios de nombres de dominio (DNS) y Trivial File Transfer Protocol (TFTP), entre otros.

La capacidad para entender las partes de los encabezados y de la operación TCP y UDP es una habilidad muy importante para los ingenieros de red.

Escenario

Mediante la captura Wireshark, analizar los campos de encabezado del protocolo UDP y TCP para la transferencia de archivos entre el equipo host y Eagle Server. Si no se cargó Wireshark en el equipo host del módulo, lo puede descargar desde `ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter4/`, archivo `wireshark-setup-0.99.4.exe`.

Las utilidades de Windows de línea de comandos `ftp` y `tftp` se utilizará para conectarse a Eagle Server y descargar archivos.

Tarea 1: Identificar campos de encabezado y operación TCP mediante el uso de una captura de sesión FTP Wireshark.

Paso 1: Capture una sesión FTP.

Las sesiones TCP se controlan y administran debidamente con información que se intercambia en los campos de encabezado TCP. En esta tarea se realizará una sesión FTP con Eagle Server. Cuando finalice, se analizará la captura de sesión. Las computadoras con Windows utilizan al cliente FTP, **`ftp`**, para conectarse al servidor FTP. Una ventana de línea de comandos iniciará la sesión FTP y se descargar el archivo de configuración de texto para S1 central de Eagle Server, `/pub/eagle_labs/eagle1/chapter4/s1-central` al equipo host.

Abra una ventana de línea de comandos con un clic en Iniciar / Ejecutar, escriba cmd y luego presione Aceptar.

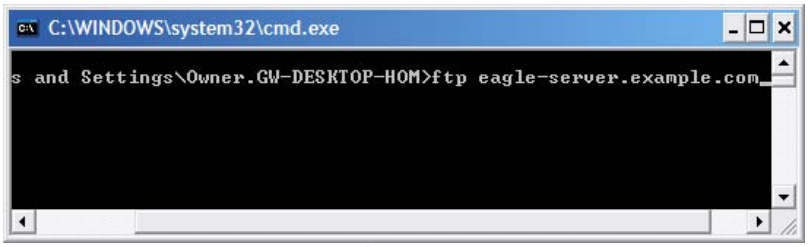


Figura 1. Ventana de línea de comandos.

Deberá abrirse una ventana similar a la Figura 1.

Inicie una captura Wireshark en la interfaz que tenga la dirección IP `172,16.Pod#.[1-2].`

Inicie una conexión FTP con Eagle Server. Escriba el comando:

```
> ftp eagle-server.example.com
```

Cuando se le pida un nombre de usuario, escriba **`anonymous.`** Cuando se le pida una contraseña, presione **`<INTRO>.`**

Cambie el directorio FTP a `/pub/eagle_labs/eagle1/chapter4/`:

```
ftp> cd /pub/eagle_labs/eagle1/chapter4/
```

Descargue el archivo `s1-central`:

```
ftp> get s1-central
```

Cuando termine, finalice las sesiones FTP en cada ventana de línea de comandos con el comando FTP **`quit:`**

```
ftp> quit
```

Cierre la ventana de línea de comandos con el comando **`exit:`**

```
> exit
```

Detenga la captura Wireshark.

Paso 2: Analice los campos TCP.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	192.168.254.254	TCP	1052 > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.000568	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.000610	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.004818	192.168.254.254	172.16.1.1	FTP	Response: 220 Welcome to the eagle-server FTP service.
5	0.115430	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=1 Ack=47 Win=64194 Len=0
6	8.223541	172.16.1.1	192.168.254.254	FTP	Request: USER anonymous
7	8.224089	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [ACK] Seq=47 Ack=17 Win=5840 Len=0
8	8.224126	192.168.254.254	172.16.1.1	FTP	Response: 331 Please specify the password.
9	8.327214	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=17 Ack=81 Win=64160 Len=0
10	9.517629	172.16.1.1	192.168.254.254	FTP	Request: PASS
11	9.519135	192.168.254.254	172.16.1.1	FTP	Response: 230 Login successful.
12	9.629097	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=24 Ack=104 Win=64137 Len=0
13	32.365752	172.16.1.1	192.168.254.254	FTP	Request: CWD /pub/eagle_labs/eagle1/chapter4
14	32.366375	192.168.254.254	172.16.1.1	FTP	Response: 250 Directory successfully changed.
15	32.376653	172.16.1.1	192.168.254.254	FTP	Request: PORT 172,16,1,1,4,33
16	32.377165	192.168.254.254	172.16.1.1	FTP	Response: 200 PORT command successful. Consider using PASV.
17	32.381726	172.16.1.1	192.168.254.254	FTP	Request: RETR s1-central
18	32.382337	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [SYN] Seq=0 Len=0 MSS=1460 TSV=4755496 TSER=0 WS=2
19	32.382398	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
20	32.382777	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=4755496 TSER=0
21	32.382891	192.168.254.254	172.16.1.1	FTP	Response: 150 Opening BINARY mode data connection for s1-central (3100 bytes).
22	32.383528	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 1448 bytes
23	32.383589	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 1448 bytes
24	32.383631	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [ACK] Seq=1 Ack=2897 Win=64240 Len=0 TSV=36854 TSER=4755496
25	32.383736	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 204 bytes
26	32.383753	192.168.254.254	172.16.1.1	FTP	Response: 226 File send OK.
27	32.383773	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=100 Ack=281 Win=63960 Len=0
28	32.383779	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [FIN, ACK] Seq=3101 Ack=1 Win=5840 Len=0 TSV=4755496 TSER=0
29	32.383805	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [ACK] Seq=1 Ack=3102 Win=64036 Len=0 TSV=36854 TSER=4755496
30	32.389457	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [FIN, ACK] Seq=1 Ack=3102 Win=64036 Len=0 TSV=36854 TSER=4755496
31	32.389845	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [ACK] Seq=3102 Ack=2 Win=5840 Len=0 TSV=4755503 TSER=36854
32	34.438952	172.16.1.1	192.168.254.254	FTP	Request: QUIT
33	34.439532	192.168.254.254	172.16.1.1	FTP	Response: 221 Goodbye.
34	34.439893	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [FIN, ACK] Seq=295 Ack=106 Win=5840 Len=0
35	34.439934	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=106 Ack=296 Win=63946 Len=0
36	34.442705	172.16.1.1	192.168.254.254	TCP	1052 > ftp [FIN, ACK] Seq=106 Ack=296 Win=63946 Len=0
37	34.443144	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [ACK] Seq=296 Ack=107 Win=5840 Len=0

Figura 2. Captura FTP.

Cambie a las ventanas de captura Wireshark. La ventana superior contiene resumen de información para cada registro capturado. La captura realizada por el estudiante debe ser similar a la captura que se muestra en la Figura 2. Antes de profundizar en los detalles del paquete TCP, se necesita una explicación del resumen de información. Cuando el cliente FTP está conectado al servidor FTP, el protocolo TCP de la capa de Transporte creó una sesión confiable. El TCP se utiliza en forma continua durante una sesión para controlar la entrega del datagrama, verificar la llegada del datagrama y administrar el tamaño de la ventana. Por cada intercambio de datos entre el cliente FTP y el servidor FTP, se inicia una nueva sesión TCP. Al término de la transferencia de datos, se cierra la sesión TCP. Finalmente, cuando la sesión FTP finaliza, TCP realiza un cierre y terminación ordenados.

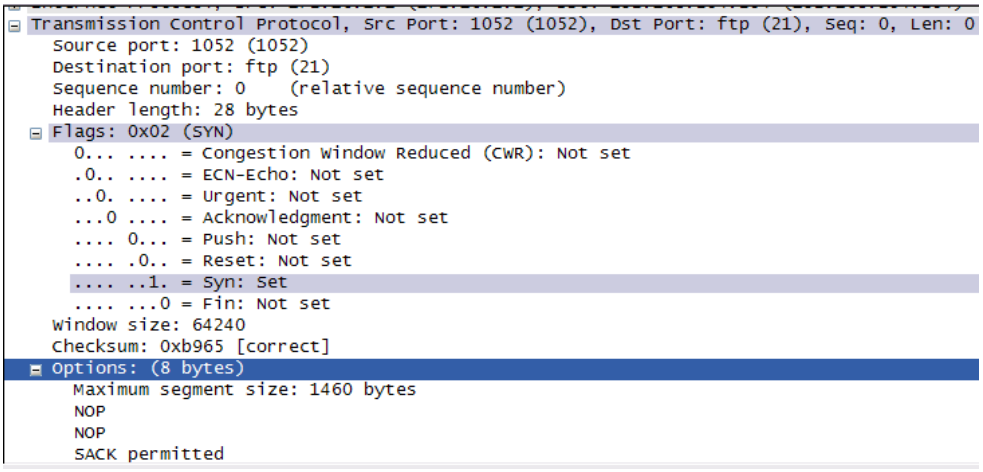


Figura 3. Captura Wireshark de un datagrama TCP.

Hay información TCP detallada disponible en la ventana del medio, en Wireshark. Resalte el primer datagrama TCP del equipo host y mueva el puntero del mouse hacia la ventana del medio. Puede ser necesario ajustar la ventana del medio y expandir el registro TCP con un clic en la casilla de expansión de protocolo. El datagrama TCP expandido debe ser similar a la Figura 3.

¿Cómo se identifica el primer datagrama en una sesión TCP?

_____

_____

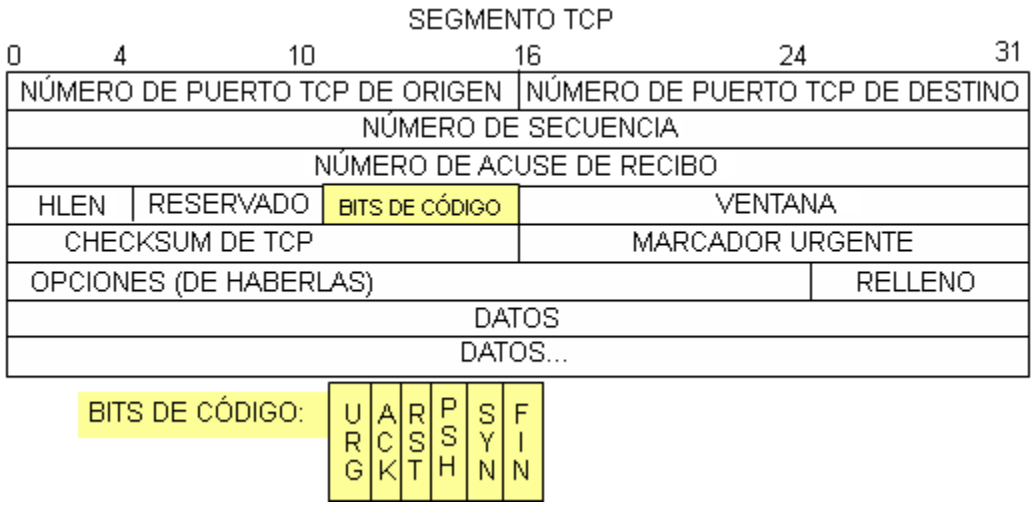


Figura 4. Campos del paquete TCP.

Observe la Figura 4, un diagrama de datagrama TCP. Se provee a los estudiantes una explicación de cada campo para refrescarles la memoria:

- **El número de puerto de origen TCP** pertenece al host de la sesión TCP que inició una conexión. Generalmente el valor es un valor aleatorio superior a 1023.
- **El número de puerto de destino** se utiliza para identificar el protocolo de capa superior o la aplicación en un sitio remoto. Los valores dentro del intervalo 0 – 1023 representan a los llamados "puertos bien conocidos" y están asociados con servicios y aplicaciones conocidos (como se describe en RFC 1700, telnet, File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), etc.). La combinación de campo cuádruple (dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino) identifica de manera exclusiva la sesión, tanto del emisor como del receptor.
- **El número de secuencia** especifica el número del último octeto en un segmento.
- **El número de acuse de recibo** especifica el próximo octeto que espera el receptor.
- **Los bits de código** tienen un significado especial en la administración de sesión y en el tratamiento de los segmentos. Entre los valores interesentes se encuentran:
  - ACK (Acuse de recibo de un segmento),
  - SYN (Sincronizar, configurar sólo cuando una sesión TCP nueva se negocia durante un protocolo de enlace de tres vías).
  - FIN (Finalizar, solicitud para cerrar la sesión TCP).
- **El tamaño de la ventana** es el valor de la ventana deslizante; cuántos octetos se pueden enviar antes de esperar un acuse de recibo.
- **El puntero urgente** se utiliza sólo con un señalizador URG (Urgente) cuando el emisor necesita enviar datos urgentes al receptor.
- **Opciones:** La única opción definida actualmente es el tamaño de segmento TCP máximo (valor opcional).

Utilice la captura Wireshark del inicio de la primera sesión TCP (bit SYN fijado en 1) para completar la información acerca del encabezado TCP.

Del equipo host del módulo a Eagle Server (sólo el bit SYN se fija en 1):

Dirección IP de origen: 172.16.___.___	
Dirección IP destino: _____	
Número de puerto de origen: _____	
Número de puerto de destino: _____	
Número de secuencia: _____	
Número de acuse de recibo: _____	
Longitud del encabezado: _____	
Tamaño de la ventana: _____	

De Eagle Server al equipo host del módulo (sólo los bits SYN y ACK se fijan en 1):

Dirección IP de origen: _____	
Dirección IP destino: 172.16.___.___	
Número de puerto de origen: _____	
Número de puerto de destino: _____	
Número de secuencia: _____	
Número de acuse de recibo: _____	
Longitud del encabezado: _____	
Tamaño de la ventana: _____	

Del equipo host del módulo a Eagle Server (sólo el bit ACK se fija en 1):

Dirección IP de origen: 172.16.___.___	
Dirección IP destino: _____	
Número de puerto de origen: _____	
Número de puerto de destino: _____	
Número de secuencia: _____	
Número de acuse de recibo: _____	
Longitud del encabezado: _____	
Tamaño de la ventana: _____	

A excepción de la sesión TCP iniciada cuando se realizó una transferencia de datos, ¿cuántos otros datagramas TCP contienen un bit SYN?

_____

_____

Los atacantes se aprovechan del protocolo de enlace de tres vías al iniciar una conexión “half-open”. En esta secuencia la sesión TCP inicial envía un datagrama TCP con el bit SYN establecido y el receptor envía un datagrama TCP relacionado con los bits SYN ACK establecidos. Un bit ACK final no se envía nunca para finalizar el intercambio TCP. En cambio, se inicia una conexión TCP nueva de manera half-open. Con suficientes sesiones TCP en estado half-open, el equipo receptor agotará recursos

y colapsará. Un colapso puede incluir una pérdida de servicios de red o un daño en el sistema operativo. De cualquier modo, el atacante gana. El servicio de red se ha detenido en el receptor. Éste es un ejemplo de ataque de denegación de servicio (DoS).

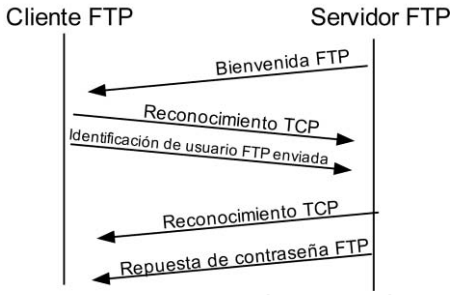


Figura 5. Administración de sesión TCP.

El cliente y el servidor FTP se comunican uno con el otro sin saber y sin importarles que TCP tenga el control y manejo de la sesión. Cuando el servidor FTP envía una Respuesta: 220 al cliente FTP, la sesión TCP del cliente FTP envía un acuse de recibo a la sesión TCP en Eagle Server. Esta secuencia se muestra en la Figura 5 y es visible en la captura Wireshark.

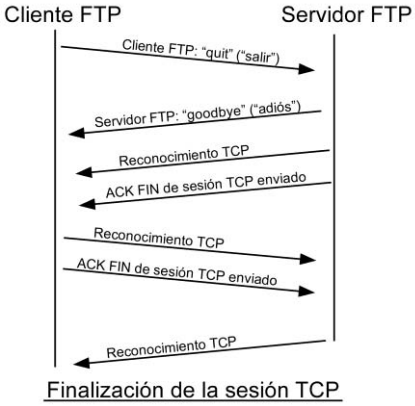


Figura 6. Terminación de la sesión TCP ordenada.

Cuando la sesión FTP terminó, el cliente FTP envía un comando para "`salir`". El servidor FTP acusa recibo de la terminación FTP con una `Respuesta 221 Adiós`. En este momento la sesión TCP del servidor FTP envía un datagrama TCP al cliente FTP que anuncia la terminación de la sesión TCP. La sesión TCP del cliente FTP acusa recibo de la recepción del datagrama de terminación y luego envía su propia terminación de sesión TCP. Cuando quien originó la terminación TCP (servidor FTP) recibe una terminación duplicada, se envía un datagrama ACK para acusar recibo de la terminación y se cierra la sesión TCP. Esta secuencia se muestra en la Figura 6 y es visible en la captura Wireshark.

Sin una terminación ordenada, como por ejemplo cuando se interrumpe la conexión, las sesiones TCP esperarán un cierto período de tiempo hasta cerrarse. El valor de límite de tiempo de espera predeterminado varía, pero normalmente es de 5 minutos.

Tarea 2: Identificar campos de encabezado y operación UDP mediante el uso de una captura de sesión TFTP Wireshark.

Paso 1: Capture una sesión TFTP.

Siga el procedimiento de la Tarea 1 de arriba y abra una ventana de línea de comandos. El comando TFTP tiene una sintaxis diferente a la de FTP. Por ejemplo: no hay autenticación. También, hay sólo dos comandos: **`get`**, para recuperar un archivo y **`put`**, para enviar un archivo.

```
>tftp –help

Transfiere los archivos a y desde un equipo remoto con el servicio TFTP en
funcionamiento.

TFTP [-i] host [GET | PUT] origen [destino]

        -i        Especifica el modo de transferencia binario (llamado también
                  octeto). En modo binario el archivo se transfiere
                  literalmente, byte a byte. Use este modo cuando
                  transfiera archivos binarios.
        host      Especifica el host remoto o local.
        GET       Transfiere el archivo destino en el host remoto al
                  archivo origen en el host local.
        PUT       Transfiere el archivo origen en el host local al
                  archivo destino en el host remoto.
        origen    Especifica el archivo a transferir.
      destino     Especifica dónde transferir el archivo.
```

Tabla 1. Sintaxis TFTP para un cliente TFTP Windows.

La Tabla 1 contiene sintaxis de cliente TFTP Windows. El servidor TFTP tiene su propio directorio en Eagle Server, `/tftpboot`, que es diferente de la estructura del directorio admitido por el servidor FTP. No se admite ninguna autenticación.

Inicie una captura Wireshark, luego descargue el archivo de configuración `s1-central` de Eagle Server con el cliente TFTP Windows. El comando y la sintaxis para realizar esto se muestran debajo:

```
>tftp eagle-server.example.com get s1-central
```

Paso 2: Analice los campos UDP.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	192.168.254.254	TFTP	Read Request, File: s1-central, Transfer type: netascii
2	0.003171	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 1
3	0.003314	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 1
4	0.003962	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 2
5	0.004021	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 2
6	0.004615	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 3
7	0.004673	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 3
8	0.005274	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 4
9	0.005332	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 4
10	0.005930	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 5
11	0.005989	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 5
12	0.006588	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 6
13	0.006644	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 6
14	0.007078	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 7 (last)
15	0.007131	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 7

Figura 7. Captura de resumen de una sesión UDP.

Cambie a las ventanas de captura Wireshark. La captura realizada por el estudiante debe ser similar a la captura que se muestra en la Figura 7. Se utilizará una transferencia TFTP para analizar la operación de capa de Transporte UDP.

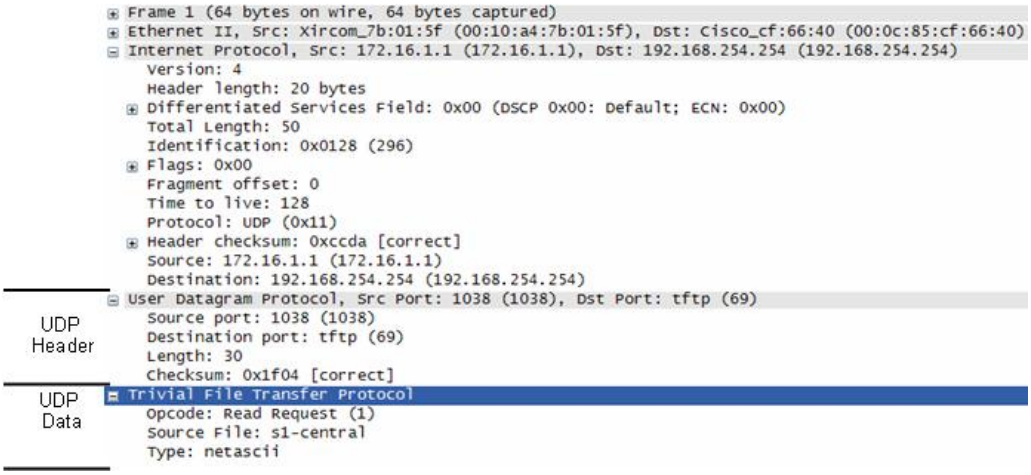


Figura 8. Captura Wireshark de un datagrama UDP.

Hay información UDP detallada disponible en la ventana del medio en Wireshark. Resalte el primer datagrama UDP del equipo host y mueva el puntero del mouse hacia la ventana del medio. Puede ser necesario ajustar la ventana del medio y expandir el registro UDP con un clic en la casilla de expansión de protocolo. El datagrama UDP expandido debe ser similar a la Figura 8.

SEGMENTO UDP

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

Figura 9. Formato UDP.

Observe la Figura 9, un diagrama de datagrama UDP. La información del encabezado está dispersa comparada con la del datagrama TCP. Sin embargo hay similitudes. Cada datagrama UDP es identificado por el puerto de origen UDP y el puerto de destino UDP.

Utilice la captura Wireshark del primer datagrama UDP para completar la información acerca del encabezado UDP. El valor de la checksum es un valor hexadecimal (base 16) indicado por el código anterior 0x:

Dirección IP de origen: 172.16.___.___	
Dirección IP destino: _____	
Número de puerto de origen: _____	
Número de puerto de destino: _____	
Longitud de mensaje UDP: _____	
Checksum de UDP: _____	

¿Cómo verifica UDP la integridad del datagrama?

_____

_____

Examine el primer paquete devuelto por Eagle Server. Complete la información acerca del encabezado UDP:

Dirección IP de origen:	
Dirección IP destino: 172.16.___.___	
Número de puerto de origen: _____	
Número de puerto de destino: _____	
Longitud de mensaje UDP: _____	
Checksum de UDP: 0x_____	

Observe que el datagrama UDP devuelto tiene un puerto de origen UDP diferente, pero este puerto de origen es utilizado para el resto de la transferencia TFTP. Dado que no hay una conexión confiable, para mantener la transferencia TFTP, sólo se utiliza el puerto de origen usado para comenzar la sesión TFTP.

Tarea 5: Reflexión

Esta práctica de laboratorio brindó a los estudiantes la oportunidad de analizar las operaciones de protocolo UDP y TCP de sesiones TFTP y FTP capturadas. TCP administra la comunicación de manera muy diferente a UDP, pero la confiabilidad y garantía ofrecidas requieren un control adicional sobre el canal de comunicación. UDP tiene menos sobrecarga y control, y el protocolo de capa superior debe proveer algún tipo de control de acuse de recibo. Sin embargo, ambos protocolos transportan datos entre clientes y servidores con el uso de los protocolos de la capa de Aplicación y son correctos para el protocolo de capa superior que cada uno admite.

Tarea 6: Desafío

Debido a que ni FTP ni TFTP son protocolos seguros, todos los datos transferidos se envían en texto sin cifrar. Esto incluye ID de usuario, contraseñas o contenidos de archivo en texto sin cifrar. Si analiza la sesión FTP de capa superior identificará rápidamente el id de usuario, contraseña y contraseñas de archivo de configuración. El examen de datos TFTP de capa superior es un poco más complicado, pero se puede examinar el campo de datos y extraer información de configuración de id de usuario y contraseña.

Tarea 7: Limpieza

Durante esta práctica de laboratorio se transfirieron varios archivos al equipo host y se deben eliminar.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 4.5.3: Examen de protocolos de la capa de transporte y aplicación

Diagrama de topología

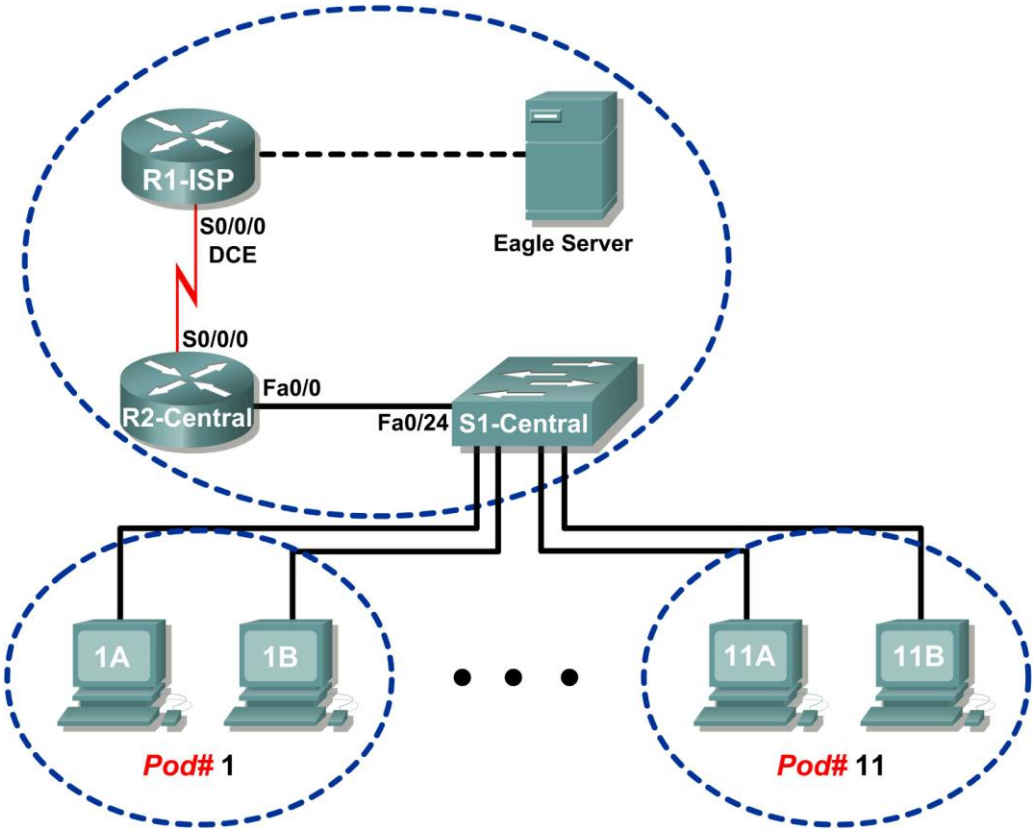


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	**S0/0/0**	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	**S0/0/0**	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Configurar la computadora host para capturar protocolos de la capa de aplicación.
- Capturar y analizar la comunicación HTTP entre la computadora host del módulo y un servidor Web.
- Capturar y analizar la comunicación FTP entre la computadora host del módulo y un servidor FTP.
- Observar los canales TCP para establecer y administrar la comunicación con conexiones HTTP y FTP.

Información básica

La función principal de la capa de transporte es mantener un registro de las conversaciones de múltiples aplicaciones en el mismo host. Sin embargo, cada aplicación tiene determinados requisitos para sus datos y, por lo tanto, se han desarrollado diferentes protocolos de transporte para que cumplan con estos requisitos. Los protocolos de la capa de aplicación definen la comunicación entre servicios de red, como un servidor Web y un cliente y un servidor FTP y un cliente. Los clientes inician la comunicación con el servidor adecuado y el servidor responde al cliente. Para cada servicio de red existe un servidor determinado que escucha, en un puerto determinado, las conexiones del cliente. Puede haber diversos servidores en el mismo dispositivo final. Un usuario puede abrir diferentes aplicaciones del cliente para el mismo servidor, pero cada cliente se comunica, en forma exclusiva, con una sesión establecida entre el cliente y el servidor.

Los protocolos de la capa de aplicación se basan en los protocolos TCP/IP de menor nivel, como TCP o UDP. Esta práctica de laboratorio examina dos protocolos populares de la capa de aplicación, HTTP y FTP, y la manera en que los protocolos de la capa de transporte, TCP y UDP, administran el canal de comunicación. También se examinan las solicitudes más comunes de los clientes y las correspondientes respuestas del servidor.

Escenario

En esta práctica de laboratorio se utilizarán las aplicaciones del cliente para conectarse a los servicios de red del eagle server. El usuario monitorea la comunicación con Wireshark y analiza los paquetes capturados.

Se utiliza un explorador Web como Internet Explorer o Firefox para conectarse al servicio de red del eagle server. Eagle server tiene varios servicios de red previamente configurados, como el HTTP, que esperan responder las solicitudes del cliente.

También se utilizará el explorador Web para examinar el protocolo FTP y el cliente de línea de comando FTP. El ejercicio demostrará que, aunque los clientes pueden diferir, la comunicación subyacente con el servidor sigue siendo la misma.

Tarea 1: Configuración de la computadora host del módulo para capturar protocolos de la capa de aplicación.

La práctica de laboratorio debe estar configurada como se muestra en el Diagrama de topología y en la tabla de dirección lógica. En caso contrario, pídale ayuda al instructor antes de continuar.

Paso 1: Descargar e instalar wireshark.

Figura 1. Descarga de FTP para Wireshark

Si Wireshark no está instalado en la computadora host del módulo, puede descargarse desde eagle-server.example.com. Vea la Figura 1. El URL de descarga es: ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3.

1. Haga clic con el botón derecho del mouse sobre el nombre del archivo wireshark. Luego, guarde el archivo en la computadora host del módulo.
2. Cuando el archivo se haya descargado, haga doble clic en el nombre del archivo e instale Wireshark con las configuraciones predeterminadas.

Paso 2: Iniciar Wireshark y configurar la Interfaz de captura.

1. Inicie Wireshark desde **Inicio > Todos los programas > Wireshark > Wireshark**.
2. Cuando se muestra la ventana que se abre, establezca la Interfaz de captura correcta. La interfaz correcta es la interfaz con la dirección IP de la computadora host del módulo. Vea la Figura 2.

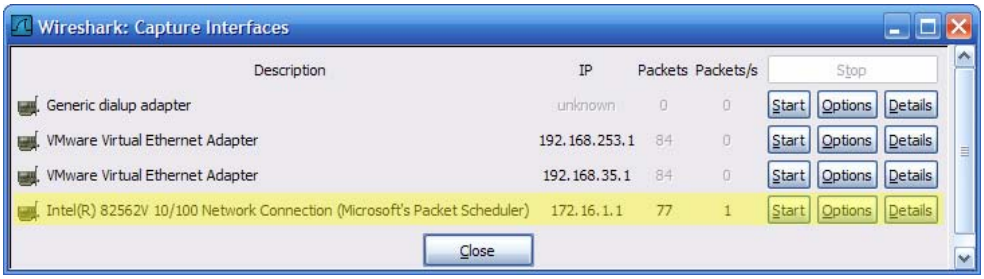


Figura 2: Ventana de captura de interfaz de Wireshark

Wireshark puede iniciarse haciendo clic en el botón **Inicio** de la interfaz. Después, la interfaz se utiliza como predeterminada y no se la necesita cambiar.

Wireshark debe comenzar a registrar datos.

3. Detenga Wireshark por ahora. Wireshark se utilizará en las siguientes tareas.

Tarea 2: Captura y análisis de la comunicación HTTP entre la computadora host del módulo y un servidor Web.

HTTP es un protocolo de capa de aplicación que depende de los protocolos de menor nivel, como TCP, para establecer y administrar el canal de comunicación. HTTP versión 1.1 se define en RFC 2616, en el año 1999. Esta parte de la práctica de laboratorio demostrará cómo las sesiones entre múltiples clientes Web y el servidor Web se mantienen separadas.

Paso 1: Iniciar las capturas de Wireshark.

Inicie una captura de Wireshark. Wireshark mostrará capturas basadas en el tipo de paquete.

Paso 2: Iniciar el explorador Web del host del módulo.

1. Con un explorador Web, como Internet Explorer o Firefox, conéctese al URL http://eagle-server.example.com. Se muestra una página Web similar a la de la Figura 3. No cierre este explorador Web hasta que se le indique.

Figura 3: Explorador Web conectado al servidor Web

2. Haga clic en el botón **Actualizar** del explorador Web. No debe haber cambios en la pantalla del cliente Web.
3. Abra un segundo explorador Web y conéctese al URL http://eagle-server.example.com/page2.html. En la pantalla aparece una página Web diferente.

   No cierre ningún explorador hasta que la captura de Wireshark se detenga.

Paso 3: Detener las capturas de Wireshark y analizar los datos capturados.

1. Detenga las capturas de Wireshark.
2. Cierre los exploradores Web.

Se muestran los datos Wireshark resultantes. En el paso 2, se crearon al menos tres sesiones HTTP. La primera sesión HTTP comenzó con una conexión a http://eagle-server.example.com. La segunda sesión se produjo con una actualización. La tercera sesión se produjo cuando el segundo explorador Web entró a http://eagle-server.example.com/page2.html.

No.	Time	Source	Destination	Protocol	Info
10	10.168217	172.16.1.2	192.168.254.254	TCP	1056 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.170734	192.168.254.254	172.16.1.2	TCP	http > 1056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
12	10.170767	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	10.171086	172.16.1.2	192.168.254.254	HTTP	GET / HTTP/1.1
14	10.171625	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=1 Ack=208 Win=6432 Len=0
15	10.172518	192.168.254.254	172.16.1.2	HTTP	HTTP/1.1 200 OK (text/html)
16	10.172540	192.168.254.254	172.16.1.2	TCP	http > 1056 [FIN, ACK] Seq=448 Ack=208 Win=6432 Len=0
17	10.172567	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=208 Ack=449 Win=63793 Len=0
18	10.174196	172.16.1.2	192.168.254.254	TCP	1056 > http [FIN, ACK] Seq=208 Ack=449 Win=63793 Len=0
19	10.174661	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=449 Ack=209 Win=6432 Len=0

Figura 4: Sesión de HTTP capturada

En la Figura 4 se muestra un ejemplo de una sesión HTTP capturada. Antes de que la HTTP pueda comenzar, se debe crear una sesión TCP. Esto se ve en las tres primeras líneas de sesión, números 10, 11 y 12. Utilice los resultados de captura de Wireshark o similares para responder las siguientes preguntas:

3. Complete la siguiente tabla con la información presentada en la sesión HTTP:

Dirección IP del explorador Web	
Dirección IP del servidor Web	
Protocolo de la capa de transporte (UDP/TCP)	
Número de puerto del explorador Web	
Número de puerto del servidor Web	

4. ¿Qué computadora inició la sesión HTTP y cómo lo hizo?

_____

_____

5. ¿Qué computadora señaló inicialmente un fin a la sesión HTTP y cómo lo hizo?

_____

_____

6. Resalte la primera línea del protocolo HTTP, una solicitud **GET** (Obtener) del explorador Web. En la Figura 4 de arriba, la solicitud **GET** está en la línea 13. Vaya a la segunda ventana de Wireshark (la del medio) para examinar los protocolos en capas. Si es necesario, expanda los campos.
7. ¿Qué protocolo se lleva (encapsulado) dentro del segmento TCP?

_____

8. Expanda el último registro de protocolo y cualquier subcampo. Ésta es la información real enviada al servidor Web. Complete la siguiente tabla utilizando la información del protocolo.

Versión del protocolo	
Método de solicitud	
* Solicitud URI	
Idioma	

* La solicitud URI es la ruta para el documento solicitado. En el primer explorador, la ruta es el directorio raíz del servidor Web. Aunque no se solicitó ninguna página, algunos servidores Web están configurados para mostrar un archivo predeterminado, si está disponible.

El servidor Web responde con el próximo paquete HTTP. En la Figura 4 se puede ver en la línea 15. Una respuesta para el explorador Web es posible porque el servidor Web (1) comprende el tipo de solicitud y (2) tiene que devolver un archivo. Los crackers a veces envían solicitudes

desconocidas o dañadas a servidores Web para intentar detener el servidor o poder acceder a la línea de comando del servidor. Además, una solicitud para una página Web desconocida da como resultado un mensaje de error.

9. Resalte la respuesta del servidor Web y luego vaya a la segunda ventana (la del medio). Abra todos los subcampos de HTTP colapsados. Observe la información que devuelve el servidor. En esta respuesta, sólo hay unas pocas líneas de texto (las respuestas del servidor Web pueden contener miles o millones de bytes). El explorador Web comprende los datos de la ventana del explorador y los formatea correctamente. .

10. ¿Cuál es la respuesta del servidor Web para la solicitud **GET** del cliente Web?

_____

11. ¿Qué significa esta respuesta?

_____

12. Desplácese hacia abajo de la ventana superior de Wireshark hasta que se muestre la segunda sesión de HTTP, actualizada. La Figura 5 muestra una captura de muestra.

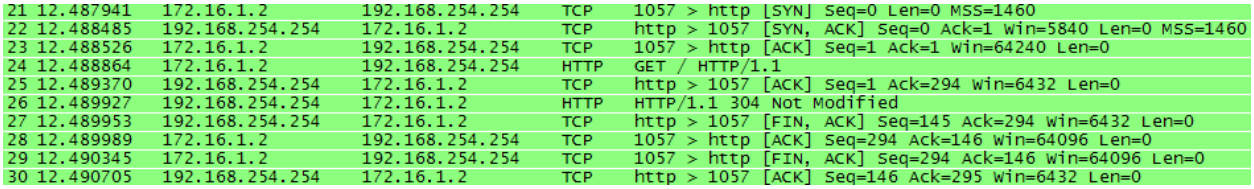


Figura 5: Sesión HTTP capturada para actualizar

El significado de la acción de actualización se encuentra en la respuesta del servidor, `304 Not Modified` (304 No modificado). Con un paquete simple devuelto para la solicitud inicial de **GET** y para la actualización, el ancho de banda utilizada es mínimo. Sin embargo, para una respuesta inicial que contenga millones de bytes, un simple paquete de respuesta puede generar un significativo ahorro de ancho de banda.

Debido a que esta página Web ha sido guardada en la caché del cliente Web, la solicitud **GET** contenía las siguientes instrucciones adicionales para el servidor Web.

```
If-modified-since: Fri, 26 Jan 2007 06:19:33 GMT\r\n
If-None-Match "98072-b8-82da8740"\r\n  <-  page tag number (ETAG)
```

13. ¿Cuál es la respuesta ETAG del servidor Web?

_____

Tarea 3: Captura y análisis de la comunicación FTP entre la computadora host del módulo y un servidor Web.

El protocolo de la capa de aplicación FTP ha recibido una revisión significativa desde que apareció por primera vez en RFC 114, en 1971. La versión 5.1 de FTP se define en RFC 959, de octubre de 1985.

El explorador Web conocido no sólo puede usarse para comunicarse con el servidor HTTP. En esta tarea, el explorador Web y una utilidad de línea de comando FTP se utilizan para descargar datos desde un servidor FTP.

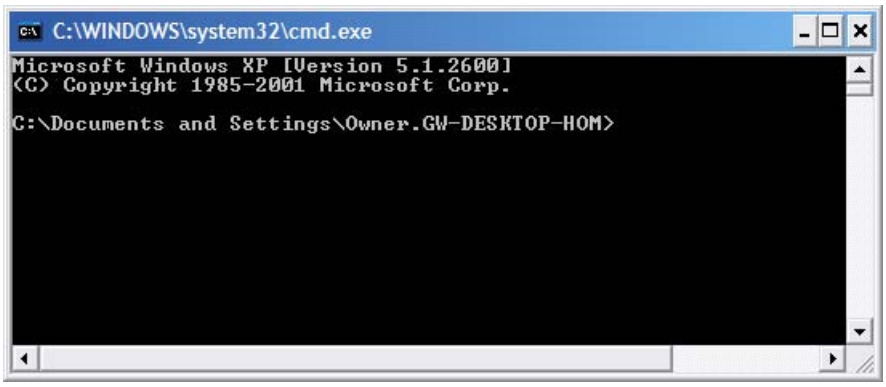


Figura 6: Pantalla de línea de comandos de Windows

Para prepararse para esta tarea, abra una línea de comandos en la computadora host del módulo. Esto puede lograrse haciendo clic en **Inicio > Ejecutar** y luego escribiendo **CMD** y haciendo clic en **Aceptar**. Se muestra una pantalla similar a la de la Figura 6.

Paso 1: Iniciar las capturas de Wireshark.

Si es necesario, consulte la Tarea 1, Paso 2, para abrir Wireshark.

Paso 2: Iniciar el cliente FTP de la línea de comandos host del módulo.

1. Inicie una sesión FTP de una computadora host del módulo con el servidor FTP, usando la utilidad del cliente FTP de Windows. Para autenticar, utilice la identificación de usuario **anonymous** (anónima). Como respuesta a la petición de contraseña, presione <**ENTER**>.

```
> ftp eagle-server.example.com
Conectado a eagle-server.example.com.
220 Bienvenido al servicio FTP de eagle-server.
Usuario (eagle-server.example.com:(ninguno)): anónimo
331 Especifique la contraseña.
Contraseña: <INTRO>
230 Conexión exitosa.
```

2. El indicador del cliente FTP es `ftp>`. Esto significa que el cliente FTP espera un comando para enviar al servidor FTP. Para ver una lista de los comandos del cliente FTP, escriba **`help`** **`<ENTER>`** (ayuda, <aceptar>):

```
ftp> help
Los comandos se pueden abreviar.  Comandos:

!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

Desafortunadamente, la gran cantidad de comandos del cliente FTP dificulta el uso de la utilidad de la línea de comandos para un principiante. Sólo usaremos unos pocos comandos para la evaluación de Wireshark.

3. Escriba el comando **dir** para mostrar los contenidos actuales del directorio:

```
ftp> dir
200 Comando PORT command exitoso. Considere usar PASV.
150 Aquí aparece el listado de directorio.
drwxr-xr-x    3 0        0            4096 Jan 12 04:32 pub
```

El cliente FTP es un directorio raíz del servidor FTP. Éste no es el directorio raíz real del servidor; sólo el punto más importante al que puede acceder el usuario **anonymous.** El usuario **anonymous** ha sido ubicado en una root jail, prohibiendo el acceso fuera del directorio actual.

4. Sin embargo, los subdirectorios se pueden recorrer y los archivos se pueden transferir a la computadora host del módulo. Vaya al directorio pub/eagle_labs/eagle1/chapter2, descargue un archivo y salga.

```
ftp> cd pub/eagle_labs/eagle1/chapter2
250 Se cambió exitosamente el directorio.
ftp> dir
200 Comando PORT command exitoso. Considere usar PASV.
150 Aquí aparece el listado de directorio.
-rw-r--r--  1 0 100     5853 Jan 12 04:26 ftptoeagle-server.pcap
-rw-r--r--  1 0 100     4493 Jan 12 04:27 http to eagle-server.pcap
-rw-r--r--  1 0 100     1486 Jan 12 04:27 ping to 192.168.254.254.pcap
-rw-r--r--  1 0 100 15163750 Jan 12 04:30 wireshark-setup-0.99.4.exe
226 Se envió correctamente el directorio.
ftp: 333 bytes received in 0.04Seconds 8.12Kbytes/sec.
ftp> get "ftptoeagle-server.pcap"
200 Comando PORT command exitoso. Considere usar PASV.
150 Abriendo la conexión de datos con el modo BINARIO para ftptoeagle-
server.pcap (5853 bytes).
226 Se envió correctamente el archivo.
ftp: 5853 bytes recibidos en 0.34 segundos 17.21 Kbytes/seg.
ftp> quit
221 Adiós.
```

5. Cierre la ventana de la línea de comandos con el comando exit (salir).
6. Detenga las capturas de Wireshark y guárdelas como FTP_Command_Line_Client.

Paso 3: Iniciar el explorador Web del host del módulo.

1. Inicie nuevamente las capturas Wireshark.

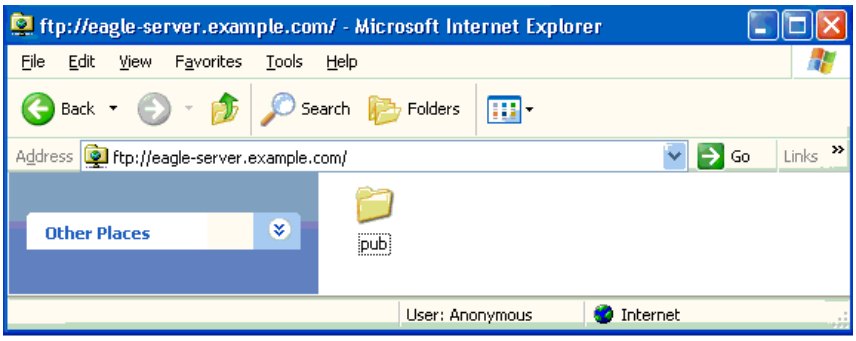
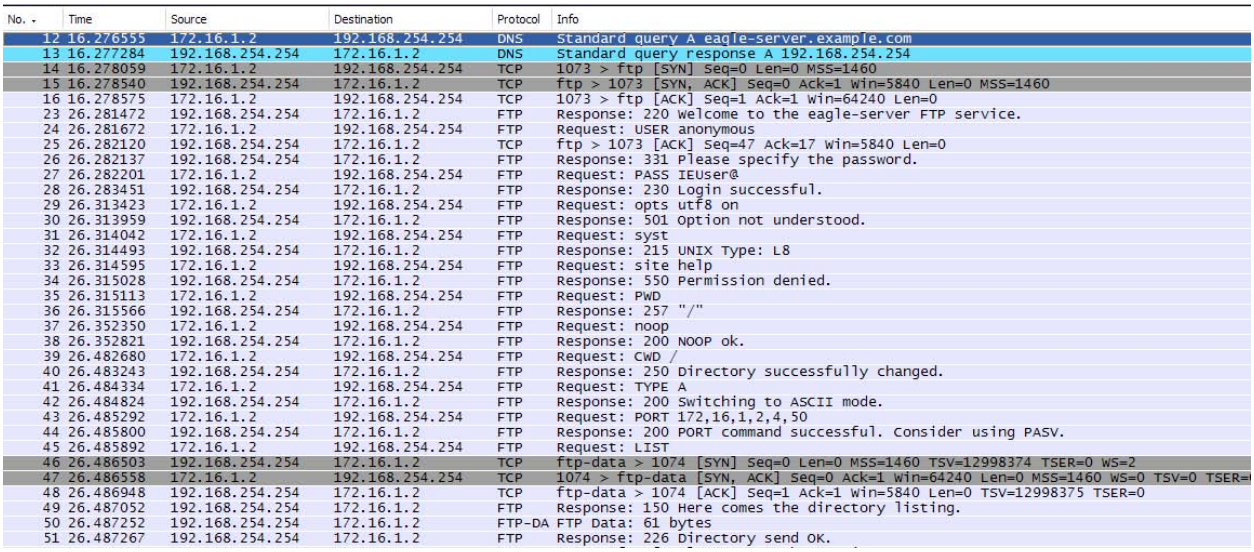


Figura 7. Explorador Web utilizado como un cliente FTP

2. Abra un explorador Web como lo muestra la Figura 7 y escriba el URL ftp://eagle-server.example.com. Se abre una ventana del explorador que muestra el directorio pub. Además, el explorador Web se registró en el servidor FTP como usuario Anonymous, como se muestra en la parte inferior de la captura de la pantalla.
3. Utilizando el explorador, vaya por los directorios hasta la ruta URL `pub/eagle-labs/eagle1/chapter2`. Haga doble clic en el archivo `ftptoeagle-server.pcap` y guarde el archivo.
4. Al finalizar, cierre el explorador Web.
5. Detenga las capturas de Wireshark y guárdelas como FTP_Web_Browser_Client.

Paso 4: Detener las capturas de Wireshark y analizar los datos capturados.

1. Si aún no está abierta, abra la captura de Wireshark FTP_Web_Browser_Client.
2. En la ventana superior de Wireshark, seleccione la captura FTP que es la primera transmisión del protocolo FTP. Respuesta: 220. En la Figura 8, es la línea número 23.



No.	Time	Source	Destination	Protocol	Info
12	16.276555	172.16.1.2	192.168.254.254	DNS	Standard query A eagle-server.example.com
13	16.277284	192.168.254.254	172.16.1.2	DNS	Standard query response A 192.168.254.254
14	16.278059	172.16.1.2	192.168.254.254	TCP	1073 > ftp [SYN] Seq=0 Len=0 MSS=1460
15	16.278540	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	16.278575	172.16.1.2	192.168.254.254	TCP	1073 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	26.281472	192.168.254.254	172.16.1.2	FTP	Response: 220 Welcome to the eagle-server FTP service.
24	26.281672	172.16.1.2	192.168.254.254	FTP	Request: USER anonymous
25	26.282120	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [ACK] Seq=47 Ack=17 Win=5840 Len=0
26	26.282137	192.168.254.254	172.16.1.2	FTP	Response: 331 Please specify the password.
27	26.282201	172.16.1.2	192.168.254.254	FTP	Request: PASS IEUser@
28	26.283451	192.168.254.254	172.16.1.2	FTP	Response: 230 Login successful.
29	26.313423	172.16.1.2	192.168.254.254	FTP	Request: opts utf8 on
30	26.313959	192.168.254.254	172.16.1.2	FTP	Response: 501 Option not understood.
31	26.314042	172.16.1.2	192.168.254.254	FTP	Request: syst
32	26.314493	192.168.254.254	172.16.1.2	FTP	Response: 215 UNIX Type: L8
33	26.314595	172.16.1.2	192.168.254.254	FTP	Request: site help
34	26.315028	192.168.254.254	172.16.1.2	FTP	Response: 550 Permission denied.
35	26.315113	172.16.1.2	192.168.254.254	FTP	Request: PWD
36	26.315566	192.168.254.254	172.16.1.2	FTP	Response: 257 "/"
37	26.352350	172.16.1.2	192.168.254.254	FTP	Request: noop
38	26.352821	192.168.254.254	172.16.1.2	FTP	Response: 200 NOOP ok.
39	26.482680	172.16.1.2	192.168.254.254	FTP	Request: CWD /
40	26.483243	192.168.254.254	172.16.1.2	FTP	Response: 250 Directory successfully changed.
41	26.484334	172.16.1.2	192.168.254.254	FTP	Request: TYPE A
42	26.484824	192.168.254.254	172.16.1.2	FTP	Response: 200 Switching to ASCII mode.
43	26.485292	172.16.1.2	192.168.254.254	FTP	Request: PORT 172,16,1,2,4,50
44	26.485800	192.168.254.254	172.16.1.2	FTP	Response: 200 PORT command successful. Consider using PASV.
45	26.485892	172.16.1.2	192.168.254.254	FTP	Request: LIST
46	26.486503	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [SYN] Seq=0 Len=0 MSS=1460 TSV=12998374 TSER=0 WS=2
47	26.486558	172.16.1.2	192.168.254.254	TCP	1074 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=
48	26.486948	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=12998375 TSER=0
49	26.487052	192.168.254.254	172.16.1.2	FTP	Response: 150 Here comes the directory listing.
50	26.487252	192.168.254.254	172.16.1.2	FTP-DA	FTP Data: 61 bytes
51	26.487267	192.168.254.254	172.16.1.2	FTP	Response: 226 Directory send OK.

Figura 8: Captura de Wireshark de una sesión FTP con un explorador Web

3. Vaya a la ventana de Wireshark del medio y expanda el protocolo FTP. FTP se comunica usando códigos, como HTTP.

¿Cuál es la respuesta 220 del servidor FTP?

_____

Cuando el servidor FTP emitió una Respuesta: 331. Especifique la contraseña. ¿Cuál fue la respuesta del explorador Web?

_____

¿Qué número de puerto utiliza el cliente FTP para conectarse al puerto 21 del servidor FTP?

_____

Cuando se transfieren datos, o con listados simples de directorios, se abre un nuevo puerto. Esto se llama modo de transferencia. El modo de transferencia puede ser activo o pasivo. En modo activo, el servidor abre una sesión TCP para el cliente FTP y transfiere datos por ese puerto. El número de puerto

de origen del servidor FTP es 20 y el número de puerto del cliente FTP es un número mayor a 1023. Si embargo, en el modo pasivo, el cliente abre un nuevo puerto para el servidor para la transferencia de datos. Ambos números de puerto son mayores a 1023.

¿Cuál es el número de puerto de Datos FTP utilizado por el servidor FTP?

_____

4. Abra la captura de Wireshark FTP_Web_Browser_Client y observe la comunicación FTP. Aunque los clientes sean diferentes, los comandos son similares.

Paso 5: Modos de transferencia FTP activo y pasivo

Las implicaciones entre los dos modos son muy importantes desde el punto de vista de seguridad de la información. El modo de transferencia establece cómo se configura el puerto de datos.

En el modo de transferencia activo, un cliente inicia una sesión FTP con el servidor del puerto TCP 21 bien conocido. Para transferir datos, el servidor inicia una conexión desde el puerto bien conocido TCP 20 para un puerto alto del cliente, un número de puerto mayor a 1023. Vea la figura 9.

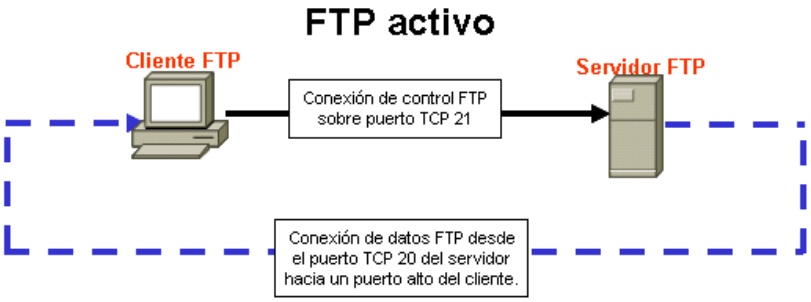


Figura 9.

A menos que el firewall del cliente FTP esté configurado para permitir conexiones desde afuera, la transferencia de datos puede fallar. Para establecer conectividad para la transferencia de datos, el cliente FTP debe permitir las conexiones relacionadas al FTP (que implican un filtrado de paquetes con estado) o deshabilitar el bloqueo.

En el modo de transferencia pasivo, un cliente inicia una sesión FTP con el servidor del puerto 21 TCP bien conocido, la misma conexión usada en el modo de transferencia activo. Sin embargo, para transferir datos existen dos cambios importantes. Primero, el cliente inicia la conexión de datos con el servidor. Segundo, los puertos altos se utilizan en ambos extremos de la conexión. Vea la Figura 10.

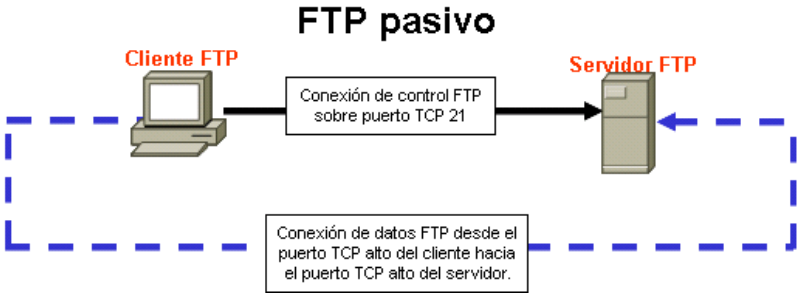


Figura 10.

A menos que el servidor FTP esté configurado para permitir una conexión a un puerto alto aleatorio, la transferencia de datos fallará. No todas las aplicaciones del cliente FTP admiten cambios para el modo de transferencia.

Tarea 4: Reflexión

Los protocolos HTTP y FTP dependen de TCP para comunicarse. TCP administra la conexión entre el cliente y el servidor para asegurar la entrega de datagramas.

Una aplicación de cliente puede ser un explorador Web o una utilidad de línea de comando, pero cada una debe enviar y recibir mensajes que puedan ser interpretados en forma correcta. El protocolo de comunicación se define normalmente en un RFC.

El cliente FTP debe autenticarse al servidor FTP aunque la autenticación esté abierta al mundo. El usuario Anonymous tiene, normalmente, acceso restringido al servidor FTP y no puede cargar archivos.

Una sesión HTTP comienza cuando se realiza una solicitud al servidor HTTP y finaliza cuando el cliente HTTP ha acusado recibo. En cambio, una sesión FTP finaliza cuando el cliente indica que la deja, utilizando el comando **`quit`**.

HTTP utiliza un protocolo simple para comunicarse con el servidor HTTP. El servidor escucha en el puerto 80 para conexiones de clientes. En cambio, FTP utiliza dos protocolos. El servidor FTP escucha en el puerto 21 TCP, como la línea de comandos. Según el modo de transferencia, el servidor o cliente puede iniciar la conexión de datos.

Se puede acceder a los protocolos de capa de aplicación múltiple mediante un explorador Web simple. A pesar de que sólo se examinaron HTTP y FTP, el explorador también admite Telnet y Gopher. El explorador actúa como un cliente para el servidor, enviando solicitudes y procesando respuestas.

Tarea 5: Desafío

Habilite la captura de Wireshark, utilice un explorador Web para navegar a R2 en http://172.16.255.254/level/7/exec o utilice un cliente Telnet para conectarse a un dispositivo de Cisco, como S1-Central o R2-Central. Observe el comportamiento de HTTP o protocolo Telnet. Emita algunos comandos para observar resultados.

¿Cuál es la similitud de Telnet del protocolo de la capa de aplicación con HTTP y FTP? ¿En qué difiere TELNET?

_____

_____

Tarea 6: Limpieza

Si se instaló Wireshark en la computadora host del módulo para esta práctica de laboratorio, el instructor querrá que se elimine la aplicación. Para eliminar Wireshark, haga clic en **Inicio > Panel de control > Agregar o quitar programas**. Vaya hacia abajo en la lista, haga clic con el botón derecho del mouse en **Wireshark** y haga clic en **Quitar**.

Si se deben eliminar los archivos descargados desde la computadora host del módulo, elimine todos los archivos recuperados desde el servidor FTP.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

4.6.1: Desafío de integración de habilidades: Análisis de las capas de aplicación y de transporte

Diagrama de topología

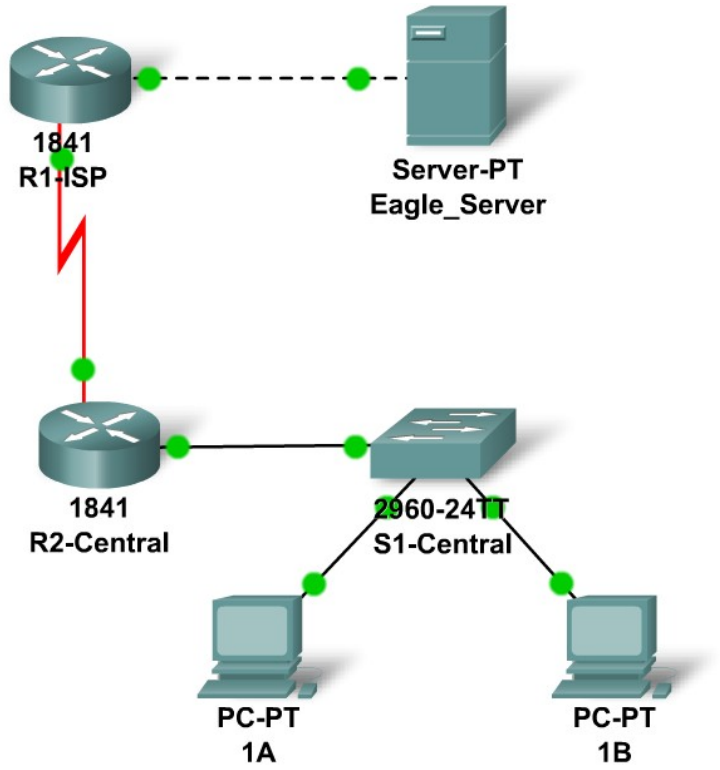


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Configurar hosts y servicios
- Conectar y configurar hosts y servicios en el modelo de red de laboratorio.
- Explorar cómo trabajan en conjunto DNS, UDP, HTTP y TCP.
- Usar el modo de simulación para visualizar el funcionamiento de DNS, UDP, HTTP y TCP en el modelo de red de laboratorio.

Información básica

A lo largo del curso, utilizará una configuración de laboratorio estándar creada a partir de PC, servidores, routers y switches reales para aprender los conceptos sobre redes. Al final de cada capítulo, desarrollará secciones cada vez más largas de esta topología en el Packet Tracer y analizará interacciones de protocolos cada vez más complejas.

Tarea 1: Reparación y prueba de la topología.

Se ha reemplazado el servidor. Debe encenderse. Configúrelo con los siguientes parámetros: Dirección IP 192.168.254.254, Máscara de subred 255.255.255.0, Gateway por defecto 192.168.254.253, DNS habilitado, con la asociación de eagle-server.example.com con la dirección IP del servidor, HTTP habilitado. Conecte el Eagle Server al puerto Fa0/0 en el router R1-ISP mediante un cable de conexión cruzada.

PC 1A perdió la información de su dirección IP. Configúrela con los siguientes parámetros: Dirección IP 172.16.1.1, Máscara de subred 255.255.0.0, Gateway por defecto 172.16.255.254 y Servidor DNS 192.168.254.254. Conecte la PC 1A al puerto Fa0/1 del switch S1-Central mediante un cable de conexión directa.

Verifique su trabajo utilizando la evaluación con el botón **Verificar resultados** y la ficha **Puntos de evaluación**. Pruebe la conectividad, en tiempo real, mediante AGREGAR PDU SIMPLE para probar la conectividad entre la PC 1A y el Eagle Server.

Tenga en cuenta que cuando agrega una PDU simple, ésta aparece en la ventana Lista de PDU como parte de “Situación 0”. La primera vez que ejecute este mensaje ping para un solo lanzamiento, aparecerá como **Fallido**, esto se debe al proceso ARP que se explicará posteriormente. Al hacer doble clic en el botón “Disparar” en la ventana Lista de PDU, enviará esta prueba de ping simple por segunda vez. Esta vez tendrá éxito. En el Packet Tracer, el término “situación” significa una configuración específica de uno o más paquetes de prueba. Puede crear diferentes situaciones de paquetes de prueba con el botón **Nuevo**; por ejemplo, Situación 0 podría tener un paquete de prueba de la PC 1A al Eagle Server, Situación 1 podría tener paquetes de prueba entre la PC 1B y los routers, y así sucesivamente. Puede retirar todos los paquetes de prueba de una situación en particular al utilizar el botón **Eliminar**. Por ejemplo, si utiliza el botón **Eliminar** para la Situación 0, el paquete de prueba que acaba de crear entre la PC 1A y el Eagle Server se retirará; hágalo antes de pasar a la siguiente tarea.

Tarea 2: Exploración del funcionamiento en conjunto de DNS, UDP, HTTP y TCP

Cambie del modo de tiempo real al modo de simulación. Asegúrese de que el filtro de eventos esté establecido para mostrar DNS, UDP, HTTP, TCP e ICMP. Abra un explorador Web desde el escritorio de 1A. Escriba el URL eagle-server.example.com, presione Enter y luego use el botón **Capturar / Reenviar** de la **Lista de eventos** para capturar la interacción de DNS, UDP, HTTP y TCP.

Puede examinar el paquete de dos maneras: haciendo clic en el sobre del paquete como se muestra en la animación o haciendo clic en la columna **Información** para dicha instancia del paquete, como se enumera en la **Lista de eventos.** Reproduzca esta animación y examine el contenido del paquete (Ventana de **Información de PDU**, **Detalles de PDU entrantes, Detalles de PDU salientes**) para cada evento de la lista de eventos, especialmente cuando los paquetes están en la PC 1A o en el Eagle Server. Si recibe el mensaje “Búfer lleno”, haga clic en el botón **Ver eventos anteriores**. Si bien es posible que aún no comprenda el procesamiento de los paquetes por parte del switch y los routers, debe poder ver cómo trabajan en forma conjunta DNS, UDP, HTTP y TCP estudiando los paquetes y utilizando la ventana Información de la PDU para ver “dentro” de éstos.

Reflexión

¿Puede realizar un diagrama de la secuencia de eventos de protocolo involucrada en la solicitud de una página Web mediante un URL? ¿En qué lugar podrían presentarse errores? Compare y contraste DNS y HTTP con UDP y TCP.

Práctica de laboratorio 5.5.1: Examen del gateway de un dispositivo

Diagrama de topología

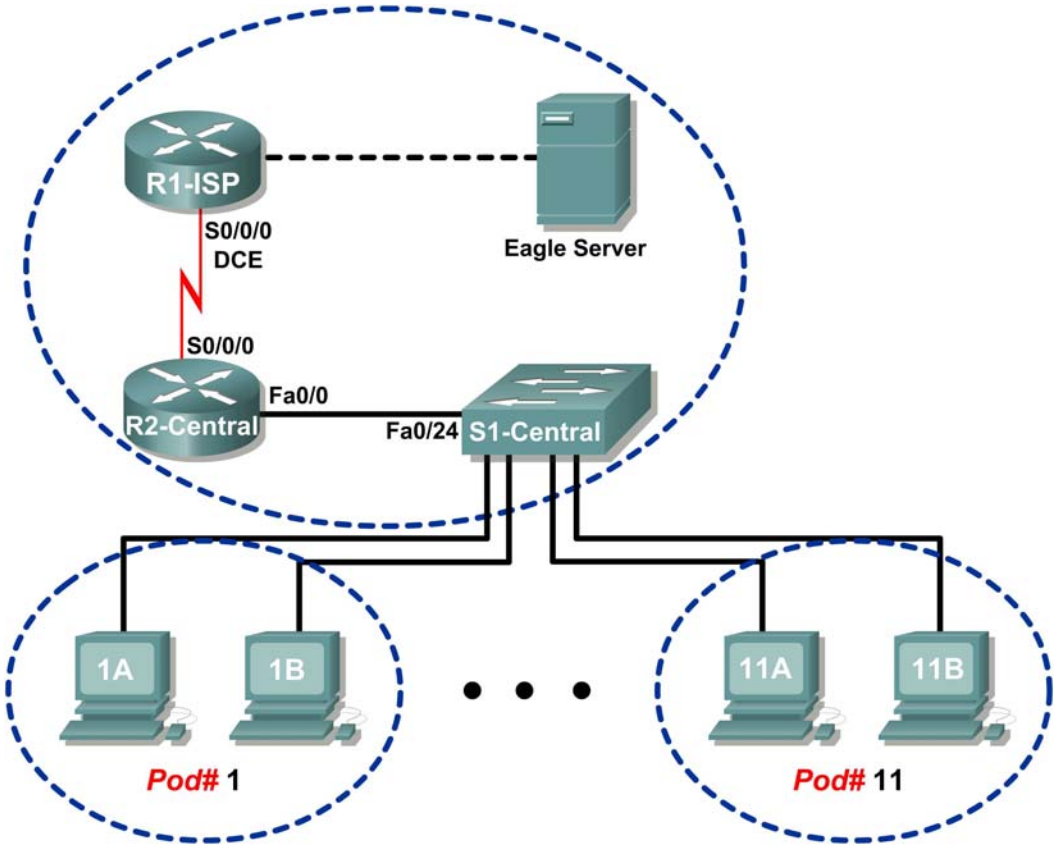


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#*A	*No aplicable*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	*No aplicable*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Comprender y explicar el objetivo de una dirección de gateway.
- Comprender la configuración de la información de la red en una computadora Windows.
- Resolver un problema escondido en la dirección de gateway.

Información básica

Una dirección IP está compuesta de una porción de red y de una porción de host. Una computadora que se comunica con otro dispositivo primero debe saber cómo llegar al dispositivo. Para los dispositivos de la misma red de área local (LAN), la porción de host de la dirección IP se utiliza como identificador. La porción de red del dispositivo de destino es igual a la porción de red del dispositivo host.

Sin embargo, los dispositivos que se encuentran en redes diferentes tienen diferentes números de red de origen y de destino. La porción de red de la dirección IP se utiliza para identificar cuándo debe enviarse un paquete a la dirección de gateway, la que se asigna a un dispositivo de red que envía paquetes entre redes lejanas.

Se asigna un router a la dirección de gateway para todos los dispositivos en la LAN. Uno de los objetivos del router es servir como punto de entrada para los paquetes que ingresan a la red y como punto de salida para los paquetes que dejan la red.

Las direcciones de gateway son muy importantes para los usuarios. Cisco calcula que el 80% del tráfico de red será destinado a dispositivos de otras redes y sólo el 20% del tráfico de red irá a los dispositivos locales. Esto se conoce como regla 80/20. Por lo tanto, si los dispositivos de LAN no pueden alcanzar el gateway, los usuarios no podrán realizar su trabajo.

Escenario

Las computadoras host del módulo deben comunicarse con Eagle Server, pero Eagle Server está ubicado en una red diferente. Si la dirección de gateway de la computadora host del módulo no está configurada correctamente, fallará la conectividad con Eagle Server.

La configuración de red de una computadora host del módulo se verificará utilizando varias utilidades comunes.

Tarea 1: Comprensión y explicación del objetivo de una dirección de gateway.

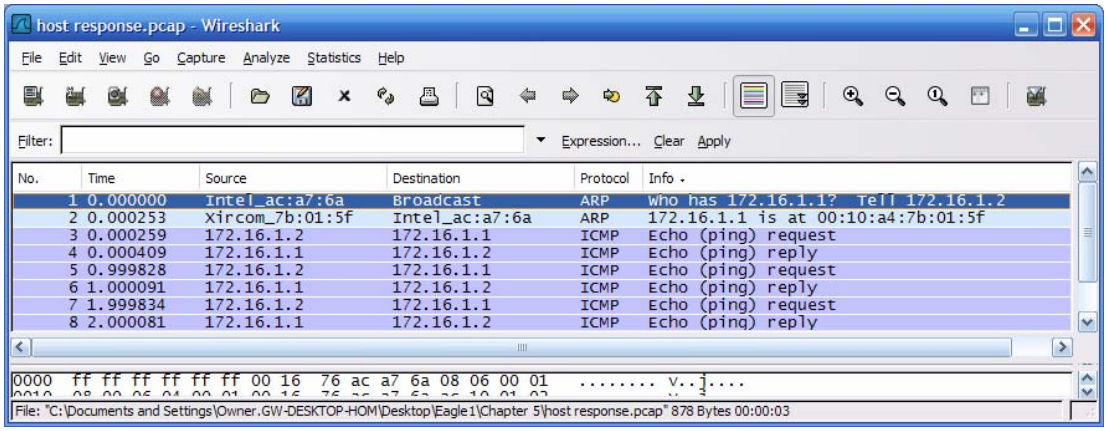


Figura 1. Comunicación entre dispositivos LAN

Para el tráfico de la red de área local (LAN), la dirección de gateway es la dirección del dispositivo Ethernet conectado a la LAN. La Figura 1 muestra dos dispositivos en la misma red comunicándose con el comando **ping**. Todo dispositivo que tenga la misma dirección de red, en este ejemplo `172.16.0.0`, se encuentra en la misma LAN.

Consulte la Figura 1: ¿Cuál es la dirección MAC del dispositivo de red en la dirección IP 172.16.1.1?

_____

Existen varios comandos de Windows que mostrarán una dirección de gateway de red. Un comando de uso generalizado es **`netstat -r.`** En la siguiente transcripción, el comando **`netstat -r`** se utiliza para visualizar las direcciones de gateway para esta computadora. El punto destacado superior muestra qué dirección de gateway se utiliza para enviar todos los paquetes de red fuera de la LAN. El destino de red "quad-zero" y los valores Netmask, `0.0.0.0` y `0.0.0.0`, hacen referencia a *toda* red no conocida específicamente. Para una red que no sea local, esta computadora utilizará `172.16.255.254` como gateway por defecto. El segundo punto destacado en amarillo muestra la información de manera que las personas puedan leerla. Las redes más específicas se alcanzan a través de otras direcciones de gateway. Una interfaz local, llamada interfaz loopback, se asigna automáticamente a la red `127.0.0.0`. La interfaz se utiliza para identificar el host local para los servicios de red local. Remítase a la entrada resaltada en gris. Por último, todo dispositivo en la red `172.16.0.0` puede accederse a través del gateway `172.16.1.2`, que es la dirección IP para esta interfaz Ethernet. Esta entrada está resaltada en verde.

```
C:\>netstat -r

Tabla de rutas
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a  Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Rutas activas:
Destino de red     Máscara de red        Gateway     Interfaz  Métrica
          0.0.0.0          0.0.0.0   172.16.255.254  172.16.1.2   1
        127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1   1
      172.16.0.0      255.255.0.0      172.16.1.2  172.16.1.2  20
      172.16.1.2  255.255.255.255        127.0.0.1   127.0.0.1  20
  172.16.255.255  255.255.255.255      172.16.1.2  172.16.1.2  20
255.255.255.255  255.255.255.255      172.16.1.2  172.16.1.2   1
Gateway por defecto:    172.16.255.254
===========================================================================
Rutas persistentes:
  Ninguna
C:\>
```

Paso 1: Abrir una ventana terminal en la computadora host del módulo.

¿Cuál es la dirección de gateway por defecto?

_____

Paso 2: Utilizar el comando ping para verificar la conectividad con la dirección IP `127.0.0.1.`

¿Fue exitoso el ping? _____

Paso 3: Utilizar el comando `ping` para hacer ping en diferentes direcciones IP en la red `127.0.0.0` y `127.255.255.255`.

¿Las respuestas fueron exitosas? Si no es así, ¿por qué?

_____

_____

La dirección de gateway predeterminada permite que un dispositivo de red se comunique con otros dispositivos en diferentes redes. De hecho, es la puerta a otras redes. Todo el tráfico destinado a diferentes redes debe atravesar el dispositivo de red que tiene la dirección de gateway por defecto.

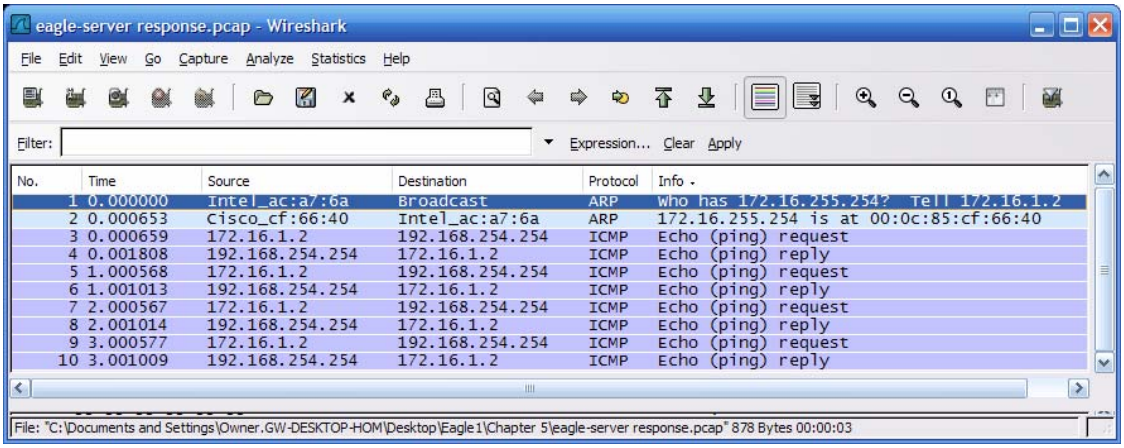


Figura 2. Comunicación entre dispositivos que se encuentran en diferentes redes

Como muestra la Figura 2, la comunicación entre dispositivos ubicados en diferentes redes es diferente a la comunicación entre dispositivos ubicados en una LAN. La computadora host del módulo N.º 2, dirección IP `172.16.1.2`, inicia el ping a la dirección IP `192.168.254.254`. Debido a que la red `172.16.0.0` es diferente de la `192.168.254`, la computadora host del módulo solicita la dirección MAC del dispositivo de gateway por defecto. Este dispositivo de gateway, un router, responde con su dirección MAC. La computadora crea el encabezado de la Capa 2 con la dirección MAC de destino del router y coloca las tramas del cable en el dispositivo de gateway.

Consulte la Figura 2: ¿Cuál es la dirección MAC del dispositivo de gateway?

_____

Consulte la Figura 2: ¿Cuál es la dirección MAC del dispositivo de red con dirección IP 192.168.254.254?

_____

Tarea 2: Comprensión de la configuración de la información de red en una computadora Windows.

Muchas veces los problemas de conectividad se atribuyen a redes mal configuradas. En la resolución de problemas de conectividad hay varias herramientas disponibles para determinar rápidamente la configuración de red en cualquier computadora Windows.

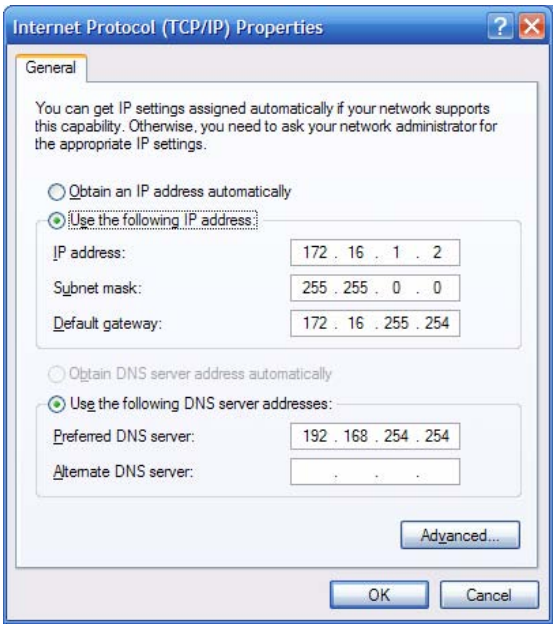


Figura 3. Interfaz de red con dirección IP estática

Paso 1: Examinar las configuraciones de propiedades de red.

Un método que puede ser útil para determinar las propiedades IP de la interfaz de red consiste en examinar las configuraciones de las propiedades de red de la computadora host del módulo. Para acceder a esta ventana:

1. Haga clic en **Inicio > Panel de control > Conexiones de red**.
2. Haga clic con el botón derecho en **Conexión de área local** y seleccione **Propiedades**.
3. En la ficha **General**, desplácese hacia abajo en la lista de elementos en el panel, seleccione **Protocolo de Internet (TCP/IP)** y luego haga clic en el botón **Propiedades**. Se verá una ventana similar a la que se muestra en la Figura 3.

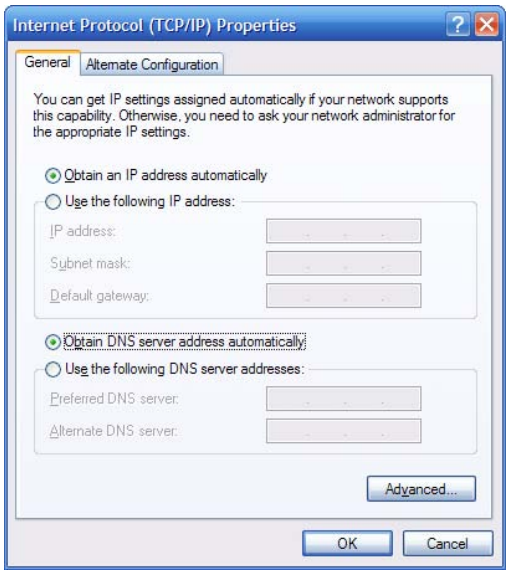


Figura 4. Interfaz de red con dirección IP dinámica

Sin embargo, como muestra la Figura 4, es posible configurar una dirección IP dinámica. En este caso, la ventana de configuraciones de propiedades de red no es demasiado útil para determinar la información de dirección IP.

Un método sistemáticamente más confiable para determinar las configuraciones de red en una computadora Windows consiste en utilizar el comando **ipconfig**:

```
C:\ >ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
      1 IP Address. . . . . . . . . . . . : 172.16.1.2
      2 Subnet Mask . . . . . . . . . . . : 255.255.0.0
      3 Default Gateway . . . . . . . . . : 172.16.255.254
```

❶ Dirección IP para esta computadora host del módulo
❷ Máscara de subred
❸ Dirección de gateway por defecto

Existen varias opciones disponibles con el comando **ipconfig**, a las que se puede acceder con el comando **ipconfig /?**. Para mostrar la mayor parte de información sobre las conexiones de red, utilice el comando **ipconfig /all**.

```
C:\>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : GW-desktop-hom
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) 82562V 10/100
Network Connection
        Physical Address. . . . . . . . . : 00-16-76-AC-A7-6A
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.16.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.255.254
      1 DNS Servers . . . . . . . . . . . : 192.168.254.254
C:\ >
```

❶ Dirección IP del servidor nombre de dominio

Paso 2: Utilizando el comando `ipconfig /all`, completar la siguiente tabla con la información de su computadora host del módulo.

Descripción	Dirección
Dirección IP	
Máscara de subred	
Gateway por defecto	
Servidor DNS	

Tarea 3: Resolución de un problema escondido en la dirección de gateway.

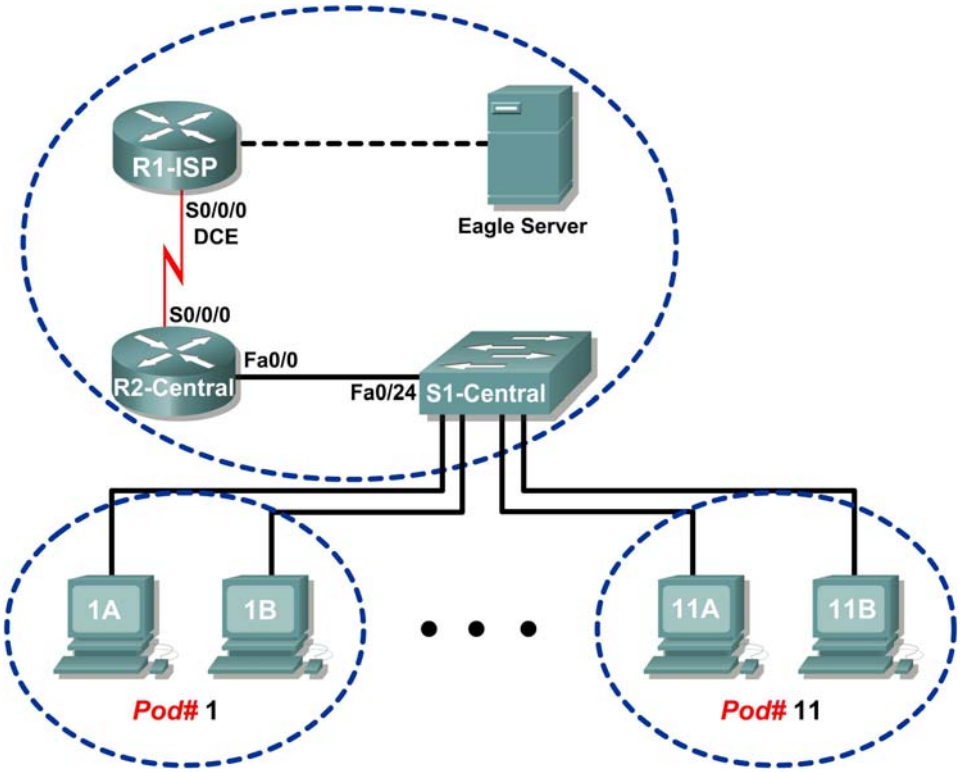


Figura 5. Diagrama de topología

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.4	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.3	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Tabla 1. Asignaciones de direcciones lógicas

Al resolver problemas en la red, una profunda comprensión de la red puede ayudar en la identificación del problema real. Consulte la topología de red en la Figura 5 y las asignaciones de dirección IP lógica en la Tabla 1.

Como ingeniero de Cisco del servicio de asistencia técnica del tercer turno, el técnico del servicio de asistencia le pide ayuda. El técnico recibió un informe de problema de un usuario en la computadora host-1A, en el que se queja de que la computadora host-11B, `host-11B.example.com`, no responde a los pings. El técnico verificó los cables y las configuraciones de red en ambas computadoras, pero no encontró nada inusual. Usted verifica con el ingeniero de red de la empresa, quien informa que R2-Central ha sido desactivada temporalmente para realizar una actualización de hardware.

Asintiendo con la cabeza para demostrar que comprende, le pide al técnico que haga ping en la dirección IP para el host-11B, `172.16.11.2` desde el host-1A. Los pings tienen éxito. Luego le pide al técnico que haga ping en la dirección IP de gateway, `172.16.254.254`, y los pings fallan.

¿Qué está mal?

_____

_____

Le indica al técnico del servicio de asistencia que le diga al usuario que utilice temporalmente la dirección IP para host-11B y que el usuario puede establecer conectividad con la computadora. Dentro de la hora, el router de gateway vuelve a conectarse y se reanuda el funcionamiento normal de la red.

Tarea 4: Reflexión

La dirección de gateway es crítica para la conectividad de red, y en algunas situaciones los dispositivos LAN necesitan un gateway por defecto para comunicarse con otros dispositivos ubicados en la LAN.

Al utilizar utilidades de línea de comandos Windows como **`netstat –r`** y **`ipconfig /all`** se informarán las configuraciones de gateway de las computadoras host.

Tarea 5: Desafío

Utilice Wireshark para capturar un ping entre dos computadoras host del módulo. Puede ser necesario reiniciar la computadora host para purgar la caché DNS. Primero utilice el nombre de host de la computadora de destino del módulo para DNS para responder con la dirección IP de destino. Observe la secuencia de comunicación entre dispositivos de red, en especial el gateway. Luego, capture un ping entre los dispositivos de red utilizando sólo direcciones IP. La dirección de gateway no será necesaria.

Tarea 6: Limpieza

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 5.5.2: Examen de una ruta

Diagrama de topología

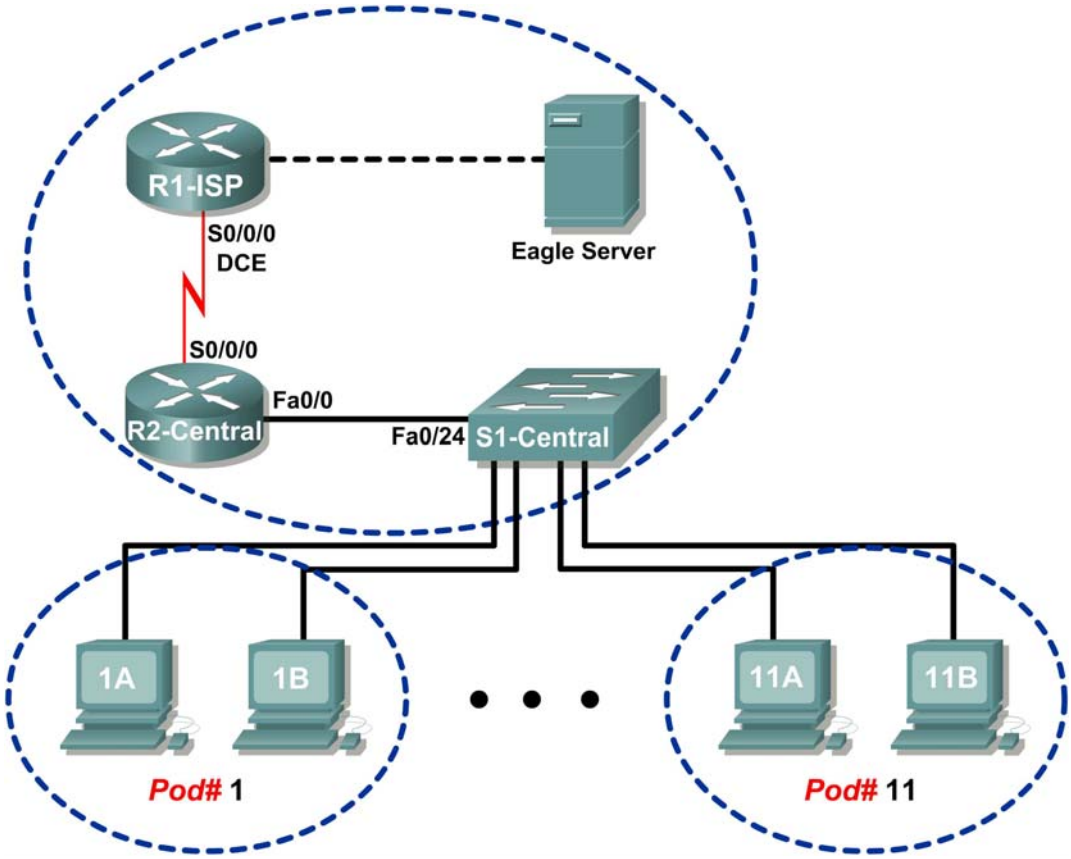


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
hostPod#**A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hostPod#**B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Utilizar el comando **route** para modificar una tabla de enrutamiento en una computadora de Windows.
- Utilizar un comando **telnet** de un cliente Telnet de Windows para conectarse a un router Cisco.
- Analizar las rutas del router usando los comandos IOS básicos de Cisco.

Información básica

Para que los paquetes viajen a través de una red, un dispositivo debe conocer la ruta hacia la red de destino. Esta práctica de laboratorio compara cómo se utilizan las rutas en computadoras de Windows y el router de Cisco.

Algunas rutas se agregan automáticamente a las tablas de enrutamiento, basándose en la información de configuración en la interfaz de red. El dispositivo considera que una red está conectada directamente cuando tiene una dirección IP y máscara de red configuradas, y la ruta de red se ingresa automáticamente en la tabla de enrutamiento. Para las redes que no están conectadas directamente, se configura una dirección IP de gateway por defecto que enviará tráfico a un dispositivo que debe tener conocimiento sobre la red.

Escenario

Examine la tabla de enrutamiento con el comando **route** e identifique las diferentes rutas y direcciones IP de gateway para la ruta utilizando una computadora host del pod. Elimine la ruta de gateway por defecto, pruebe la conexión y luego agregue la ruta de gateway por defecto a la tabla de host.

Utilice una computadora host del módulo para telnet en R2-Central, y examine la tabla de enrutamiento.

Tarea 1: Utilización del comando route para modificar una tabla de enrutamiento en una computadora de Windows.

```
C:\>netstat -r

Tabla de rutas
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a  Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Rutas activas:
Destino de red     Máscara de red        Gateway     Interfaz  Métrica
        0.0.0.0          0.0.0.0   172.16.255.254  172.16.1.2   1
      127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1   1
     172.16.0.0      255.255.0.0       172.16.1.2  172.16.1.2  20
     172.16.1.2  255.255.255.255        127.0.0.1   127.0.0.1  20
 172.16.255.255  255.255.255.255       172.16.1.2  172.16.1.2  20
255.255.255.255  255.255.255.255       172.16.1.2  172.16.1.2   1
Gateway por defecto:    172.16.255.254
===========================================================================
Rutas persistentes:
  Ninguna
C:\>
```

Figura 1. Resultado del comando netstat

La Figura 1 muestra el resultado del comando **netstat –r** que sirve para determinar la información de ruta y gateway.

Paso 1: Examinar las rutas activas en una computadora Windows.

El comando **route** es un comando útil para modificar la tabla de enrutamiento. A diferencia del comando **netstat –r**, el comando **route** se puede utilizar para ver, agregar, eliminar o cambiar las entradas de la tabla de enrutamiento. Para ver información detallada sobre el **comando route**, utilice la opción **route /?**.

A continuación se muestra una lista de opciones abreviada para el comando **route**:

```
route PRINT       Imprime rutas activas
route ADD         Agrega una ruta:
                  route ADD network MASK mask gateway
route DELETE      Elimina una ruta:
                  route DELETE network
route CHANGE      Modifica una ruta existente
```

Para ver rutas activas, emita el comando **route PRINT:**

```
C:\ >route PRINT
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x70003 ...00 16 76 ac a7 6a .Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Rutas activas:
Destino de red     Máscara de red        Gateway     Interfaz  Métrica
        0.0.0.0          0.0.0.0  172.16.255.254   172.16.1.2     1
      127.0.0.0        255.0.0.0       127.0.0.1    127.0.0.1     1
     172.16.0.0      255.255.0.0      172.16.1.2   172.16.1.2    20
     172.16.1.2  255.255.255.255       127.0.0.1    127.0.0.1    20
 172.16.255.255  255.255.255.255      172.16.1.2   172.16.1.2    20
255.255.255.255  255.255.255.255      172.16.1.2   172.16.1.2     1
Gateway por defecto: 172.16.255.254
===========================================================================
Rutas persistentes:
  Ninguna
C:\>
```

Verifique la conectividad de red a Eagle Server:

```
C:\> ping eagle-server.example.com
Pinging eagle-server.example.com [192.168.254.254] with 32 bytes
of data:

Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.254.254:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

¿Cuál es la dirección de gateway para `eagle-server.example.com`?

_____

Paso 2: Eliminar una ruta de la tabla de enrutamiento de una computadora Windows.

¿Cuán importante es la ruta de gateway por defecto? Elimine la ruta de gateway e intente hacer ping en Eagle Server. La sintaxis para quitar la ruta de gateway por defecto es:

```
route DELETE network

C:/> route DELETE 0.0.0.0
```

Examine la tabla de enrutamiento activa y verifique que se haya eliminado la ruta de gateway por defecto:

¿Cuál es la dirección IP de gateway por defecto?

_____

Intente hacer ping en Eagle Server. ¿Cuáles son los resultados?

_____

Si se elimina la dirección IP de gateway por defecto, ¿cómo se puede acceder al servidor DNS para resolver `eagle-server.example.com`?

¿Se puede acceder a otro dispositivo LAN, como `172.16.255.254`?

_____

Paso 3: Insertar una ruta en la tabla de enrutamiento de una computadora Windows.

En la siguiente configuración, utilice la dirección IP asignada a la interfaz host del módulo. La sintaxis para agregar una ruta a la tabla de enrutamiento de una computadora Windows es:

```
route ADD network MASK mask gateway-IP address

C:/> route ADD 0.0.0.0 MASK 0.0.0.0 172.16.255.254
```

Examine la tabla de enrutamiento activa y verifique que se haya restaurado la ruta de gateway por defecto:

¿Se restauró la ruta de gateway por defecto? _____

Intente hacer ping en Eagle Server. ¿Cuáles son los resultados?

_____

Tarea 2: Utilización de un comando telnet de un cliente Telnet de Windows para conectarse a un router de Cisco.

En esta tarea se hará telnet en el router R2-Central y se usarán comandos IOS comunes para examinar la tabla de enrutamiento del router. Los dispositivos de Cisco tienen un servidor Telnet y, si está configurado en forma adecuada, permitirá conexiones remotas. Sin embargo, el acceso al router es restringido y requiere un nombre de usuario y contraseña. La contraseña para todos los usuarios es `cisco`. El nombre de usuario depende del módulo. El nombre de usuario `ccna1` es para los usuarios de computadoras del módulo 1, `ccna2` es para estudiantes en las computadoras del módulo 2, y así sucesivamente.

Paso 1: Conectarse al router de Cisco utilizando el cliente Telnet de Windows.

Abra una ventana terminal haciendo clic en **Inicio > Ejecutar**. Ingrese: `cmd` y haga clic en **Aceptar**. Deben estar disponibles una ventana terminal y un indicador. La utilidad Telnet tiene varias opciones y se puede ver con el comando **`telnet /?`**. Se requiere un nombre de usuario y una contraseña para conectarse al router. La contraseña correspondiente para todos los nombres de usuario es `cisco`.

Número del módulo	Nombre de usuario
1	ccna1
2	ccna2
3	ccna3
4	ccna4
5	ccna5
6	ccna6
7	ccna7
8	ccna8
9	Ccna9
10	ccna10
11	ccna11

Para iniciar una sesión Telnet con el router R2-central, ingrese el comando:

```
C:/> telnet 172.16.255.254 <ENTER>
```

Una ventana de conexión pedirá un nombre de usuario, como se muestra a continuación. Ingrese el nombre de usuario correspondiente y presione **<ENTER>**. Ingrese la contraseña, `cisco`, y presione **<ENTER>**. El indicador del router debe estar visible luego de una conexión exitosa.

```
**************************************************************
               This is Eagle 1 lab router R2-Central.
               Authorized access only.
**************************************************************

User Access Verification

Nombre de usuario: ccna1
Password: cisco (hidden)
R2-Central#
```

En el indicador, `R2-Central#`, se creó una conexión Telnet exitosa. Sólo se permiten permisos limitados para nombres de usuario `ccnax`; por lo tanto no se pueden modificar ni ver las configuraciones de los routers. El objetivo de esta tarea era establecer una sesión Telnet, y se logró. En la tarea siguiente, se examinará el router de la tabla de enrutamiento.

Tarea 3: Examen de las rutas del router utilizando los comandos IOS básicos de Cisco.

Como con cualquier dispositivo de red, las direcciones de gateway indican al dispositivo cómo alcanzar otras redes cuando no se encuentra disponible ninguna otra información. Al igual que la dirección IP del gateway por defecto, un router también puede emplear un gateway por defecto. Al igual que una computadora host, un router también está informado sobre redes conectadas directamente.

Esta tarea no examina los comandos IOS de Cisco en detalle, pero utiliza un comando IOS común para ver la tabla de enrutamiento. La sintaxis para ver la tabla de enrutamiento es:

```
show ip route <ENTER>
```

Paso 1: Introducir el comando para mostrar la tabla de enrutamiento del router.

La información de ruta que se muestra es mucho más detallada que la información de ruta de una computadora host. Se espera que esto suceda porque el trabajo de un router es enrutar el tráfico entre redes. Sin embargo, la información que se solicita en esta tarea no es difícil de conseguir. La Figura 2 muestra la tabla de enrutamiento para `R2-Central`.

```
R2-Central#show ip route
Codes: 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

Gateway of last resort is 10.10.10.6 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figura 2. Resultado del comando IOS de Cisco `show ip route`

La sección `Codes(códigos)` que se muestra en la Figura 3 proporciona una explicación para los símbolos de la izquierda de cada entrada de ruta.

```
R2-Central#show ip route
Codes: 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

Gateway of last resort is 10.10.10.6 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figura 3. Explicación de los códigos

❶ `C` denota redes conectadas directamente y la interfaz que respalda la conexión.
❷ `S` denota una ruta estática, que ingresa manualmente el ingeniero de red de Cisco.
❸ Debido a que la ruta es “quad-zero”, es una `posible ruta predeterminada`.
❹ Si no existe ninguna otra ruta en la tabla de enrutamiento, utilice este gateway de dirección IP `de último recurso` para enviar paquetes.

¿Cómo se muestra la información de la mascara de IP en una tabla de enrutamiento de router?

_____

_____

¿Qué haría el router con los paquetes destinados a 192.168.254.254?

_____

_____

Cuando termine de examinar la tabla de enrutamiento, salga del router con el comando **`exit <ENTER>`**. El cliente Telnet también cierra la conexión con la secuencia de escape telnet **`<CTRL> ]`** y **`quit`**. Cierre la ventana terminal.

Tarea 4: Reflexión

Se utilizaron dos comandos nuevos de Windows en esta práctica de laboratorio. El comando **`route`** se utilizó para ver, eliminar y agregar información de ruta en la computadora host del módulo.

El cliente Telnet de Windows, **`telnet`**, se utilizó para conectar a un router de laboratorio, R2-Central. Esta técnica se usará en otras prácticas de laboratorio para conectar dispositivos de red de Cisco.

Se examinó la tabla de enrutamiento del router con el comando IOS de Cisco **`show ip route`**. Se muestran las rutas para las redes conectadas directamente, las rutas asignadas de forma estática y el gateway de información de último recurso.

Tarea 5: Desafío

Se pueden usar otros comandos IOS de Cisco para ver la información de dirección IP en un router. Al igual que el comando **`ipconfig`** de Windows, el comando IOS de Cisco **`show ip interface brief`** mostrará las asignaciones de dirección IP.

```
R2-Central#show ip interface brief
Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  172.16.255.254  YES manual up                    up
FastEthernet0/1  unassigned      YES unset  administratively down down
Serial0/2/0      10.10.10.5      YES manual up                    up
Serial0/2/1      unassigned      YES unset  administratively down down
R2-Central#
```

Compare el resultado de la información de red utilizando los comandos de Windows y los comandos IOS de Cisco en esta práctica de laboratorio. ¿Qué faltó? ¿Qué información de red crítica fue similar?

_____

_____

Tarea 6: Limpieza.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

5.6.1: Desafío de integración de habilidades: Enrutamiento de paquetes IP

Diagrama de topología

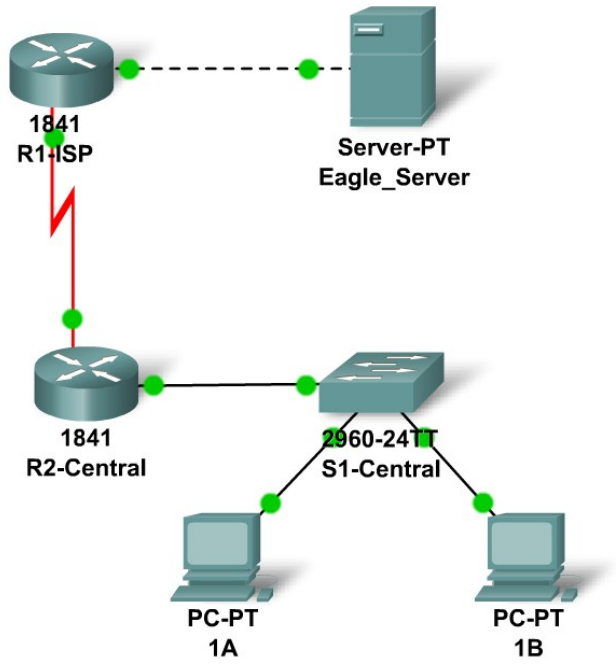


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Configurar una interfaz de router mediante GUI.
- Explorar una tabla de enrutamiento.
- Configurar una ruta estática mediante GUI.
- Explorar el enrutamiento de paquetes IP.

Información básica

A lo largo del curso, utilizará una configuración de laboratorio estándar creada a partir de PC, servidores, routers y switches reales para aprender los conceptos sobre redes. Al final de cada capítulo, desarrollará secciones cada vez más largas de esta topología en el Packet Tracer y analizará interacciones de protocolos cada vez más complejas. Ya ha estudiado una variedad de protocolos de aplicaciones, como DNS, HTTP, TFTP, DHCP y Telnet, y dos protocolos de capa de Transporte, TCP y UDP. Es posible que haya notado que independientemente de los protocolos de aplicación y de transporte utilizados, en la vista **Detalles de la PDU entrante** y **saliente** siempre están encapsulados en paquetes IP. En esta actividad, examinaremos el funcionamiento del Internet Protocol, el protocolo de la capa de Red dominante en Internet, en el contexto de un ejemplo simple de enrutamiento IP.

Tarea 1: Configuración de la interfaz del router.

Se observan problemas en la red del área local: PC 1A no puede acceder al Eagle Server (verifique que se encuentre en el modo de tiempo real). Es probable que haya un problema con el router. Mueva el mouse sobre el router R2-Central y observe el estado de la interfaz Fa0/0 (a qué switch está conectada). Esta interfaz debe tener una dirección IP, una máscara de subred y debe encenderse para funcionar como gateway por defecto para la LAN. Haga clic en el router R2-Central y vaya a la ficha de **Configuración**. Al finalizar el curso, aprenderá a utilizar la Interfaz de línea de comandos (CLI) del Sistema operativo Internetwork (IOS) de Cisco para realizar esta tarea. En este momento, la ficha **Configuración** es más sencilla y le permitirá concentrarse en la idea básica del enrutamiento IP. En la lista que se muestra, busque **INTERFAZ, FastEthernet0/0**. Agregue la dirección IP 172.16.255.254 con la máscara de subred 255.255.0.0 y encienda el puerto. Cierre la ventana del router. Verifique que la interfaz del router (puerto) funciona moviendo el mouse sobre ella. Intente alcanzar el Eagle Server. La solicitud aún falla. ¿Cuáles son algunos de los posibles motivos?

Tarea 2: Examen de las rutas.

Utilice la **Herramienta de inspección** (la lupa) para examinar la tabla de enrutamiento de R2-Central. Verá las redes conectadas directamente al router pero no hay manera de alcanzar la red del Eagle Server.

Tarea 3: Configuración de una ruta mediante GUI.

Haga clic en el router R2-Central y vaya a la ficha de **Configuración**. En la lista que se muestra, busque **ENRUTAMIENTO**, **Estático**. Configure lo que se conoce como una ruta estática predeterminada, mediante la utilización de la dirección 0.0.0.0, máscara 0.0.0.0 y el siguiente salto de 10.10.10.6 (la interfaz S0/0/0 en el router R1-ISP) y haga clic en el botón **Agregar**. Esta ruta se configura de modo que cualquiera sea el lugar al que estén destinados los paquete de la LAN 172.16.0.0 /16, éstos se dirigirán al router R1-ISP. En **GLOBAL, Configuración**, haga clic en el botón **Guardar** para guardar la configuración de la interfaz y la ruta que acaba de realizar en NVRAM en caso de que se encienda y apague el router. Utilice la **Herramienta de inspección** (la lupa) para examinar la tabla de enrutamiento de R2-Central nuevamente. Ahora deberá ver la ruta que configuró en la tabla de enrutamiento.

Verifique su trabajo utilizando la evaluación con el botón **Verificar resultados** y la ficha **Puntos de evaluación**. Pruebe la conectividad, en tiempo real, mediante AGREGAR PDU SIMPLE para probar la conectividad entre la PC 1A y el Eagle Server. La PDU, un ping para un solo lanzamiento, aparecerá en la Lista de PDU creada por el usuario para su uso en el futuro también. El primer intento del ping fallará debido a que no se completaron las tablas de enrutamiento; haga doble clic en **Disparar** para volver a enviarlo; esta vez deberá tener éxito.

Tarea 4: Examen del enrutamiento del paquete IP.

Cambie a modo de simulación. Usando la PDU que creó en la Tarea 3, rastree el tramo de los paquetes desde la PC 1A hacia el Eagle Server y viceversa, usando el botón **Capturar/Reenviar** y examinando el contenido del paquete, ya sea haciendo clic sobre el sobre o sobre el cuadrado coloreado en la columna **Información** de la **Lista de eventos**.

Reflexión

¿Qué datos puede contener un paquete IP? ¿Qué significa la frase “Se enrutó el paquete IP”? ¿Qué es una ruta? ¿En qué lugar podrían presentarse errores?

Práctica de laboratorio 6.7.1: Ping y Traceroute

Diagrama de topología

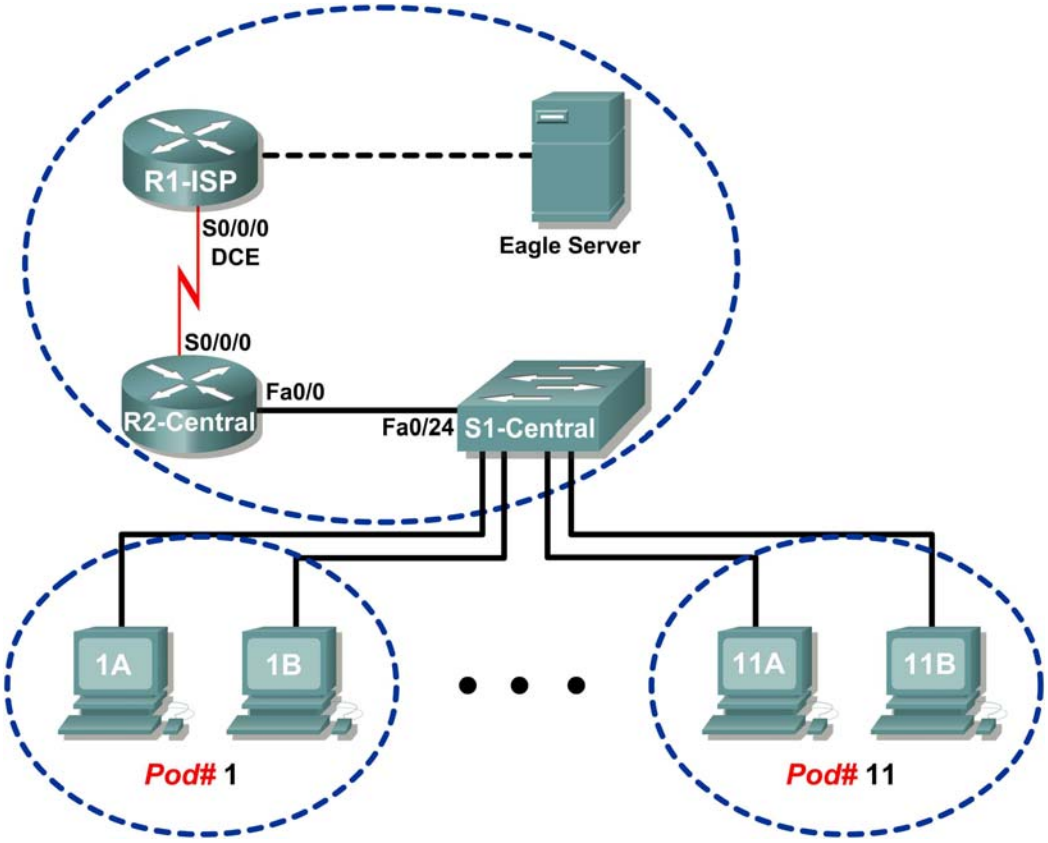


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#***A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Utilizar el comando **ping** para verificar la conectividad de red TCP/IP simple.
- Utilizar el comando **tracert/traceroute** para verificar la conectividad TCP/IP.

Información básica

Ping y **tracert** son dos herramientas indispensables al momento de probar la conectividad de red TCP/IP. La utilidad **ping** está disponible en Windows, Linux, y Cisco IOS y prueba la conectividad de red. La utilidad **tracert** está disponible en Windows y **traceroute**, utilidad similar, está disponible en Linux y Cisco IOS. Además de utilizarse para probar la conectividad, **tracert** puede utilizarse para verificar la latencia de red.

Por ejemplo, cuando un explorador Web no se conecta a un servidor Web, el problema puede estar en cualquier parte entre el cliente y el servidor. Un ingeniero de red puede utilizar el comando **ping** para probar la conectividad de red local o conexiones con pocos dispositivos. En redes complejas se utiliza el comando **tracert**. Se ha discutido mucho el tema sobre dónde comenzar las pruebas de conectividad y por lo general depende de la experiencia del ingeniero de red y de la familiaridad con la red.

Ping y **tracert** utilizan el Control Message Protocol (ICMP) para enviar mensajes entre dispositivos. ICMP es un protocolo de capa de red de TCP/IP, definido por primera vez en RFC 792, en septiembre del año 1981. Los tipos de mensajes ICMP se expandieron más tarde en RFC 1700.

Escenario

En esta práctica de laboratorio, se examinarán los comandos **ping** y **tracert**, y se utilizarán las opciones de comando para modificar el comportamiento del comando. Para que los estudiantes se familiaricen con el uso de comandos, se probarán los dispositivos en el laboratorio de Cisco.

Es probable que el tiempo de demora medido sea menor que el de una red de producción. Esto se debe a que hay poco tráfico de red en el laboratorio Eagle 1.

Tarea 1: Uso del comando ping para verificar la conectividad de la red TCP/IP simple.

El comando **ping** se utiliza para verificar la conectividad de capa de red TCP/IP en la computadora host local u otro dispositivo en la red. El comando puede utilizarse con una dirección IP destino o nombre calificado, como por ejemplo eagle-server.example.com, para probar la funcionalidad de servicios de nombres de dominios (DNS). Sólo se utilizan direcciones IP para esta práctica de laboratorio.

El funcionamiento del comando **ping** es sencillo. La computadora de origen envía una solicitud de eco ICMP al destino. El destino responde con una respuesta de eco. En caso de interrupción entre el origen y el destino, un router puede responder con un mensaje ICMP que establece que el host o la red de destino son desconocidos.

Paso 1: Verificar la conectividad de la capa de red TCP/IP en la computadora host local.

```
C:\> ipconfig
Configuración IP de Windows
Conexión de área local del adaptador Ethernet:
        Sufijo de conexión específica DNS. :
        Dirección IP . . . . . . . . . . . . : 172.16.1.2
        Máscara de subred. . . . . . . . . . : 255.255.0.0
        Gateway por defecto. . . . . . . . . : 172.16.255.254
C:\>
```

Figura 1. Información de red TCP/IP local

1. Abra un terminal de Windows y determine la dirección IP de la computadora host del módulo del grupo con el comando **ipconfig**, como indica la Figura 1.

   El resultado debe ser igual excepto por la dirección IP. Cada computadora host del módulo del grupo debe tener la misma máscara de red y dirección de gateway por defecto; sólo la dirección IP puede ser diferente. Si falta información o si la máscara de subred y el gateway por defecto son diferentes, vuelva a configurar los parámetros de TCP/IP para hacer coincidir las configuraciones para esta computadora host del módulo del grupo.

2. Registre la información sobre la información de red TCP/IP local:

Información TCP/IP	Valor
Dirección IP	
Máscara de subred	
Gateway por defecto	

```
C:\>ping 127.16.1.2❶

Haciendo ping a 127.16.1.2 con 32 bytes de datos:

❷Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
 Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
 Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
 Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128

❸Estadísticas de ping para 127.16.1.2❹ ❺ ❻
     Paquetes: enviados = 4, recibidos = 4, perdidos = 0
     (0% perdidos),
❼Tiempos aproximados de ida y vuelta en milisegundos:
     Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\>
```

Figura 2. Resultado del comando `ping` en el stack TCP/IP local

3. Use el comando **ping** para verificar la conectividad de la capa de red TCP/IP en la computadora host local.

   Cuatro solicitudes de ping se envían al destino en forma predeterminada y se recibe información de respuesta. El resultado debe ser similar al que se visualiza en la Figura 2.

   ❶ Dirección de destino, configurada en la dirección IP para la computadora local.

   ❷ Información de respuesta:

   bytes: tamaño del paquete ICMP.

   tiempo: tiempo transcurrido entre la transmisión y la respuesta.

   TTL: valor TTL predeterminado del dispositivo DESTINATION, menos la cantidad de routers en la ruta. El valor TTL máximo es 255, y para los equipos de Windows más nuevos el valor predeterminado es 128.

   ❸ Resumen de información sobre las respuestas:

   ❹ Paquetes enviados: cantidad de paquetes transmitidos. Se envían cuatro paquetes en forma predeterminada.

   ❺ Paquetes recibidos: cantidad de paquetes recibidos.

   ❻ Paquetes perdidos: diferencia entre la cantidad de paquetes enviados y recibidos.

❼ Información sobre la demora de respuestas, medida en milisegundos. Los tiempos mínimos de ida y vuelta indican enlaces más rápidos. El temporizador de una computadora se configura en 10 milisegundos. Los valores más rápidos de 10 milisegundos se visualizarán como 0.

4. Complete los resultados del comando **ping** en su computadora:

Campo	Valor
Tamaño del paquete	
Cantidad de paquetes enviados	
Cantidad de respuestas	
Cantidad de paquetes perdidos	
Demora mínima	
Demora máxima	
Demora promedio	

Paso 2: Verificar la conectividad de la capa de red TCP/IP en la LAN.

```
C:\> ping 172.16.255.254
Pinging 172.16.255.254 with 32 bytes of data:
Reply from 172.16.255.254: bytes=32 time=1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Figura 3. Resultado del comando ping para el gateway por defecto

1. Use el comando **ping** para verificar la conectividad de la capa de red TCP/IP al gateway por defecto. Los resultados deben ser similares a los que se visualizan en la Figura 3.

   El valor TTL predeterminado de Cisco IOS se configura en 255. Debido a que los datagramas no viajaron al router, el valor TTL devuelto es 255.

2. Complete los resultados del comando **ping** para el gateway por defecto.

Campo	Valor
Tamaño del paquete	
Cantidad de paquetes enviados	
Cantidad de respuestas	
Cantidad de paquetes perdidos	
Demora mínima	
Demora máxima	
Demora promedio	

¿Cuál sería el resultado de una pérdida de conectividad al gateway por defecto?

_____

Paso 3: Verificar la conectividad de la capa de red TCP/IP con una red remota.

```
C:\> ping 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 4. Resultado del comando `ping` para Eagle Server

1. Utilice el comando **`ping`** para verificar la conectividad de la capa de red TCP/IP con un dispositivo en una red remota. En este caso, se utilizará el Eagle Server. Los resultados deben ser similares a los que se visualizan en la Figura 4.

   El valor TTL predeterminado de Linux está configurado en 64. Debido a que los datagramas viajaron a través de dos routers para acceder a Eagle Server, el valor TTL devuelto es 62.

2. Complete los resultados del comando **`ping`** en su computadora:

Campo	Valor
Tamaño del paquete	
Cantidad de paquetes enviados	
Cantidad de respuestas	
Cantidad de paquetes perdidos	
Demora mínima	
Demora máxima	
Demora promedio	

```
C:\> ping 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
El tiempo de respuesta expiró.
El tiempo de respuesta expiró.
El tiempo de respuesta expiró.
El tiempo de respuesta expiró.
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 5. Resultado de un comando `ping` con paquetes perdidos

El comando **`ping`** es extremadamente útil al resolver problemas en la conectividad de red. Sin embargo existen limitaciones. En la Figura 5 el resultado muestra que el usuario no puede acceder a Eagle Server. ¿El problema está en Eagle Server o en un dispositivo de la ruta? El comando **`tracert`**, que se examinará luego, puede mostrar la latencia de red e información de ruta.

Tarea 2: Uso del comando `tracert` para verificar la conectividad de TCP/IP.

El comando **`tracert`** es útil para aprender sobre la latencia de red e información de ruta. En lugar de utilizar el comando **`ping`** para probar la conectividad de cada dispositivo uno por uno al destino, puede utilizarse el comando **`tracert`**.

En los dispositivos Linux y Cisco IOS, el comando equivalente es el **`traceroute`**.

Paso 1: Verificar la conectividad de la capa de red TCP/IP con el comando `tracert`.

1. Abra una terminal de Windows y emita el siguiente comando:

```
C:\> tracert 192.168.254.254
```

```
C:\> tracert 192.168.254.254
Tracing route to 192.168.254.254 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  172.16.255.254
  2    <1 ms    <1 ms    <1 ms  10.10.10.6
  3    <1 ms    <1 ms    <1 ms  192.168.254.254
Trace complete.
C:\>
```

Figura 6. Resultado del comando `tracert` para Eagle Server.

El resultado del comando **`tracert`** debe ser similar al visualizado en la Figura 6.

2. Registre sus resultados en la siguiente tabla:

Campo	Valor
Cantidad máxima de saltos	
Dirección IP del primer router	
Dirección IP del segundo router	
¿Se accedió al destino?	

Paso 2: Observar la salida del comando `tracert` a un host que perdió conectividad de red.

Si hubiera una pérdida de conectividad hacia un dispositivo final, como Eagle Server, el comando **`tracert`** puede proporcionar pistas valiosas en cuanto al origen del problema. El comando **`ping`** muestra la falla pero no proporciona otro tipo de información sobre los dispositivos en la ruta. En cuanto al Diagrama de topología de la práctica de laboratorio Eagle 1, tanto R2-Central como R1-ISP se utilizan para la conectividad entre las computadoras host del módulo del grupo y Eagle Server.

```
C:\> tracert -w 5 -h 4 192.168.254.254
Tracing route to 192.168.254.254 over a maximum of 4 hops
  1    <1 ms    <1 ms    <1 ms  172.16.255.254
  2    <1 ms    <1 ms    <1 ms  10.10.10.6
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.

Trace complete.
C:\>
```

Figura 7. Resultado del comando `tracert`

Consulte la Figura 7. Las opciones se utilizan con el comando **tracert** para reducir el tiempo de espera (en milisegundos), **-w 5** y el número máximo de saltos **-h 4**. Si Eagle Server fuera desconectado de la red, el gateway por defecto respondería de manera adecuada, al igual que R1-ISP. El problema debe estar en la red `192.168.254.0/24`. En este ejemplo, Eagle Server ha sido apagado.

¿Cuál sería el resultado de **tracert** si R1-ISP falló?

_____

¿Cuál sería el resultado de **tracert** si R2-Central falló?

_____

Tarea 3: Desafío

Los valores predeterminados para el comando **ping** normalmente funcionan en casi todas las situaciones de resolución de problemas. A veces, sin embargo, las opciones de **ping** de ajuste más refinado pueden ser útiles. Al ejecutar el comando **ping** sin una dirección de destino se visualizan las opciones presentadas en la Figura 8:

```
C:\> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-
Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout      Timeout in milliseconds to wait for each reply.
C:\>
```

Figura 8. Resultado de un comando `ping` sin dirección de destino

Las opciones más útiles están resaltadas en amarillo. Algunas opciones, como por ejemplo **-t** y **-n,** no funcionan juntas. Otras opciones pueden utilizarse juntas. Experimente con las siguientes opciones:

Para hacer **ping** a la dirección de destino hasta que se detenga, utilice la opción **-t**. Para detener, presione <CTRL> C:

```
C:\> ping -t 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Ping statistics for 192.168.254.254:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>
```

Figura 9: Resultado de un comando ping utilizando la opción -t

Para hacer **ping** una vez al destino y registrar los saltos del router, utilice las opciones **-n** y **-r**, como se muestra en la Figura 10.

Nota: No todos los dispositivos aceptarán la opción **-r**.

```
C:\> ping -n 1 -r 9 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 192.168.254.254: bytes=32 time=1ms TTL=63
    Route:      10.10.10.5 ->
           192.168.254.253 ->
           192.168.254.254 ->
                10.10.10.6 ->
            172.16.255.254
Ping statistics for 192.168.254.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>
```

Figura 10: Resultado de un comando ping utilizando las opciones –n y –r

Tarea 4: Reflexión

Los ingenieros de redes utilizan los comandos **ping** y **tracert** para probar la conectividad de red. El comando **ping** funciona mejor en una conectividad básica. Para probar la latencia y la ruta de red, se prefiere el comando **tracert**.

Se espera que un ingeniero de redes tenga la capacidad de diagnosticar rápidamente y con exactitud las cuestiones relacionadas con la conectividad de redes. El conocimiento sobre protocolos TCP/IP y la práctica con comandos para resolver problemas construyen esa capacidad.

Tarea 5: Limpieza

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 6.7.2: Examen de paquetes ICMP

Diagrama de topología

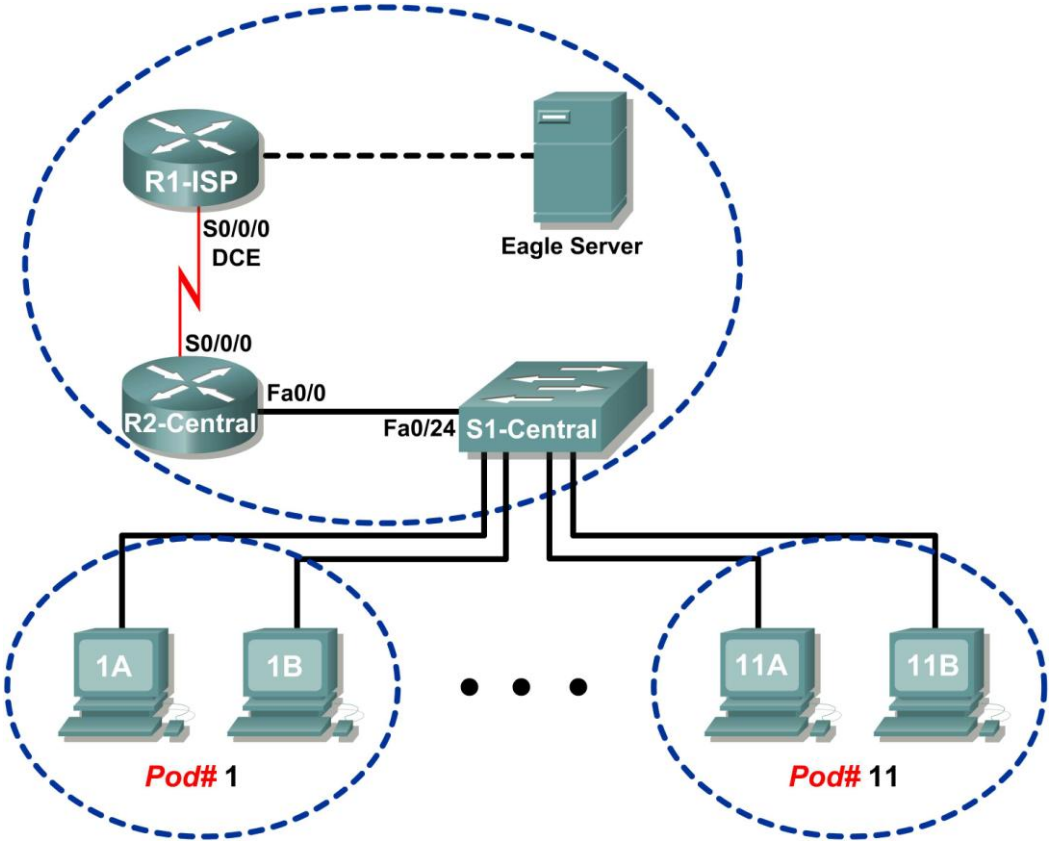


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#***A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Comprender el formato de los paquetes ICMP.
- Usar Wireshark para capturar y examinar mensajes ICMP.

Información básica

El Internet Control Message Protocol (ICMP) se definió por primera vez en RFC 792, en septiembre de 1981. Los tipos de mensajes ICMP luego se expandieron en RFC 1700. ICMP funciona en la capa de red TCP/IP y se usa para intercambiar información entre dispositivos.

Los paquetes ICMP cumplen muchos usos en la red de computadoras actuales. Cuando un router no puede enviar un paquete al host o a la red de destino, se devuelve un mensaje informativo. Los comandos **ping** y **tracert** también envían mensajes ICMP a los destinos y los destinos responden con mensajes ICMP.

Escenario

Con el laboratorio Eagle 1, las capturas de Wireshark se realizan con paquetes ICMP entre los dispositivos de red.

Tarea 1: Comprensión del formato de paquetes ICMP.

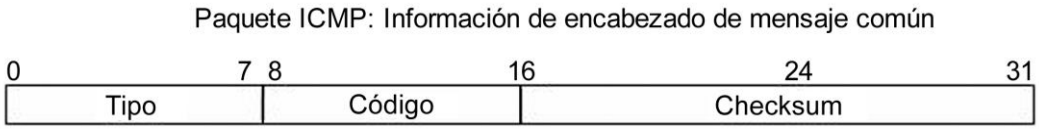


Figura 1. Encabezado de mensajes ICMP

Consulte la figura 1. Los campos de encabezados ICMP son comunes a todos los tipos de mensajes ICMP. Cada mensaje ICMP comienza con un campo Tipo de 8-bits, un campo Código de 8-bits y una Checksum calculada de 16-bits. El tipo de mensaje ICMP describe los campos ICMP restantes. La tabla de la Figura 2 muestra los tipos de mensajes ICMP de RFC 792:

Valor	Significado
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen
5	Redirigir
8	Eco
11	Tiempo superado
12	Problema de parámetros
13	Marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información

Figura 2. Tipos de mensajes ICMP

Los códigos proporcionan información adicional al campo Tipo. Por ejemplo, si el campo Tipo es 3, destino inalcanzable, se devuelve la información adicional sobre el problema al campo Código. La tabla de la Figura 3 muestra los códigos de mensajes para un mensaje Tipo 3 ICMP, destino inalcanzable, de RFC 1700:

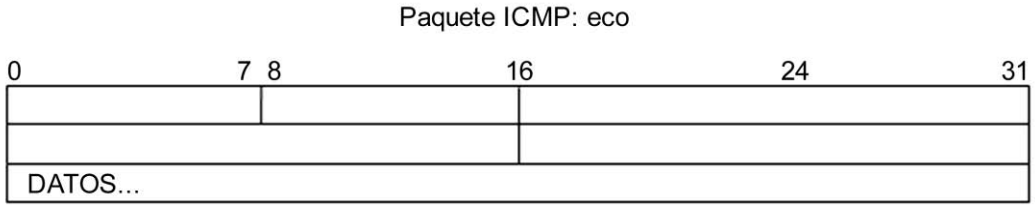
Código Valor	Significado
0	Red inalcanzable
1	Host inalcanzable
2	Protocolo inalcanzable
3	Puerto inalcanzable
4	Se necesita fragmentación y no se configuró un fragmento
5	Falló la ruta origen
6	Red de destino desconocida
7	Host de destino desconocido
8	Host de origen aislado
9	La comunicación con la red de destino se encuentra administrativamente prohibida.
10	La comunicación con el host de destino se encuentra administrativamente prohibida
11	Red de destino inalcanzable para el tipo de servicio
12	Host de destino inalcanzable para el tipo de servicio

Figura 3. Códigos de mensajes ICMP Tipo 3

Complete los campos para la solicitud de eco de paquetes ICMP con la captura de mensajes ICMP que se muestra en la Figura 4. Los valores que comienzan con 0x son números hexadecimales:

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x365c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

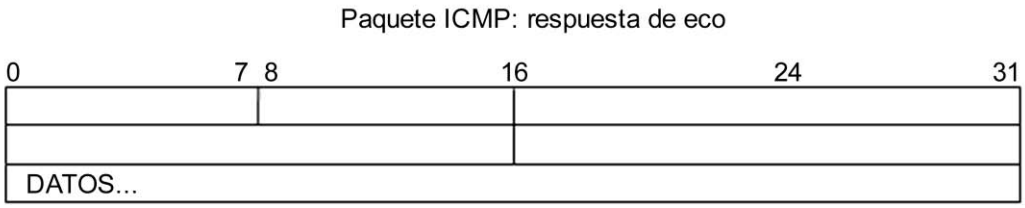
Figura 4. Solicitud de eco de paquetes ICMP



Complete los campos para la respuesta de eco de paquetes ICMP con la captura de mensajes ICMP que se muestra en la Figura 5:

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x3e5c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figura 5. Respuesta de eco de paquetes ICMP



En la capa de red TCP/IP no se garantiza la comunicación entre dispositivos. Sin embargo, ICMP sí proporciona controles mínimos para que una respuesta coincida con la solicitud. A partir de la información proporcionada en el mensaje ICMP anteriormente, ¿cómo sabe el emisor que la respuesta es para un eco específico?

_____

_____

Tarea 2: Utilización de Wireshark para capturar y examinar mensajes ICMP

Figura 6. Sitio de descarga de Wireshark

Si no se ha cargado Wireshark en la computadora host del grupo, se puede descargar desde Eagle Server.

1. Abra un explorador Web, URL FTP://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6, como se muestra en la Figura 6.
2. Haga clic con el botón derecho del mouse sobre el nombre del archivo Wireshark, haga clic en **Guardar enlace como**, y guarde el archivo en la computadora host del grupo.
3. Cuando se haya descargado el archivo, abra e instale Wireshark.

Paso 1: Capturar y evaluar los mensajes de eco ICMP para Eagle Server.

En este paso, Wireshark se usa para examinar los mensajes de eco ICMP.

1. Abra una terminal de Windows en la computadora host del módulo del grupo.
2. Una vez listo, inicie la captura de Wireshark.

```
C:\> ping eagle-server.example.com
Pinging eagle-server.example.com [192.168.254.254] with 32 bytes of
data:
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 7. Respuestas de `ping` exitosas de Eagle Server

3. Desde la terminal de Windows, haga **`ping`** en Eagle Server. Se deben recibir cuatro respuestas exitosas de Eagle Server, como se muestra en la Figura 7.
4. Detenga la captura de Wireshark. Debe haber un total de cuatro solicitudes de eco ICMP y respuestas eco que coincidan, similares a las que se muestran en la Figura 8.

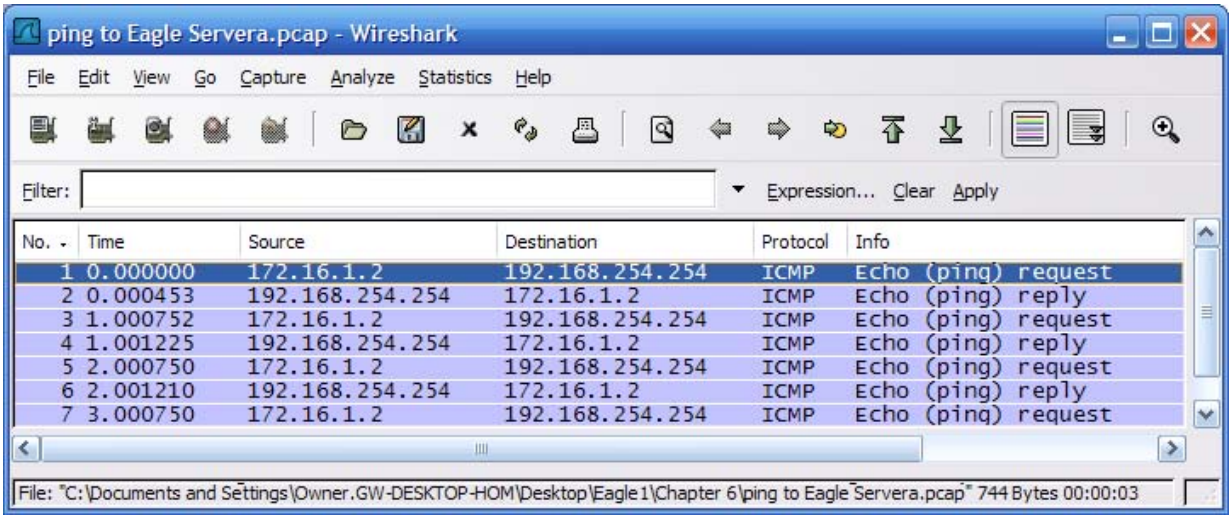


Figura 8. Captura de Wireshark de solicitudes de `ping` y respuestas

¿Qué dispositivo de red responde a la solicitud de eco ICMP? _____

5. Expanda la ventana del medio en Wireshark, y expanda el registro de Internet Control Message Protocol hasta que se visualicen todos los campos. También se necesitará la ventana inferior para examinar el campo Datos.
6. Registre la información del *primer* paquete de solicitud de eco a Eagle Server.

Campo	Valor
Tipo	
Código	
Checksum	
Identificador	
Número de secuencia	
Datos	

¿Existen 32 bytes de datos? _____

7. Registre la información del *primer* paquete de respuesta de eco de Eagle Server:

Campo	Valor
Tipo	
Código	
Checksum	
Identificador	
Número de secuencia	
Datos	

¿Qué campos, de haber alguno, cambian desde la solicitud de eco?

_____

8. Continúe evaluando las solicitudes y respuestas de eco restantes. Complete la siguiente información de cada ping nuevo:

Paquete	Checksum	Identificador	Número de secuencia
Solicitud N.º 2			
Respuesta N.º 2			
Solicitud N.º 3			
Respuesta N.º 3			
Solicitud N.º 4			
Respuesta N.º 4			

¿Por qué cambiaron los valores de Checksum con cada nueva solicitud?

_____

Paso 2: Capturar y evaluar los mensajes de eco ICMP a 192.168.253.1.

En este paso, los pings se envían a un host y red ficticios. Los resultados de captura de Wireshark se evaluarán, y pueden ser sorprendentes.

Intente hacer ping en la dirección IP 192.168.253.1.

```
C:\> ping 192.168.253.1
```

```
C:\> ping 192.168.253.1
Pinging 192.168.253.1 with 32 bytes of data:
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Ping statistics for 192.168.253.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 9. Resultados de pings de un destino ficticio

Vea la Figura 9. En lugar del límite de tiempo de la solicitud, hay una respuesta de eco.

¿Qué dispositivo de red responde a pings para un destino ficticio?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

Figura 10. Captura de Wireshark de un destino ficticio

Las capturas de Wireshark a un destino ficticio se muestran en la Figura 10. Expanda la ventana Wireshark del medio y el registro de Internet Control Message Protocol.

¿Qué tipo de mensaje ICMP se usa para devolver información al emisor?

_____

¿Cuál es el código asociado con el tipo de mensaje?

_____

Paso 3: Capturar y evaluar los mensajes de eco ICMP que exceden el valor TTL.

En este paso, se envían pings con un valor TTL bajo, simulando un destino que es inalcanzable. Haga ping en Eagle Server y establezca el valor TTL para **1**:

```
C:\> ping -i 1 192.168.254.254
```

```
C:\> ping -i 1 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 11. Resultados de pings para un TTL excedido

Vea la Figura 11, que muestra respuestas de ping cuando el valor de TTL ha sido superado.

¿Qué dispositivo de red responde a pings que superaron el valor de TTL?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Figura 12. Captura del valor de TTL excedido

Las capturas de Wireshark a un destino ficticio se muestran en la Figura 12. Expanda la ventana Wireshark del medio y el registro de Internet Control Message Protocol.

¿Qué tipo de mensaje ICMP se usa para devolver información al emisor?

_____

¿Cuál es el código asociado con el tipo de mensaje?

_____

¿Qué dispositivo de red es responsable de la disminución del valor de TTL?

_____

Tarea 3: Desafío

Utilice Wireshark para capturar una sesión **`tracert`** para Eagle Server y luego para 192.168.254.251. Examine el mensaje de TTL ICMP superado. Esto demuestra cómo el comando **`tracert`** rastrea la ruta de red hacia el destino.

Tarea 4: Reflexión

El protocolo ICMP es muy útil al resolver problemas relacionados con la conectividad de red. Sin los mensajes ICMP, un emisor no tiene forma de informar porqué falló una conexión de destino. Se capturaron y evaluaron diferentes valores de tipos de mensajes ICMP con el comando **`ping`**.

Tarea 5: Limpieza

Wireshark pudo haber sido cargado en la computadora host del módulo del grupo. Si se debe eliminar el programa, haga clic en **Inicio > Panel de control > Agregar o quitar programas,** desplácese por la pantalla hasta llegar a Wireshark. Haga clic en el nombre del archivo, luego en **Quitar** y siga las instrucciones para desinstalar el programa.

Elimine cualquier archivo pcap de Wireshark que haya sido creado en la computadora host del módulo del grupo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Actividad 6.7.3: División en subredes de direcciones IPv4, Parte I

Objetivos de aprendizaje

Al completar esta actividad, usted podrá determinar la información de red para una dirección IP y una máscara de red específicas.

Información básica

Esta actividad está diseñada para enseñar a calcular la información de la dirección IP de una red a partir de un determinada dirección IP.

Escenario

Al tener una determinada dirección IP y máscara de red podrá determinar información adicional sobre la dirección IP, como por ejemplo:

- Dirección de red
- Dirección de broadcast de red
- Cantidad total de bits de host
- Cantidad de hosts

Tarea 1: Identificación de la información de red de una dirección IP específica.

Dado:

Dirección IP del host	**172.25.114.250**
Máscara de red	**255.255.0.0 (/16)**

Encontrar:

Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Paso 1: Traducir la dirección IP del host y de la máscara de red en una notación binaria.

Convierta la dirección IP y la máscara de red del host en binario:

	172	**25**	**114**	**250**
Dirección IP	10101100	00011001	01110010	11111010
Máscara de red	11111111	11111111	00000000	00000000
	255	**255**	**0**	**0**

Paso 2: Identificar la dirección de red.

1. Trace una línea debajo de la máscara.
2. Realice una operación AND de bits en la dirección IP y en la máscara de subred.

   Nota: 1 AND 1 da como resultado 1, 0 AND cualquier número da como resultado 0.
3. Exprese el resultado en notación decimal punteada.
4. El resultado es la dirección de red para esta dirección IP del host, la cual es **172.25.0.0.**

	172	**25**	**114**	**250**
Dirección IP	10101100	00011001	01110010	11111010
Máscara de subred	11111111	11111111	00000000	00000000
Dirección de red	10101100	00011001	00000000	00000000
	172	**25**	**0**	**0**

Paso 3: Identificar la dirección de broadcast para la dirección de red

La máscara de red separa la porción de red de la porción del host en la dirección. La dirección de red tiene sólo ceros en la porción del host de la dirección y la dirección de broadcast tiene sólo unos en la porción del host de la dirección.

	172	**25**	**0**	**0**
Dirección de red	10101100	00011001	00000000	00000000
Máscara	11111111	11111111	00000000	00000000
Broadcast.	10101100	00011001	11111111	11111111
	172	**25**	**255**	**255**

Contando la cantidad de bits de host podemos determinar la cantidad total de hosts disponibles para esta red.

Bits del host: 16

Cantidad total de hosts:

$2^{16} = 65.536$

65.536 – 2 = 65.534 (direcciones que no pueden usar la dirección de *sólo ceros*, la dirección de red o la dirección de *sólo unos*, dirección de broadcast).

Agregue esta información en la tabla:

Dirección IP del host	**172.25.114.250**
Máscara de red	**255.255.0.0 (/16)**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host Cantidad de hosts	

Tarea 2: Desafío

Para todos los problemas:

Cree una hoja de cálculo de subredes para mostrar y guardar todo el trabajo para cada problema.

Problema 1

Dirección IP del host	**172.30.1.33**
Máscara de red	**255.255.0.0**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Problema 2

Dirección IP del host	**172.30.1.33**
Máscara de red	**255.255.255.0**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Problema 3

Dirección IP del host	**192.168.10.234**
Máscara de red	**255.255.255.0**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Problema 4

Dirección IP del host	**172.17.99.71**
Máscara de red	**255.255.0.0**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Problema 5

Dirección IP del host	**192.168.3.219**
Máscara de red	**255.255.0.0**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Problema 6

Dirección IP del host	**192.168.3.219**
Máscara de red	**255.255.255.224**
Dirección de red	
Dirección de broadcast de red	
Cantidad total de bits de host	
Cantidad de hosts	

Tarea 3: Limpieza

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Actividad 6.7.4: División en subredes de direcciones IPv4, Parte 2

Objetivos de aprendizaje

Al completar esta actividad, usted podrá determinar la información de subred para una dirección IP y una máscara de subred específicas.

Información básica

Bits prestados

¿Cuántos bits se deben pedir prestados para crear una determinada cantidad de subredes o de hosts por subred?

Con esta tabla es sencillo determinar la cantidad de bits que se deben pedir prestados.

Temas para tener en cuenta:

- Reste 2 de la cantidad disponible de hosts por subred, uno para la dirección de subnet y uno para la dirección de broadcast de la subred.

2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
1,024	512	256	128	64	32	16	8	4	2	1
Cantidad de bits prestados:										
10	9	8	7	6	5	4	3	2	1	1
1,024	512	256	128	64	32	16	8	4	2	1
Hosts o subredes										

Valores posibles de máscara de subred

Debido a que las máscaras de subred pueden ser unos contiguos seguidos por ceros contiguos, la notación decimal punteada convertida puede contener uno de una determinada cantidad de valores:

Decimal	*Binario*
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Escenario

Al tener una determinada dirección IP, máscara de red y máscara de subred podrá determinar información adicional sobre la dirección IP, como por ejemplo:

- La dirección de subred de esta subred
- La dirección de broadcast de esta subred
- El rango de direcciones de host para esta subred
- La cantidad máxima de subredes para esta máscara de subred
- La cantidad de hosts para cada subred
- La cantidad de bits de subred
- El número de esta subred

Tarea 1: Identificación de la información de subred de una dirección IP y de la máscara de subred específicas.

Dado:

Dirección IP del host	**172.25.114.250**
Máscara de red	**255.255.0.0 (/16)**
Máscara de subred	**255.255.255.192 (/26)**

Encontrar:

Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Paso 1: Traducir la dirección IP del host y de la máscara de subred a notación binaria.

	172	**25**	**114**	**250**
Dirección IP	10101100	11001000	01110010	11111010
	11111111	11111111	11111111	11000000
Máscara de subred	**255**	**255**	**255**	**192**

Paso 2: Identificar la red (o subred) a la cual pertenece esta dirección de host.

1. Trace una línea debajo de la máscara.
2. Realizar una operación AND de bits en la dirección IP y en la máscara de subred.

   Nota: 1 AND 1 da como resultado 1, 0 AND cualquier número da como resultado 0.

3. Exprese el resultado en notación decimal punteada.
4. El resultado es la dirección de subred de esta subred: **172.25.114.192**

	172	25	114	250
Dirección IP	10101100	11001000	01110010	11111010
Máscara de subred	11111111	11111111	11111111	11000000
Dirección de subred	10101100	11001000	01110010	11000000
	172	25	114	192

Agregue esta información en la tabla:

Dirección de subred para esta dirección IP	172.25.114.192

Paso 3: Identificar los bits de la dirección que contienen información de red y los bits que contienen información de host:

1. Trace la *División principal* (M.D.) con una línea ondeada donde terminan los unos de la máscara de red principal (también la máscara si no existiera división en subredes). En el ejemplo, la máscara de red principal es 255.255.0.0, o los 16 primeros bits de la izquierda.
2. Trace la *División de subred* (S.D.) con una línea recta donde terminan los unos en la máscara de subred determinada. La información de red termina donde terminan los unos en la máscara.

		M.D.		S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← 10 bits →		

3. El resultado es la cantidad de bits de subred, que se puede determinar contando simplemente la cantidad de bits entre M.D. y S.D., que en este caso es de 10 bits.

Paso 4: Identificar los rangos de bits para las subredes y los hosts.

1. Rotule el *rango de recuento de subred* entre M.D. y S.D. Este rango contiene los bits que se incrementan para crear los números o direcciones de subred.
2. Rotule el *rango de recuento de host* entre S.D y los últimos bits sobre la derecha. Este rango contiene los bits que se incrementan para crear los números o direcciones de host.

		M.D.		S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← subnet counting range →		←host→ counting range

Paso 5: Identificar el rango de las direcciones de host disponibles de esta subred y la dirección de broadcast de esta subred.

1. Copie todos los bits de red/subred de la dirección de red (es decir, todos los bits que se encuentran antes de S.D.).
2. En la porción del host (a la derecha del S.D.), haga que los bits del host sean sólo ceros, excepto el bit que se encuentra más a la derecha (o el bit menos significativo), que tiene que ser 1. Esto nos proporciona la *primera* dirección IP de host en esta subred, que es la *primera parte* del resultado para el *rango de direcciones de host para esta subred*, que, en el ejemplo, es **172.25.114.193**.
3. A continuación, en la porción del host (a la derecha del S.D.), haga que los bits del host sean sólo unos, excepto el bit que se encuentra más a la derecha (o el bit menos significativo), que tiene que ser 0. Esto nos proporciona la *última* dirección IP de host en esta subred, que es la *última parte* del resultado para el *rango de direcciones de host para esta subred*, que, en el ejemplo, es **172.25.114.254**.
4. En la porción del host (a la derecha del S.D.) haga que todos los bits sean unos. Esto nos proporciona la dirección IP de broadcast de esta subred. Éste es el resultado para *Dirección de broadcast de esta subred*, que en el ejemplo es **172.25.114.255**.

		M.D.		S.D.	
IP Address	10101100	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10101100	11001000	01110010	11	000000
			← subnet → counting range		← host → counting range
First Host	10101100	11001000	01110010	11	000001
	172	25	114		193
Last Host	10101100	11001000	01110010	11	111110
	172	25	114		254
Broadcast	10101100	11001000	01110010	11	111111
	172	25	114		255

Agreguemos parte de esta información en nuestra tabla:

Dirección IP del host	**172.25.114.250**
Máscara de red principal	**255.255.0.0 (/16)**
Dirección de red principal (base)	172.25.0.0
Dirección de broadcast de red principal	172.25.255.255
Cantidad total de bits de host Cantidad de hosts	16 bits o 2^{16} ó 65.536 hosts totales 65.536 – 2 = 65.534 hosts utilizables
Máscara de subred	**255.255.255.192 (/26)**
Cantidad de bits de subred Cantidad de subredes	
Cantidad de bits de host por subred Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Paso 6: Determinar la cantidad de subredes.

La cantidad de subredes se determina por la cantidad de bits que se encuentran en el *rango de recuento de subred* (en este ejemplo, 10 bits).

Use la fórmula 2^n, donde *n* es la cantidad de bits en el *rango de recuento de subred*.

1. $2^{10} = 1024$

Cantidad de bits de subred Cantidad de subredes (todos los 0 usados, no todos los 1 usados)	10 bits $2^{10} = 1024$ subredes

Paso 7: Identificar la cantidad de hosts disponibles por subred.

La cantidad de hosts disponibles por subred se determina por la cantidad de bits de host (en el ejemplo, 6 bits) menos 2 (1 por la dirección de subred y 1 por la dirección de broadcast de la subred).

$2^6 – 2 = 64 – 2 = 62$ hosts por subred

Cantidad de bits de host por subred Cantidad de hosts disponibles por subred	6 bits $2^6 – 2 = 64 – 2 = 62$ hosts por subred

Paso 8: Respuestas finales

Dirección IP del host	**172.25.114.250**
Máscara de subred	**255.255.255.192 (/26)**
Cantidad de bits de subred Cantidad de subredes	10 bits 2^{10} = 1024 subredes
Cantidad de bits de host por subred Cantidad de hosts disponibles por subred	6 bits $2^6 – 2 = 64 – 2 = 62$ hosts por subred
Dirección de subred para esta dirección IP	172.25.114.192
Dirección IP del Primer host en esta subred	172.25.114.193
Dirección IP del Último host en esta subred	172.25.114.254
Dirección de broadcast para esta subred	172.25.114.255

Tarea 2: Desafío.

Para todos los problemas:

Cree una hoja de cálculo de subredes para mostrar y guardar todo el trabajo para cada problema.

Problema 1

Dirección IP del host	**172.30.1.33**
Máscara de subred	**255.255.255.0**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Problema 2

Dirección IP del host	**172.30.1.33**
Máscara de subred	**255.255.255.252**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Problema 3

Dirección IP del host	**192.192.10.234**
Máscara de subred	**255.255.255.0**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Problema 4

Dirección IP del host	**172.17.99.71**
Máscara de subred	**255.255.0.0**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Problema 5

Dirección IP del host	**192.168.3.219**
Máscara de subred	**255.255.255.0**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Problema 6

Dirección IP del host	**192.168.3.219**
Máscara de subred	**255.255.255.252**
Cantidad de bits de subred	
Cantidad de subredes	
Cantidad de bits de host por subred	
Cantidad de hosts disponibles por subred	
Dirección de subred para esta dirección IP	
Dirección IP del Primer host en esta subred	
Dirección IP del Último host en esta subred	
Dirección de broadcast para esta subred	

Tarea 3: Limpieza

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 6.7.5: configuración de subred y router

Diagrama de topología

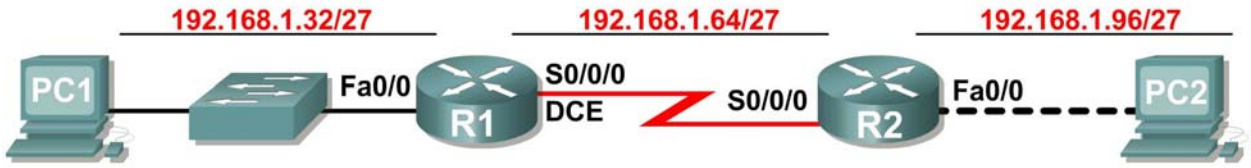


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/0			No aplicable
	S0/0/0			No aplicable
R2	Fa0/0			No aplicable
	S0/0/0			No aplicable
PC1	NIC			
PC2	NIC			

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Dividir en subredes un espacio de dirección según determinados requisitos.
- Asignar las direcciones correspondientes a interfaces y documentos.
- Configurar y activar las interfaces seriales y FastEthernet.
- Probar y verificar las configuraciones.
- Reflexionar sobre la implementación de la red y documentarlo.

Escenario

En esta actividad de laboratorio, el usuario diseñará y aplicará un esquema de direccionamiento IP para la topología presentada en el Diagrama de topología. Se proporcionará un bloque de direcciones, al que debe dividir en subredes para brindar un esquema de direccionamiento lógico para la red. Por lo tanto los routers estarán listos para la configuración de la dirección de la interfaz de acuerdo con el esquema de direccionamiento IP del usuario. Una vez que se complete la configuración, verifique que la red esté funcionando adecuadamente.

Tarea 1: División en subredes del espacio de dirección.

Paso 1: Examine los requisitos de la red.

Se ha suministrado al usuario el espacio de dirección 192.168.1.0/24 para que lo utilice en el diseño de red. La red consta de los siguientes elementos:

- La LAN conectada al router R1 requiere suficientes direcciones IP para admitir 15 hosts.
- La LAN conectada al router R2 requiere suficientes direcciones IP para admitir 30 hosts.
- El enlace entre el router R1 y el router R2 requiere direcciones IP en cada extremo del enlace.

El plano debe tener subredes de igual tamaño y utilizar los tamaños de subredes más pequeños que incorporarán la cantidad adecuada de hosts.

Paso 2: Considere las siguientes preguntas al crear el diseño de red.

¿Cuántas subredes se necesitan para esta red? _____

¿Cuál es la máscara de subred de esta red en formato decimal punteado? _____

¿Cuál es la máscara de subred de la red en formato de barra diagonal? _____

¿Cuántos hosts utilizables existen en cada subred? _____

Paso 3: Asigne direcciones de subred al Diagrama de topología.

1. Asigne la segunda subred a la red conectada al router R1.
2. Asigne la tercera subred al enlace entre R1 y R2.
3. Asigne la cuarta subred a la red conectada al router R2.

Tarea 2: Identificar las direcciones de interfaz.

Paso 1: Asigne las direcciones correspondientes para las interfaces del dispositivo.

1. Asigne la primera dirección de host válida en la segunda subred para la interfaz LAN en R1.
2. Asigne la última dirección de host válida en la segunda subred para PC1.
3. Asigne la primera dirección de host válida en la tercera subred para la interfaz WAN en R1.
4. Asigne la última dirección de host válida en la tercera subred para la interfaz WAN en R2.
5. Asigne la primera dirección de host válida en la cuarta subred para la interfaz LAN de R2.
6. Asigne la última dirección de host válida en la cuarta subred para PC2.

Paso 2: Documente las direcciones a utilizarse en la tabla proporcionada debajo del Diagrama de topología.

Tarea 3: Configuración de las direcciones seriales y FastEthernet.

Paso 1: Configure las interfaces del router.

Configure las interfaces en R1 y R2 con las direcciones IP del diseño de red. Observe que para completar la actividad en el Packet Tracer es necesario utilizar la ficha configuración. Cuando haya finalizado, asegúrese de guardar la configuración en ejecución para la NVRAM del router.

Paso 2: Configure las interfaces de la PC.

Configure las interfaces Ethernet de PC1 y PC2 con las direcciones IP y gateways por defecto del diseño de red.

Tarea 4: Verificar las configuraciones.

Responda las siguientes preguntas para verificar que la red esté funcionando correctamente.

¿Es posible hacer ping al gateway por defecto desde el host conectado a R1? _____

¿Es posible hacer ping al gateway por defecto desde el host conectado a R2? _____

¿Es posible hacer ping a la interfaz serial 0/0/0 de R2 desde R1? _____

¿Es posible hacer ping a la interfaz serial 0/0/0 de R2 desde R1? _____

La respuesta a las preguntas anteriores debe ser **sí**. En caso en que fallen los pings mencionados arriba, verifique las configuraciones y conexiones físicas.

Tarea 5: Reflexión

¿Existen dispositivos en la red que no puedan hacer ping entre sí?

_____

_____

¿Qué falta en la red que impide la comunicación entre estos dispositivos?

_____

_____

6.8.1: Desafío de integración de habilidades: Planificación de subredes y configuración de direcciones IP

Diagrama de topología

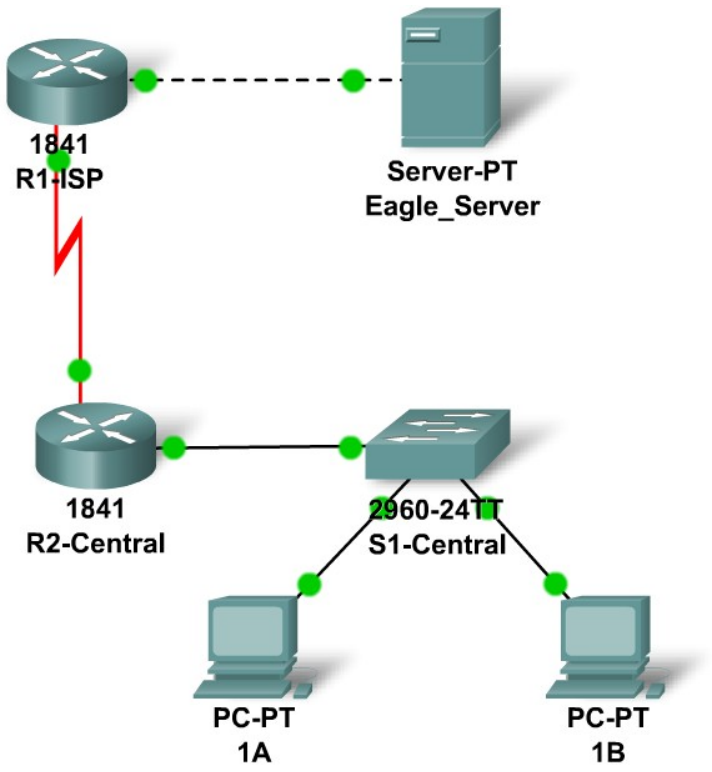


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0			No aplicable
	S0/0/0			No aplicable
R2-Central	Fa0/0			No aplicable
	S0/0/0			No aplicable
PC1A	NIC			
PC1B	NIC			
Eagle Server	NIC			

Objetivos de aprendizaje

- planificación de subredes IP
  - Practicar de las habilidades para división en subredes.
- Creación de la red.
  - Conectar dispositivos con Ethernet y con cables seriales.
- Configuración de la red.
  - Aplicar el esquema de división en subredes a las interfaces del servidor, de las PC y del router; configurar servicios y enrutamiento estático.
- Probar la red.
  - Usar ping, rastreo, tráfico Web, herramienta **Inspeccionar**.

Información básica

Se le ha pedido que implemente la topología del laboratorio estándar, pero con un esquema de direccionamiento IP. Utilizará muchas habilidades que ha aprendido hasta ahora en este curso.

Tarea 1: Planificación de subredes IP.

Recibió un bloque de direcciones IP de 192.168.23.0 /24. Debe prever las redes existentes y el futuro crecimiento.

Las asignaciones de subred son:

- 1.ª subred, LAN actual de estudiantes (fuera del router R2-Central), hasta 60 hosts;
- 2.ª subred, LAN futura de estudiantes, hasta 28 hosts;
- 3.ª subred, LAN ISP existente, hasta 12 hosts;
- 4.ª subred, LAN futura ISP, hasta 8 hosts;
- 5.ª subred, WAN existente, enlace punto a punto;
- 6.ª subred, WAN futura, enlace punto a punto;
- 7.ª subred, WAN futura, enlace punto a punto;

Dirección IP de la interfaz:

- Para el servidor, configure la segunda dirección IP más utilizable en la subred ISP LAN existente.
- Para la interfaz F0/0 de R1-ISP configure la dirección IP más utilizable en la subred ISP LAN existente.
- Para la interfaz F0/0/0 de R1-ISP configure la dirección más utilizable en la subred WAN existente.
- Para la interfaz F0/0/0 de R2-Central use la dirección menos utilizable en la subred WAN existente.
- Para la interfaz F0/0 de R2-Central use la dirección más utilizable en la subred LAN de estudiante existente.
- Para los hosts 1A y 1B use las dos primeras direcciones IP (las dos direcciones menos utilizables) de la subred LAN de estudiantes existente.

Configuraciones adicionales:

- Para las PC 1A y 1B, además de la configuración IP, configúrelos para usar servicios DNS.
- Para el servidor, habilite los servicios DNS, use el nombre de dominio eagle-server.example.com y habilite los servicios HTTP.
- Para la interfaz serial del router R1-ISP necesitará establecer la frecuencia de reloj (un mecanismo de tiempo necesario en el extremo DCE de enlaces seriales) en 64000.
- No se necesita frecuencia de reloj en el lado DTE, en este caso, la interfaz serial de R2-Central.

Tarea 2: Finalización de la creación de la red en el Packet Tracer.

Agregue cables donde sea necesario.

- Conecte un cable DCE serial a R1-ISP S0/0/0 con el otro extremo de R2-Central S0/0/0.
- Conecte la PC 1A al primer puerto FastEhernet en el switch S1-Central.
- Conecte la PC 1B al segundo puerto FastEhernet en el switch S1-Central.
- Conecte la interfaz Fa0/0 del router R2-Central al puerto FastEthernet más alto del switch S1-Central.
- Para todos los dispositivos asegúrese de que estén encendidos tanto el dispositivo como las interfaces.

Tarea 3: Configuración de la red.

Deberá configurar el servidor, ambos routers y las dos PC. No será necesario que configure el switch ni que IOS CLI configure los routers. Parte de la configuración del router ya la realizó: todo lo que debe hacer es configurar las rutas estáticas y las interfaces a través de GUI. La ruta estática en R1-ISP debe apuntar a la subred LAN de estudiante existente a través de la dirección IP de la interfaz serial de R2-Central; la ruta estática en R2-Central tiene que ser una ruta estática que apunta a través de la dirección IP de la interfaz serial de R1-ISP. Estos procedimientos se explicaron en el Capítulo 5: Desafío de integración de aptitudes.

Tarea 4: Prueba de la red.

Use ping, rastreo, tráfico Web, herramienta **Inspeccionar**. Rastree el flujo del paquete en el modo Simulación, con HTTP, DNS, TCP, UDP e ICMP visible, para probar su comprensión de cómo funciona la red.

Tarea 5: Reflexión

¡Piense cuánto ha aprendido hasta ahora! La práctica de las habilidades de división de subredes IP y de construcción de redes, y las habilidades de prueba y configuración le servirán mucho a lo largo de los cursos sobre conexiones de redes.

Práctica de laboratorio 7.5.2: Examen de trama

Diagrama de topología

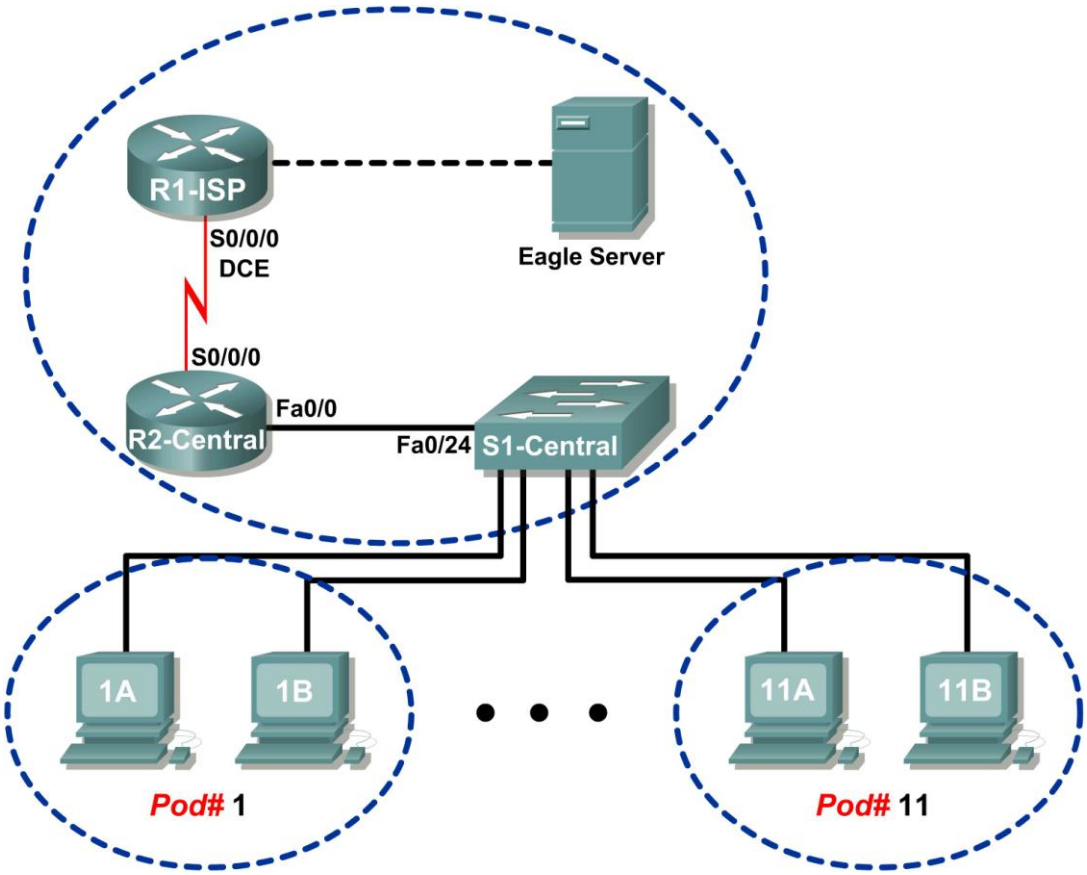


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#***A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

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

Información básica

Cuando los protocolos de capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas OSI y se encapsulan en la trama de la Capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si el protocolo de capa superior es TCP/IP y el acceso al medio es Ethernet, la encapsulación de la trama de la Capa 2 será Ethernet II.

Cuando se aprende sobre los conceptos de la Capa 2, es útil analizar la información del encabezado de la trama. El encabezado de la trama de Ethernet II se examinará en esta práctica de laboratorio. Las tramas de Ethernet II pueden admitir diversos protocolos de la capa superior, como TCP/IP.

Escenario

Se utiliza Wireshark para capturar y analizar los campos de encabezado de tramas de Ethernet II. Si no se cargó Wireshark en la computadora host del módulo, lo puede descargar desde el URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter7/`, archivo `wireshark-setup-0.99.4.exe`.

El comando **`ping`** de Windows se usa para generar el tráfico de red para que Wireshark capture.

Tarea 1: Explicación de los campos de encabezado en una trama de Ethernet II.

El formato de una trama de Ethernet II se muestra en la Figura 1.

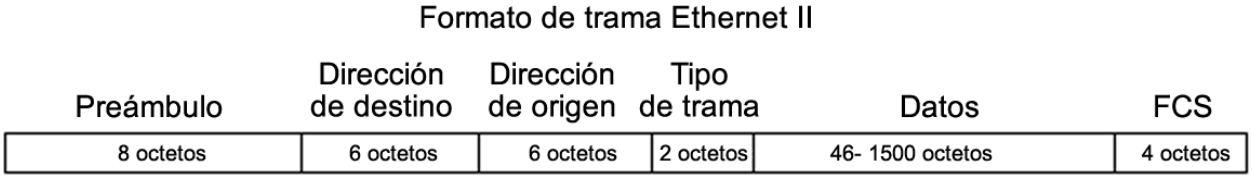


Figura 1. Formato de la trama de Ethernet II

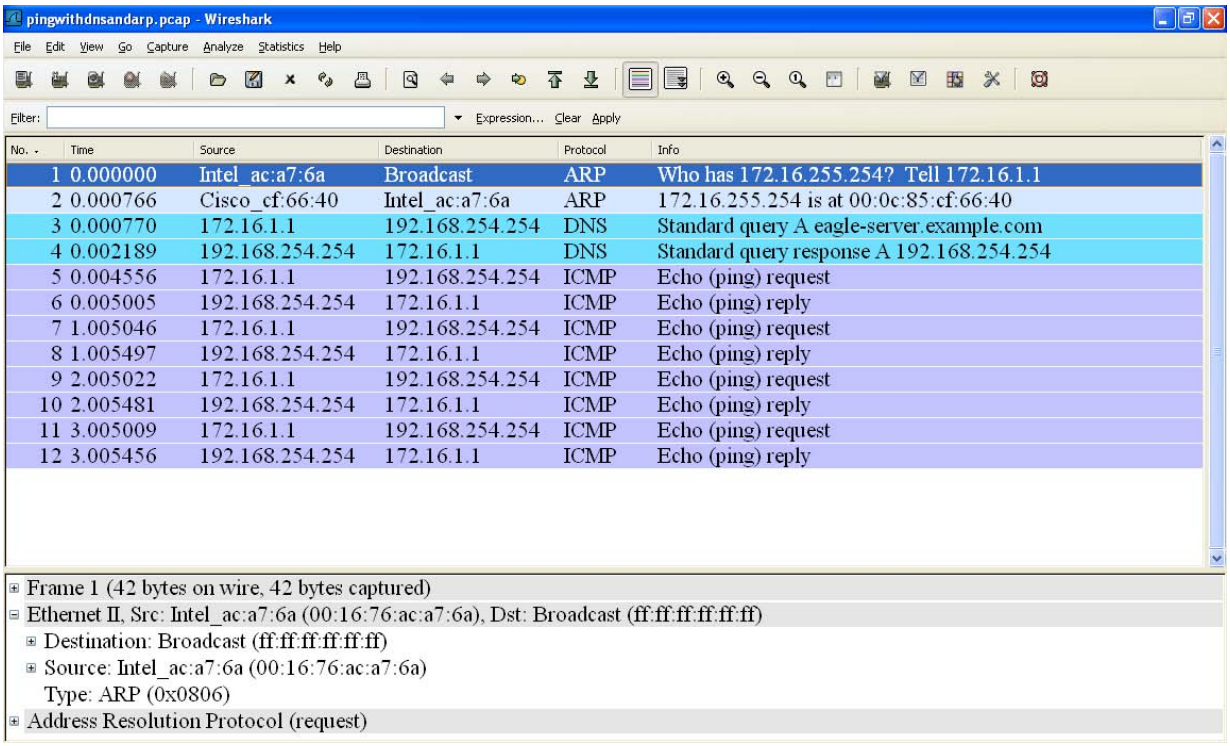


Figura 2. Captura de Wireshark del comando `ping`

En la Figura 2, la ventana de la Lista de panel muestra una captura de Wireshark del comando **`ping`** entre una computadora host del módulo y Eagle Server. La sesión comienza con el protocolo ARP haciendo consultas para la dirección MAC del router de Gateway, seguida de una consulta DNS. Finalmente, el comando **`ping`** emite solicitudes de eco.

En la Figura 2, la ventana de Detalles del paquete muestra la información detallada de la Trama 1. Se puede obtener la siguiente información de la trama de Ethernet II utilizando esta ventana:

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	`ff:ff:ff:ff:ff:ff`	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 bytes, expresado como 12 dígitos hexadecimales, `0-9, A-F`. Un formato común es `12:34:56:78:9A:BC`. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC). Remítase a http://www.neotechcc.org/forum/macid.htm para obtener una lista de códigos del fabricante. Los últimos seis dígitos hexadecimales, `ac:a7:6a`, representan el número de serie de NIC. La dirección de destino puede ser un broadcast que contiene sólo `1` o unicast. La dirección de origen es siempre unicast.
Dirección de origen	`00:16:76:ac:a7:6a`	
Tipo de trama	`0x0806`	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior admitidos por Ethernet II. Dos tipos

Campo	Valor	Descripción
		comunes de trama son: Valor Descripción 0x0800 Protocolo IPv4 0x0806 Address resolution protocol (ARP)
Datos	ARP	Contiene el protocolo del nivel superior encapsulado. El campo de datos está entre 46 y 1500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica.

¿Cuál es el significado de sólo **1** en el campo de dirección de destino?

_____

_____

Conteste las siguientes preguntas sobre la dirección MAC de origen y de destino, con la información que contiene la ventana de Lista de paquetes para la **primera** trama.

Dirección de destino:

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

Dirección de origen:

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

Conteste las siguientes preguntas sobre la dirección MAC de origen y de destino, con la información que contiene la ventana de Lista de paquetes para la **segunda** trama.

Dirección de destino:

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

Dirección de origen:

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

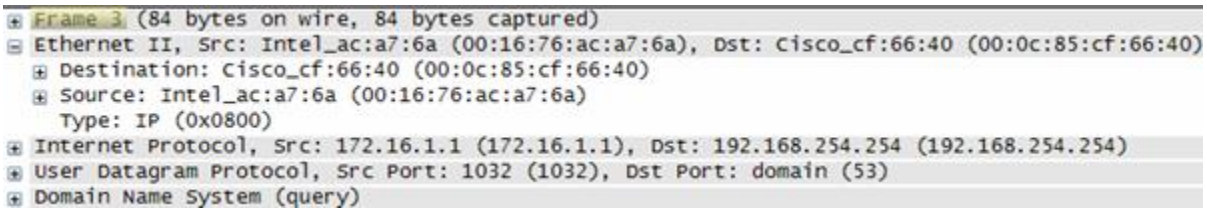


Figura 3. Campos de Trama 3

La figura 3 contiene una vista ampliada de la captura de Wireshark de Trama 3. Utilice la información para completar la siguiente tabla:

Campo	Valor
Preámbulo	
Dirección de destino	
Dirección de origen	
Tipo de trama	
Datos	
FCS	

En la siguiente tarea, Wireshark se utilizará para capturar y analizar paquetes capturados en la computadora host del módulo.

Tarea 2: Utilización de Wireshark para capturar y analizar tramas de Ethernet II.

Paso 1: Configurar Wireshark para las capturas de paquetes.

Prepare Wireshark para las capturas. Haga clic en **Captura > Interfaz**, y luego haga clic en el botón de inicio que corresponde a la dirección IP de interfaz 172.16.x.y. Con esta acción se inicia la captura de paquetes.

Paso 2: Comenzar a hacer ping a Eagle Server y capturar la sesión.

Abra una ventana terminal de Windows. Haga clic en **Inicio > Ejecutar**, escriba **cmd** y haga clic en **Aceptar**.

```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\> ping eagle-server.example.com

Pinging eagle-server.example.com [192.168.254.254] with 32 bytes of data:

Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 4. Ping a eagle-server.example.com

Haga ping a eagle-server.example.com como se muestra en la Figura 4. Cuando el comando haya finalizado la ejecución, detenga las capturas de Wireshark.

Paso 3: Analizar la captura de Wireshark.

La ventana de la Lista de paquetes de Wireshark debe comenzar con una solicitud y respuesta ARP para la dirección MAC del Gateway. Luego, se realiza una solicitud DNS para la dirección IP de eagle-server.example.com. Finalmente, se ejecuta el comando **ping**. La captura debe verse similar a la que se mostró en la Figura 2.

Utilice la captura de Wireshark del comando **ping** para contestar las siguientes preguntas:

Información de la dirección MAC de la computadora del módulo.

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

Información de la dirección MAC de R2-Central:

Dirección MAC: _____
Fabricante de NIC: _____
Número de serie de NIC: _____

Un estudiante de otra escuela quisiera saber la dirección MAC para Eagle Server. ¿Qué le diría al estudiante?

¿Cuál es el valor del tipo de trama de Ethernet II para una solicitud ARP? _____

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta ARP? _____

¿Cuál es el valor del tipo de trama de Ethernet II para una solicitud ARP? _____

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta de solicitud DNS? _____

¿Cuál es el valor del tipo de trama de Ethernet II para un eco ICMP? _____

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta de eco ICMP? _____

Tarea 3: Desafío

Utilice Wireshark para capturar sesiones de otros protocolos TCP/IP, como FTP y HTTP. Analice los paquetes capturados y verifique que el tipo de trama de Ethernet II continúe siendo `0x0800`.

Tarea 4: Reflexión

En esta práctica de laboratorio se examinó la información del encabezado de trama de Ethernet II. Un campo de preámbulo contiene siete bytes de secuencias que alternan `0101`, y un byte que indica el inicio de la trama, `01010110`. Cada una de las direcciones MAC de origen y de destino contiene 12 dígitos hexadecimales. Los primeros seis dígitos hexadecimales contienen el fabricante de la NIC y los últimos seis dígitos contienen el número de serie de NIC. Si la trama es broadcast, la dirección MAC de destino contiene sólo 1. Un campo del tipo de trama de 4 bytes contiene un valor que indica el protocolo en el campo de datos. El valor para IPv4 es `0x0800`. El campo de datos es variable y contiene el protocolo de capa superior encapsulado. Al final de la trama, se utiliza el valor FCS de 4 bytes para verificar que no hubo errores durante la transmisión.

Tarea 5: Limpieza

Se instaló Wireshark en la computadora host del módulo. Si debe desinstalarlo, haga clic en **Inicio > Panel de control**. Abra **Agregar o quitar programas**. Marque Wireshark y haga clic en **Quitar**.

Elimine todos los archivos creados durante la práctica de laboratorio en la computadora host del módulo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

7.6.1: Desafío de integración de capacidades: Temas relacionados con la capa de enlace de datos

Diagrama de topología

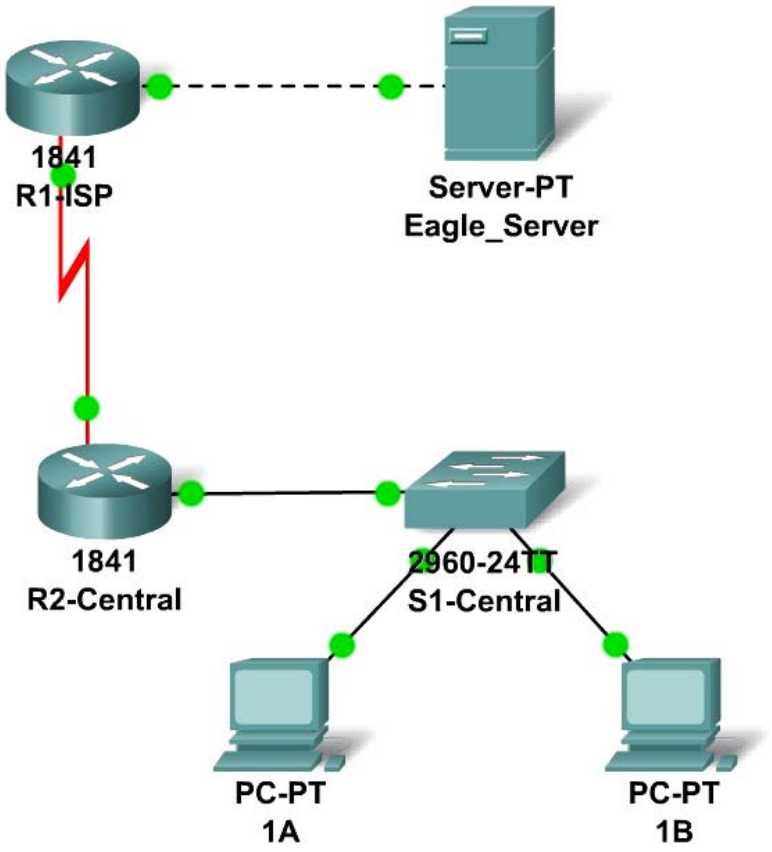


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0			No aplicable
	S0/0/0			No aplicable
R2-Central	Fa0/0			No aplicable
	S0/0/0			No aplicable
PC1A	NIC			
PC1B	NIC			
Eagle Server	NIC			

Objetivos de aprendizaje

- Planificación de subredes IP
  - Practicar de las habilidades para división en subredes.
- Creación de la red.
  - Conectar dispositivos con Ethernet y con cables seriales.
- Configuración de la red.
  - Aplicar el esquema de división en subredes a las interfaces del servidor, de las PC y del router; configurar servicios y enrutamiento estático.
- Probar la red.
  - Usar ping, rastreo, tráfico Web, herramienta **Inspeccionar**.

Información básica

Las tarjetas de interfaz de red (NIC) son a veces consideradas dispositivos de Capa 2 y 1 (o componentes de Capa 2 y 1 de dispositivos que funcionan en las 7 capas). A veces la tarjeta de interfaz de red para una conexión serial, utilizada generalmente en conexiones WAN, se denomina una tarjeta de interfaz WAN o WIC. En este desafío, debe agregar un WIC a un dispositivo para completar la red. Además, se le pidió que implemente un esquema de direccionamiento IP nuevo en la topología de laboratorio de exploración.

Tarea 1: Planificación de subredes IP.

Recibió un bloque de direcciones IP de 172.16.0.0 /22. Debe prever las redes existentes y el futuro crecimiento.

Las asignaciones de subred son:

- 1.ª subred, LAN de estudiantes actual, hasta 400 hosts (Fa0/0 en R2-Central);
- 2.ª subred, LAN futura de estudiantes, hasta 180 hosts (aún no implementada);
- 3.ª subred, LAN del ISP actual, hasta 40 hosts (Fa0/0 en R1-ISP);
- 4.ª subred, LAN de ISP futuro, hasta 18 hosts (aún no implementada);
- 5.ª subred, WAN actual, enlace punto a punto (S0/0/0 en R1-ISP y en R2-Central);
- 6.ª subred, WAN futura, enlace punto a punto (aún no implementada);
- 7.ª subred, WAN futura, enlace punto a punto; (aún no implementada).

Dirección IP de la interfaz:

- Para el servidor, configure la segunda dirección IP más utilizable en la subred ISP LAN.
- Para la interfaz F0/0 de R1-ISP configure la dirección IP más utilizable en la subred ISP LAN.
- Para la interfaz F0/0/0 de R1-ISP configure la dirección más utilizable en la subred WAN existente.
- Para la interfaz F0/0/0 de R2-Central use la dirección menos utilizable en la subred WAN existente.
- Para la interfaz F0/0 de R2-Central use la dirección más utilizable en la subred LAN de estudiante existente.
- Para las PC 1A y 1B use las dos primeras direcciones IP (las dos direcciones menos utilizables) de la subred LAN de estudiantes existente.

Configuraciones adicionales:

- Para las PC 1A y 1B, además de la configuración IP, configúrelos para usar servicios DNS.
- Para el servidor, habilite los servicios DNS, use el nombre de dominio eagle-server.example.com y habilite los servicios HTTP.

Tarea 2: Termine de crear la red en el Packet Tracer prestando atención a algunos temas relacionados con la Capa 2.

En el router R2-Central falta una tarjeta de interfaz de red para la conexión serial con R1-ISP: agregue un WIC-2T en la ranura del lado derecho. Además, en R2-Central, Fa0/0 está desactivada, enciéndala. Conecte un cable DCE serial a R1-ISP S0/0/0, con el otro extremo en R2-Central S0/0/0. Para todos los dispositivos, asegúrese de tener encendidos todos los dispositivos e interfaces.

Tarea 3: Configuración de la red.

Deberá configurar el servidor, ambos routers y las dos PC. No será necesario que configure el switch ni que IOS CLI configure los routers. Parte de la configuración del router ya la realizó: todo lo que debe hacer es configurar las rutas estáticas y las interfaces a través de GUI. La ruta estática en R1-ISP debe apuntar a la subred LAN de estudiante existente a través de la dirección IP de la interfaz serial de R2-Central; la ruta estática en R2-Central tiene que ser una ruta estática que apunta a través de la dirección IP de la interfaz serial de R1-ISP. Se explicaron estos procedimientos en el Capítulo 5 Desafío de integración de aptitudes y se practicaron en el Capítulo 6 Desafío de integración de aptitudes.

Tarea 4: Prueba de la red.

Use ping, rastreo, tráfico Web, herramienta **Inspeccionar**. Rastree el flujo del paquete en el modo Simulación, con HTTP, DNS, TCP, UDP e ICMP visible, para probar su comprensión de cómo funciona la red. Observe en particular qué encapsulación de la Capa 2 se utiliza en cada paso de los tramos del paquete y cómo los encabezados de PDU de la Capa 2 se modifican.

Tarea 5: Reflexión

Considere un paquete de solicitud de eco ICMP enviado desde la PC 1A al Servidor Eagle y el paquete de respuesta de eco ICMP que se obtiene. ¿Qué direcciones permanecen iguales en esta situación y qué direcciones se modifican?

Práctica de laboratorio 8.4.1: Actividad de laboratorio sobre conectores de medios

Analizador de cables típico

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Pruebe los cables usando un analizador de cables y un multímetro de red
- Familiarizarse con las funciones más comunes de un analizador de cables.
- Verificar diferentes cables según el tipo y los problemas de cableado.

Información básica

Los cables de par trenzado no blindado (UTP) categoría 5 (CAT 5) están conectados de acuerdo con la función. Los dispositivos finales, como routers y computadoras host, se conectan a switches con cables de conexión directa CAT 5. Sin embargo, al conectarse, se debe utilizar un cable de conexión cruzada CAT 5. Lo mismo deberá realizarse con los switches. Al conectar un switch con otro, se vuelve a utilizar un cable de conexión cruzada CAT 5.

Los problemas relacionados con cables son una de las causas más comunes de fallas de las redes. Las pruebas básicas de cableado pueden resultar de gran ayuda en la resolución de problemas de cableado realizado con UTP. La calidad de los componentes de cableado utilizados, el tendido e instalación del cable y la calidad de las terminaciones de los conectores serán los factores principales en la determinación de la calidad del cableado.

Se necesitan los siguientes recursos:

- Buenos cables CAT 5 de conexión directa y de conexión cruzada de diferentes colores.
- Cables CAT 5 de conexión directa y de conexión cruzada con conexiones de cables abiertas en el medio o uno o más conductores en cortocircuito en un extremo de diferentes colores y diferentes longitudes.
- Un analizador de cables.
- Un multímetro de red.

El cableado TIA/EIA 568B es diferente del cableado TIA/EIA 568A. Los cables de conexión directa TIA/EIA 568A pueden identificarse por el código de colores. Al igual que en la Figura 2 que aparece a continuación, el diagrama correcto de cableado que comienza con el cable verde y blanco es idéntico en ambos extremos.

Escenario

Primero se determinará visualmente si el tipo de cable CAT 5 es de conexión cruzada o de conexión directa. Después se utilizará el analizador de cables para verificar el tipo de cable, así como también las características comunes disponibles con el analizador.

Por último, se utilizará el analizador de cables para verificar si hay cables en mal estado que no pueden distinguirse con una inspección visual.

Tarea 1: Familiarización con las funciones más comunes de un analizador de cables.

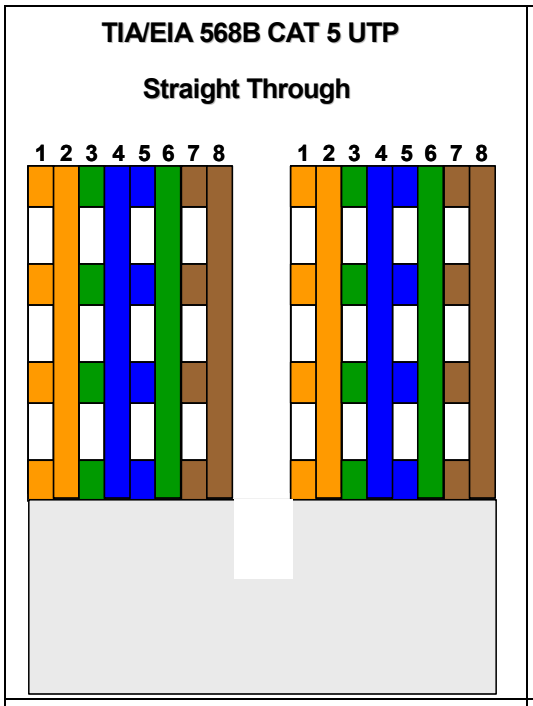


Figura 1. Ubicación del cable de conexión directa

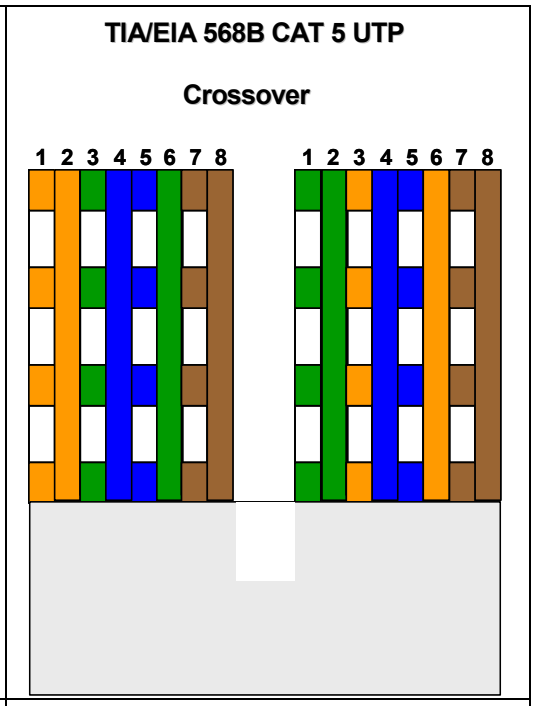


Figura 2. Ubicación del cable de conexión cruzada

Las Figuras 1 y 2 muestran las posiciones de hilos TIA/EIA 568B CAT 5 UTP para un cable de conexión directa y uno de conexión cruzada, respectivamente. Cuando los conectores CAT 5 se mantienen juntos, el color del hilo es una forma rápida de determinar el tipo de cable.

Paso 1: Determinar en forma visual los tipos de cable.

Debe haber dos cables numerados disponibles. Inspeccione visualmente los cables y luego complete la tabla que aparece a continuación con el color del cable, tipo de cable y uso:

Cable N.º	**Cable Color**	**Tipo de cable** (de conexión directa o de conexión cruzada)	**Uso del cable** (encerrar en un círculo el dispositivo correcto)
1			Switch a: host/ switch
2			Switch a: host/ switch

Ahora hay que verificar el tipo de cable y aprender acerca de las características comunes del analizador de cables.

Paso 2: Ejecución de configuración inicial del analizador de cables.

Coloque el analizador de cables en el modo mapa de cableado. Consulte el manual de instrucciones en caso de ser necesario. La función de mapa de cableado muestra qué pins de un extremo del cable se encuentran conectados a qué pins del otro extremo.

Consulte el manual de instrucciones y elija las opciones correctas hasta que el analizador esté configurado con las siguientes características de cableado:

Opción del analizador	Configuración deseada: UTP
CABLE:	UTP
CABLEADO:	10BASE-T o EIA/TIA 4PR
CATEGORÍA:	CATEGORÍA 5
TAMAÑO DEL CABLE	AWG 24
¿CAL a CABLE?	NO
SONIDO:	ENCENDIDO o APAGADO
CONTRASTE DE LCD	De 1 a 10 (el más brillante)

Cuando esté conforme con las características correctas, salga del modo Setup.

Paso 3: Verificar el mapa de cableado del cable.

Figura 3. Acoplador de cables e identificador de cables

Utilice el siguiente procedimiento para verificar cada cable con el acoplador de cables y el identificador de cables LAN que se muestra en la Figura 3. El acoplador y el identificador de cables son accesorios que se incluyen con muchos analizadores de cables.

Coloque el extremo más cercano del cable en el jack RJ45 que lleva el rótulo UTP/FTP en el analizador. Coloque el acoplador hembra RJ 45, RJ 45 en el extremo más alejado del cable e inserte el identificador de cables en el otro extremo del acoplador.

Se mostrará el cableado de ambos extremos del cable. El conjunto superior de números que aparece en la pantalla LCD es el extremo cercano y el conjunto inferior es el extremo lejano.

Efectúe una prueba de Mapa de cableado en cada uno de los cables suministrados y complete la siguiente tabla según los resultados. Para cada cable, ingrese el número y el color e indique si el cable es de conexión directa o de conexión cruzada.

Cable N.º	Cable Color	Cable Tipo (de conexión directa o de conexión cruzada)
1		
2		

Preste atención a cualquier problema que surja durante la prueba:

Paso 4: Verificar la longitud del cable.

Consulte el manual de instrucciones para colocar el analizador de cables en el modo TEST. Si se reinicia, repita los pasos de configuración descritos en el Paso 2. La función LONGITUD del analizador muestra la longitud del cable.

Efectúe una prueba de cable básica en cada uno de los cables y complete la siguiente tabla según los resultados. Para cada cable, escriba el número y el color, la longitud del cable, los resultados de la pantalla del analizador y cuál es el problema, en caso de que lo haya.

Cable N.º	Cable Color	Cable Longitud
1		
2		

Preste atención a cualquier problema que surja durante la prueba:

Repita estos pasos hasta que esté conforme con el uso del analizador de cables. En la siguiente tarea se verificarán cables desconocidos.

Tarea 2: Verificación de diferentes cables según el tipo y los problemas de cableado.

Obtenga al menos 5 cables diferentes del instructor. Haga girar el selector de switch rotativo en el analizador hasta la posición WIRE MAP (mapa de cableado). Si se reinicia, repita los pasos de configuración descritos en la Tarea 1, Paso 2.

Consulte las instrucciones para colocar el analizador de cables en la función WIRE MAP a fin de realizar una prueba de Mapa de cableado en cada uno de los cables suministrados. Luego complete la siguiente tabla según los resultados para cada cable CAT 5 que haya probado. Para cada cable, escriba el número y color, si el cable es de conexión directa o de conexión cruzada, los resultados en la pantalla del analizador y cuál es el problema.

Cable N.º	**Tipo de cable** (Inspección visual)	**Color del cable**	**Tipo de cable** (de conexión directa o de conexión cruzada)	*** Resultados de la prueba**	**Descripción del problema**
1					
2					
3					
4					
5					

* Consulte el manual del producto para obtener una descripción detallada de los resultados de las pruebas de mapa de cableado.

Tarea 3: Ejecución de configuración inicial del multímetro de red

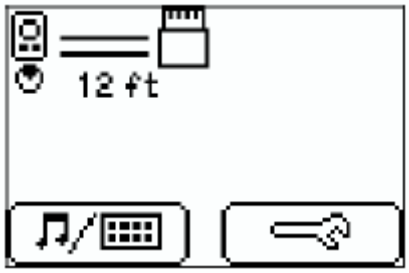
Multímetro de red típico

Paso 1: Encienda el multímetro de red.

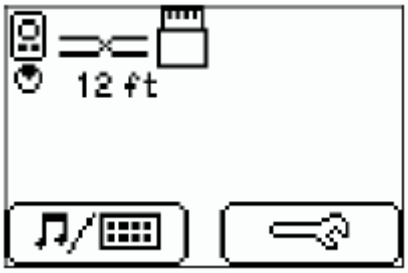
Paso 2: Apáguelo.

Paso 3: Colocar ambos extremos del cable en los puertos LAN y MAP, o equivalente, ubicados en la parte superior del multímetro de red y enciéndalo.

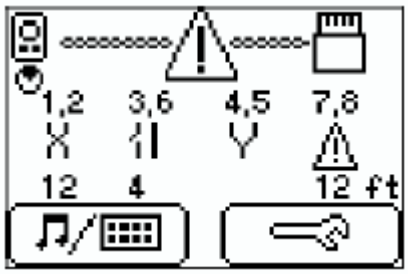
Si es un cable de conexión directa correcto, entonces las dos líneas paralelas (como se ve a continuación) aparecerán en la esquina superior izquierda de la pantalla. Consulte las instrucciones de funcionamiento si su multímetro no muestra dos líneas paralelas es éste paso y en los siguientes.



Si es un cable de conexión cruzada correcto, entonces las dos líneas cruzadas (como se ve a continuación) aparecerán en la esquina superior izquierda de la pantalla.



Si es un cable defectuoso, aparecerá ⚠ y los detalles se mostrarán debajo.



Open (abierto)
Short (corto)
Split (dividir)
Reversal (inversión)
Unknown (desconocido)

Tarea 4: Verificación de la longitud del cable.

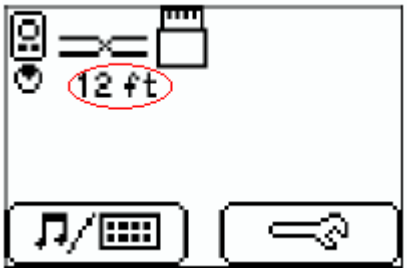
Nota: las instrucciones para verificar un cable son las mismas que para determinar la longitud del cable.

Paso 1: Encienda el multímetro de red.

Paso 2: Apáguelo.

Paso 3: Colocar ambos extremos del cable en los puertos LAN y MAP ubicados en la parte superior del multímetro de red y enciéndalo.

Paso 4: Ubicar la longitud del cable debajo del ícono que indica el tipo de cable (como se muestra a continuación).



Tarea 5: Reflexión

Los problemas relacionados con cables son una de las causas más comunes de fallas de las redes. Los técnicos de red deben ser capaces de determinar cuándo usar cables de conexión directa y cuándo de conexión cruzada CAT 5 UTP.

Se usa un analizador de cables para determinar el tipo de cable, la longitud y el mapa de cableado. En un ambiente de laboratorio, los cables se mueven constantemente y se vuelven a conectar. Un cable que hoy funciona correctamente puede romperse mañana. Esto no es poco común y forma parte del proceso de aprendizaje.

Tarea 6: Desafío

Busque oportunidades para verificar otros cables con el analizador de cables. Los conocimientos adquiridos en esta práctica de laboratorio le permiten resolver rápidamente problemas de tipos de cables incorrectos y problemas de cables rotos.

Tarea 7: Limpieza

El analizador de cables es muy caro y no se lo debe dejar nunca sin supervisión. Al finalizar, devuelva el analizador de cables al instructor.

Pregúntele al instructor dónde devolver los cables usados. Guarde los cables prolijamente para la próxima clase.

8.5.1: Desafío de integración de habilidades: Conexión de dispositivos y exploración de la vista física

Diagrama de topología:

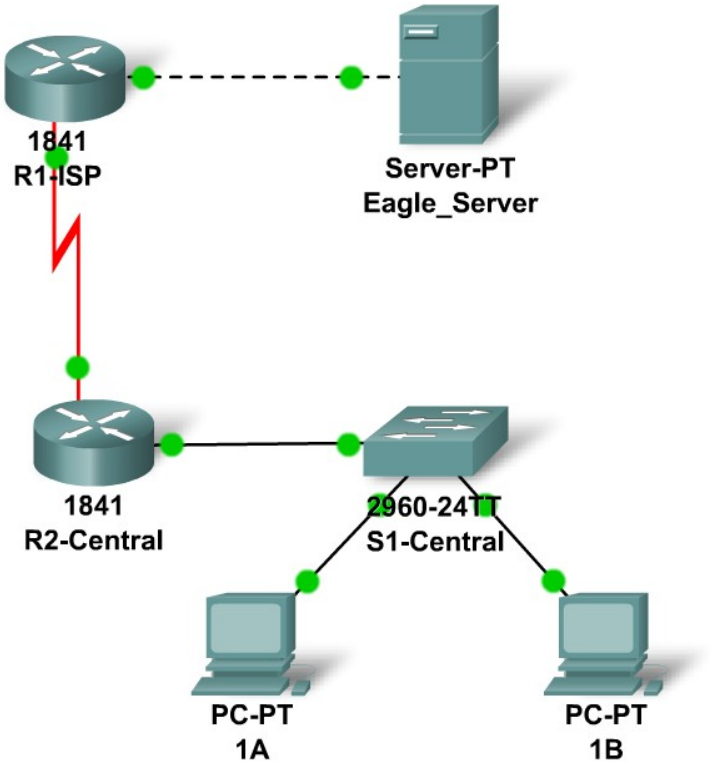


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC1A	NIC	172.16.1.1	255.255.0.0	172.16.255.254
PC1B	NIC	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	NIC	192.168.254.254	255.255.255.0	192.168.254.253

Objetivos de aprendizaje

- Conectar los dispositivos en la configuración estándar del laboratorio
  - Conectar los dispositivos
  - Verificar la conectividad
- Visualizar la configuración estándar de laboratorio en el espacio de trabajo físico
  - Ingresar al espacio físico de trabajo y examinarlo.
  - Examinar la configuración estándar de laboratorio en los distintos niveles del espacio físico de trabajo.

Introducción

Al trabajar en el Packet Tracer, en un entorno de laboratorio o en un contexto corporativo, es importante saber cómo elegir el cable correcto y cómo conectar los dispositivos de manera adecuada. En esta actividad se analizarán configuraciones de dispositivos en el Packet Tracer, se seleccionarán los cables adecuados según la configuración y se conectarán los dispositivos. Esta actividad también explorará la vista física de la red en el Packet Tracer.

Tarea 1: Conexión de los dispositivos en la configuración estándar del laboratorio.

Paso 1: Conectar los dispositivos.

Conecte la PC 1A al primer puerto del switch S1-Central y la PC 1B al segundo puerto del switch S1-Central con los cables adecuados.

Haga clic en el router R2-Central y examine la configuración a través de la ficha **Configuración**. Conecte la interfaz adecuada del router con la Interfaz FastEthernet0/24 del switch S1-Central con el cable correspondiente.

Haga clic en ambos routers y examine la configuración a través de la ficha **Configuración**. Conecte los routers a través de las interfaces adecuadas y con los cables correspondientes

Haga clic en el router R1-ISP y examine la configuración a través de la ficha **Configuración**. Conecte la interfaz correcta del router a la interfaz correspondiente de Eagle Server utilizando el cable adecuado.

Paso 2: Verificación de la conectividad.

Desde el **Indicador de comandos** del **Escritorio** de ambas PC emita el comando **ping 192.168.254.254** a la dirección IP del Servidor Eagle. Si los pings fallan, compruebe sus conexiones y resuelva los problemas hasta que los pings den resultado. Verifique la configuración haciendo clic en el botón **Verificar resultados**.

Tarea 2: Visualización de la configuración estándar del laboratorio en el espacio de trabajo físico.

Paso 1: Ingresar al espacio físico de trabajo y examinarlo.

La mayoría de nuestro trabajo en el Packet Tracer se ha realizado en el espacio de trabajo lógico. En una internetwork, los routers pueden estar en lugares diferentes, ya sea al otro lado de la calle o a través del mundo. El enlace serial entre los routers representa una línea arrendada dedicada entre dos sitios compuesta por un DTE (equipo terminal de datos), como un router, conectado a un DCE (equipo de comunicación de datos), como un módem o una CSU/DSU. El DCE se conecta al loop local de un proveedor de servicios y las conexiones se repiten en el otro extremo del enlace. El espacio físico de trabajo nos permite ver estas relaciones con más claridad.

Ingrese al espacio físico de trabajo haciendo clic en la ficha que está en el ángulo superior izquierdo del espacio de trabajo. Muestra la conexión entre Ciudad central y Ciudad ISP.

Paso 2: Examinar la configuración estándar de laboratorio en los distintos niveles del espacio físico de trabajo.

Haga clic en Ciudad central que muestra la ciudad y la ubicación del edificio de la oficina central. Haga clic en el edificio de la Oficina central que muestra el plano del edificio y la ubicación del Armario de cableado. Haga clic en el Armario de cableado que le muestra una representación física del equipo instalado en el armario de cableado y los cables que conectan el equipo. Examine esta vista de la topología.

Haga clic en **Interciudad** en la barra **Navegación**. Repita los pasos para ver el equipo instalado en Ciudad ISP.

Práctica de laboratorio 9.8.1: Address Resolution Protocol (ARP)

Diagrama de topología

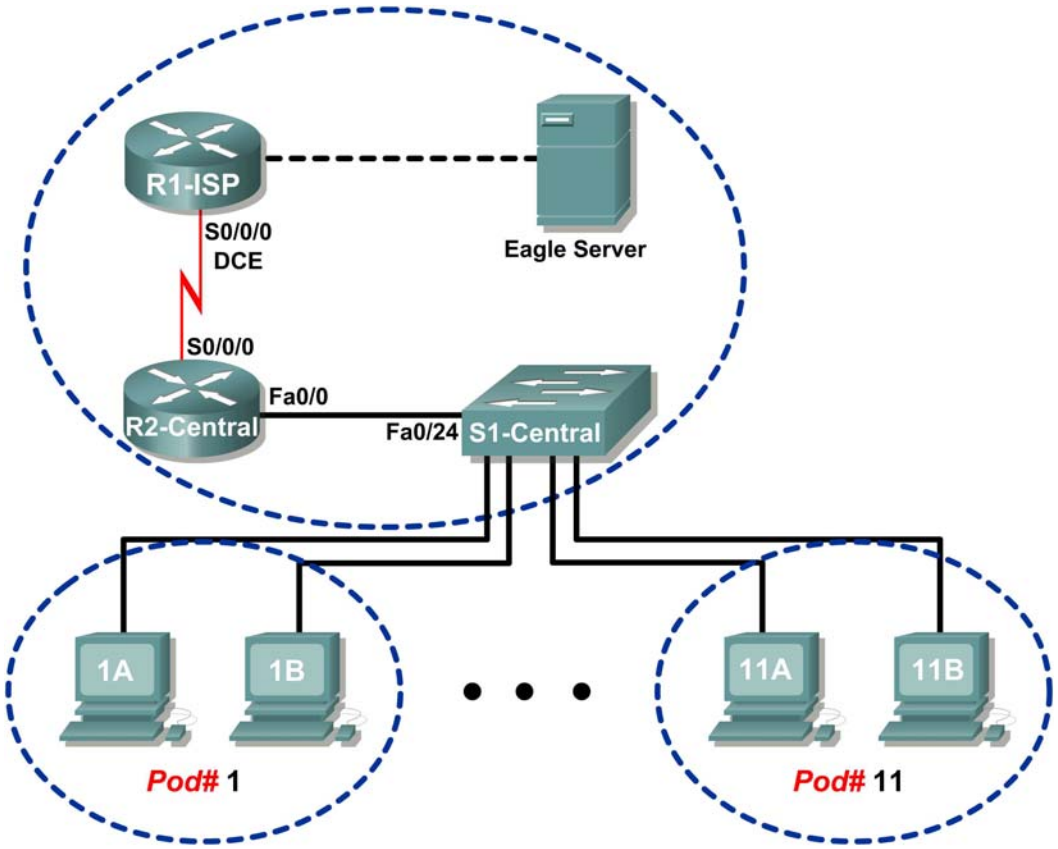


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod*#A	No aplicable	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	No aplicable	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Usar el comando **arp** de Windows.
- Utilizar Wireshark para examinar los intercambios ARP.

Información básica

TCP/IP utiliza el Address Resolution Protocol (ARP) para asignar una dirección IP de Capa 3 a una dirección MAC de Capa 2. Cuando se coloca una trama en la red, debe tener una dirección MAC de destino. Para descubrir dinámicamente la dirección MAC al dispositivo de destino, se transmite una solicitud de ARP en la LAN. El dispositivo que tiene la dirección IP de destino responde y la dirección MAC es registrada en la caché ARP. Todos los dispositivos en la LAN tienen su propia caché ARP o un área más pequeña en la RAM que conserva los resultados ARP. Un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un determinado período de tiempo. l tiempo varía según el dispositivo. Por ejemplo, algunos sistemas operativos de Windows almacenan las entradas de caché de ARP durante 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

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

Un ingeniero de redes debe estar al tanto del ARP, pero es posible que no interactúe con el protocolo regularmente. El ARP es un protocolo que permite que los dispositivos de la red se comuniquen con el protocolo TCP/IP. Sin ARP, no hay un método eficiente para construir el datagrama de la dirección de destino de Capa 2. Pero también representa un riesgo para la seguridad. El spoofing de ARP, también conocido como ARP poisoning, es una técnica que utilizan los atacantes para introducir la asociación de la dirección MAC incorrecta en una red. El individuo falsifica la dirección MAC de un dispositivo y las tramas se envían a la dirección equivocada. Una manera de evitar el ARP spoofing es configurar asociaciones de ARP estáticas manualmente. Por último, se puede configurar una lista de direcciones MAC autorizadas en los dispositivos Cisco para restringir el acceso sólo a los dispositivos aprobados.

Escenario

Con un equipo de computadora host del módulo, utilice el comando utilitario de Windows **arp** para evaluar y cambiar las entradas de caché del ARP.

En la Tarea 2 se emplea Wireshark para capturar y analizar el intercambio ARP entre los dispositivos de la red. Si no se cargó Wireshark en la computadora host del módulo, lo puede descargar desde el URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, archivo `wireshark-setup-0.99.4.exe`.

Tarea 1: Uso del comando `arp` de Windows.

Paso 1: Acceder al terminal de Windows.

```
C:\> arp
Muestra y modifica las tablas de traducción de direcciones de IP
a física utilizadas en el address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Muestra las entradas de ARP actuales al interrogar los
            datos del protocolo actual. Si se especifica inet_addr,
            se muestran las direcciones IP y física sólo en las
            computadoras especificadas. Si más de una interfaz de red
            utiliza ARP, se muestran las entradas de cada tabla ARP.
-g          Igual que -a.
inet_addr   Especifica una dirección de Internet.
-N if_addr  Muestra las entradas de ARP de la interfaz de red
            especificadas por if_addr.
-d          Elimina el host especificado mediante inet_addr. Es posible
            utilizar inet_addr como wildcard con * para eliminar todos
            los hosts.
-s          Agrega el host y asocia la dirección de Internet inet_addr
            con la dirección física eth_addr.  La dirección física
            tiene 6 bytes hexadecimales separados por guiones.
            La entrada es permanente.
eth_addr    Especifica una dirección física.
if_addr     Si está presente, identifica la dirección de Internet
            de la interfaz cuya tabla de traducción de direcciones se
            debe modificar. Si no está presente, se utiliza la primera
            interfaz aplicable.
Ejemplo:
 > arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Agrega una entrada
estática. Muestra la tabla ARP.
C:\>
```

Figura 1. Sintaxis del comando `arp`

1. Abra un terminal de Windows haciendo clic en **Inicio> Ejecutar**. Ingrese: **`cmd`** y haga clic en **Aceptar**. Sin opciones, el comando **`arp`** muestra la información de ayuda útil. Vea la Figura 1.
2. Emita el comando **`arp`** en el equipo de la computadora host y examine el resultado.
3. Responda las siguientes preguntas sobre el comando **`arp`**:

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

   _____

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

   _____

   ¿Qué comando se usaría para eliminar la entrada de la caché ARP para 172.16.255.254?

   _____

Paso 2: Usar el comando arp para examinar la caché ARP local.

```
C:\> arp -a
No se encontraron entradas de ARP
C:\>
```

Figura 2. Caché ARP vacía

Si no se cuenta con comunicación de red, la caché de ARP debe estar vacía. Esto se muestra en la Figura 2.

Ejecute el comando para mostrar las entradas de ARP. ¿Cuáles son los resultados?

_____

_____

Paso 3: Usar el comando `ping` para agregar de manera dinámica entradas en la caché ARP.

El comando **`ping`** se utiliza para verificar la conectividad de la red. Al acceder a otros dispositivos, las asociaciones de ARP se agregan de manera dinámica a la caché ARP.

```
C:\> ping 172.16.1.2
Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 3. Comando `ping` a una computadora host del módulo

1. Utilice el comando **`ipconfig /all`** para verificar la información de la Capa 2 y la Capa 3 de la computadora host del módulo.
2. Emita el comando **`ping`** hacia otra computadora host del módulo, como se muestra en la Figura 3. En la Figura 4 se muestra la nueva entrada de caché de ARP.

```
C:\> arp -a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet    Dirección física   Tipo
  172.16.1.2               00-10-a4-7b-01-5f  dinámica
C:\>
```

Figura 4. Pantalla de la caché de ARP

¿Cómo se agregó la entrada ARP a la caché de ARP? Ayuda: revise la columna Tipo.

_____

¿Cuál es la dirección física de la computadora host del módulo de destino?

_____

¿Cuál es la dirección física de la computadora host del módulo de destino?

Dirección IP	Dirección física	¿De qué manera se obtuvo?

3. No envíe tráfico a la computadora a la que accedió previamente. Espere entre 2 y 3 minutos y verifique nuevamente la caché de ARP. ¿Se eliminó la entrada de caché de ARP? _____
4. Emitir el comando **ping** al Gateway, R2-Central. Examine la entrada de caché de ARP. ¿Cuál es la dirección física del Gateway? _____

Dirección IP	Dirección física	¿De qué manera se obtuvo?

5. Emita el comando **ping** a Eagle Server, eagle-server.example.com. Examine la entrada de caché de ARP. ¿Cuál es la dirección física de Eagle Server? _____

_____

_____

Paso 4: Ajustar las entradas de caché de ARP manualmente.

Para eliminar las entradas en la caché ARP, emita el comando **arp –d {inet-addr | *}**. Las direcciones se pueden eliminar de manera individual al especificar la dirección IP, o bien todas juntas con el wildcard *.

Verifique que la caché ARP contenga dos entradas: una para el Gateway y otra para la computadora host de destino del módulo. Puede resultar más fácil hacer ping en ambos dispositivos más de una vez; de esta manera se retiene la entrada a caché durante 10 minutos aproximadamente.

```
C:\> arp –a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet   Dirección física      Tipo
  172.16.1.2              00-10-a4-7b-01-5f     dinámica
  172.16.255.254          00-0c-85-cf-66-40     dinámica
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet   Dirección física      Tipo
  172.16.1.2              00-10-a4-7b-01-5f     dinámica
C:\>
```

Figura 5. Eliminar manualmente una entrada a la caché de ARP

Consulte la Figura 5, donde se muestra cómo eliminar manualmente una entrada a caché ARP.

1. En la computadora, primero verifique que estén las dos entradas. Si no están, haga ping en la entrada faltante.
2. A continuación, elimine la entrada de la computadora host del módulo.
3. Por ultimo, verifique el cambio que realizó.

4. Registre las dos entradas en la caché ARP.

Dispositivo	Dirección IP	Dirección física	¿De qué manera se obtuvo?

5. Escriba el comando que sirve para eliminar la entrada de la computadora host del módulo:
_____

6. Emita el comando en la computadora host del módulo. Registre la entrada en la caché ARP restante:

Dispositivo	Dirección IP	Dirección física	¿De qué manera se obtuvo?

7. Simule que elimina todas las entradas. Escriba el comando que sirve para eliminar todas las entradas de la caché ARP:
_____

8. Emita el comando en la computadora host del módulo y examine la caché ARP con el comando **`arp -a`**. Todas las entradas deben haber sido eliminadas.
_____

9. Considere un entorno seguro donde el Gateway controla el acceso al servidor Web que contiene información confidencial. ¿Cuál es la capa de seguridad que se puede aplicar a las entradas de la caché ARP que ayudaría a contrarrestar el ARP spoofing?
_____

10. Escriba el comando que sirve para agregar una entrada ARP estática en la caché ARP para el Gateway:
_____

11. Examine la caché ARP nuevamente y complete la siguiente tabla:

Dirección IP	Dirección física	Tipo

En la siguiente tarea, se utiliza Wireshark para capturar y examinar el intercambio ARP. No cierre el terminal de Windows: lo usará para ver la caché ARP.

Tarea 2: Utilizar Wireshark para examinar los intercambios ARP.

Paso 1: Configurar Wireshark para las capturas de paquetes.

Prepare Wireshark para las capturas.

1. Haga clic en **Captura > Opciones**.
2. Seleccione la interfaz que corresponda a la LAN.
3. Marque la casilla para Actualizar la lista de paquetes en tiempo real.
4. Haga clic en **Inicio**.

Con esta acción se inicia la captura de paquetes.

Paso 2: Preparar la computadora host del módulo para las capturas de ARP.

1. Si aún no lo hizo, abra una ventana del terminal de Windows haciendo clic en **Inicio > Ejecutar**. Ingrese: **`cmd`** y haga clic en **Aceptar**.
2. Purgue la caché ARP, que requiere que el ARP vuelva a descubrir los mapas de direcciones. Escriba el comando que utilizó: _____

Paso 3: Capturar y evaluar la comunicación del ARP.

En este paso se envía una solicitud de ping al Gateway y otra solicitud de ping a Eagle Server. Luego la captura de Wireshark se detiene y se evalúa la comunicación ARP.

1. Envíe una solicitud de ping al Gateway, con el comando **`ping -n 1 172.16.255.254.`**
2. Envíe una solicitud de ping a Eagle Server, con el comando **`ping -n 1.192,168.254,254.`**

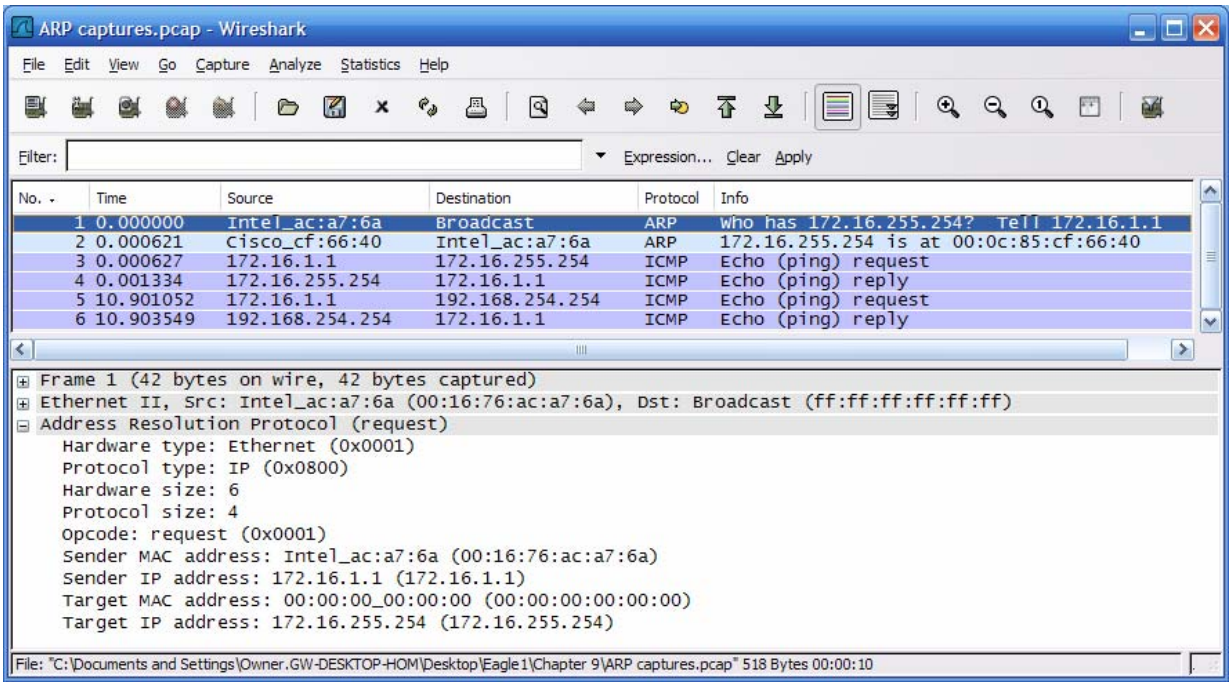


Figura 6. Captura Wireshark de la comunicación ARP

3. Detenga Wireshark y evalúe la comunicación. Debe ver una pantalla de Wireshark similar a la que se muestra en la Figura 6. En la ventana que contiene la lista de paquetes de Wireshark se muestra la cantidad de paquetes capturados. En la ventana de detalles del paquete se muestra el contenido del protocolo ARP.
4. A partir de la captura de Wireshark, responda las siguientes preguntas:

   ¿Cuál fue el primer paquete de ARP? _____

   ¿Cuál fue el segundo paquete de ARP? _____

Complete la siguiente taba con información sobre el primer paquete de ARP:

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

Complete la siguiente tabla con información sobre el segundo paquete de ARP:

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

Si la trama de Ethernet II de una solicitud ARP es un broadcast, ¿por qué la dirección MAC contiene sólo 0? _____

¿Por qué no hubo una solicitud ARP para el ping a Eagle Server? _____

_____

_____

¿Por cuánto tiempo se debe guardar la asignación del gateway en la caché ARP en la computadora host del módulo? ¿Por qué? _____

_____

Tarea 3: Reflexión

El protocolo ARP asigna direcciones IP de Capa 3 a las direcciones MAC de Capa 2. Si un paquete se debe mover por las redes, la dirección MAC de Capa 2 cambia con cada salto que hace en el router, pero la dirección de Capa 3 nunca cambia.

En la caché de ARP se guardan las asignaciones de las direcciones de ARP. Si se obtuvo la entrada de manera dinámica, eventualmente se eliminará de la caché. Si se insertó de forma manual en la caché de ARP, se trata de una entrada estática que permanecerá en la computadora hasta que se apague o se purgue manualmente la caché ARP.

Tarea 4: Desafío

Con recursos externos, realice una búsqueda sobre ARP spoofing. Analice las distintas técnicas que se utilizan para contrarrestar este tipo de ataque.

La mayoría de los routers inalámbricos admiten acceso inalámbrico a las redes. Con esta técnica, las direcciones MAC que tienen acceso permitido a la red inalámbrica se agregan manualmente al router inalámbrico. Utilizando recursos externos, evalúe las ventajas de configurar un acceso a la red inalámbrica. Debata las maneras en que se puede violar esta seguridad.

Tarea 5: Limpieza

Se instaló Wireshark en la computadora host del módulo. Si debe desinstalarlo, haga clic en **Inicio > Panel de control**. Abra **Agregar o quitar programas**. Marque Wireshark y haga clic en **Quitar**.

Elimine todos los archivos creados durante la práctica de laboratorio en la computadora host del módulo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 9.8.2: Análisis de la tabla MAC del switch Cisco

Diagrama de topología

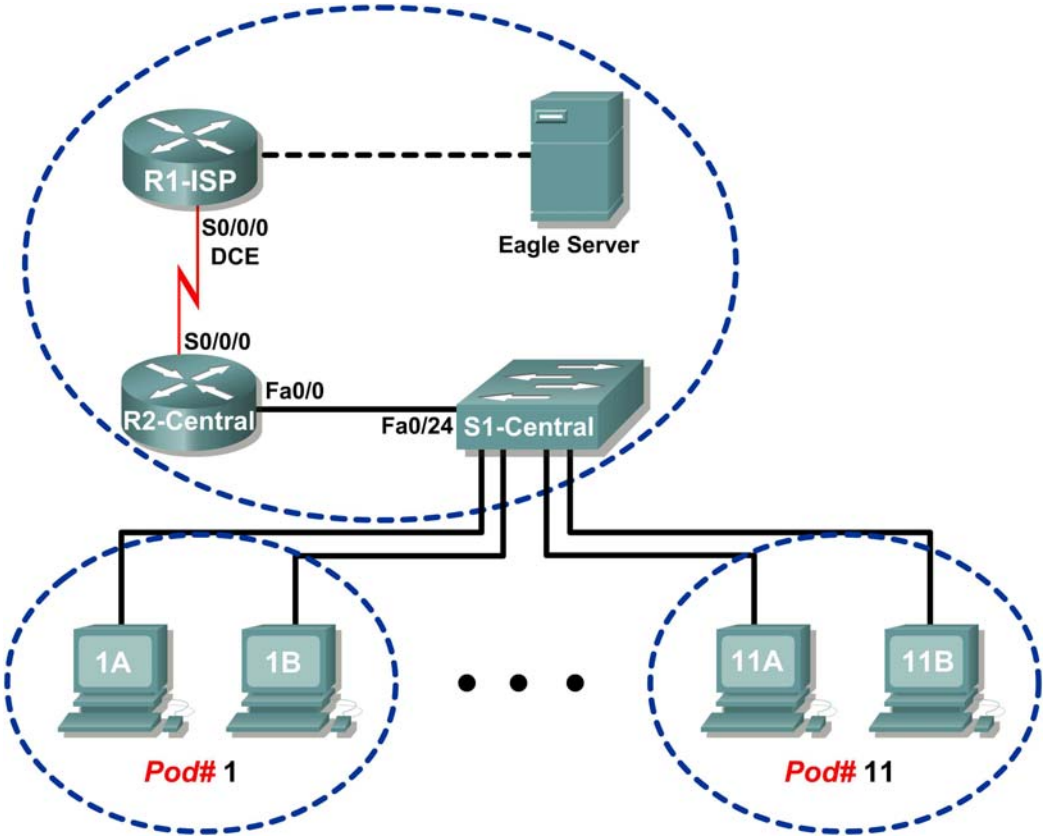


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#*A	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Utilizar el protocolo Telnet para iniciar una sesión en un switch Cisco.
- Utilizar el comando show **mac-address-table** de Cisco IOS para examinar la dirección MAC y las asociaciones del puerto.

Información básica

Los switches cuentan con una tabla de direcciones MAC y el puerto del switch correspondiente. Cuando un switch recibe una trama, la dirección MAC se verifica en la tabla y se utiliza el puerto correspondiente para enrutar la trama por el switch. Si no puede determinar por qué puerto debe enrutar la trama, o se trata de un broadcast, la trama se enruta por todos los puertos excepto por el que fue originado.

Es posible acceder a los dispositivos de Cisco de diferentes maneras. Se puede emplear un puerto de consola si el router o switch Cisco se encuentra en la misma proximidad física de una computadora. Mediante la utilidad del Hyperterminal Windows, se puede establecer una conexión serial. Si los dispositivos están físicamente lejos del ingeniero de redes, puede establecer la conectividad de la red de dos maneras. Si la red no es segura, con un módem configurado en el puerto AUX se logra el acceso telefónico. Cuando las redes son seguras, el dispositivo Cisco se puede configurar de manera que inicie una sesión Telnet. En esta práctica de laboratorio, el estudiante se conecta al switch mediante una sesión Telnet.

Práctica de laboratorio

- Telnet a S1-Central.
- Iniciar sesión con una cuenta de estudiante.
- Utilizar el comando **show mac-address-table** para examinar las direcciones MAC y la asociación de los puertos.

Escenario

Utilice el comando **show mac-address-table** de Cisco IOS para examinar la tabla de direcciones MAC y otra información relacionada.

Telnet es un servicio de red que utiliza un modelo de cliente/servidor. Los dispositivos Cisco IOS ofrecen un servidor Telnet predeterminado y los sistemas operativos como Windows tienen clientes Telnet incorporados. Con Telnet, los ingenieros de redes pueden iniciar sesión en dispositivos de red desde cualquier lugar de una red segura. El dispositivo Cisco debe configurarse para que permita el acceso Telnet; de lo contrario, se deniega el acceso. En Eagle 1, los privilegios limitados se configuraron para uso del estudiante.

Tarea 1: Uso del protocolo Telnet para iniciar sesión en un switch Cisco.

Paso 1: Acceder al terminal de Windows.

Abra un terminal de Windows haciendo clic en **Inicio> Ejecutar**. Ingrese: **cmd** y haga clic en **Aceptar**.

Paso 2: Utilizar un cliente Telnet de Windows para acceder a S1-Central.

S1-Central se configura con 11 cuentas de estudiante, desde `ccna1` hasta `ccna11`. Para permitir el acceso a cada estudiante, utilice la id de usuario que corresponda a su equipo. Por ejemplo, para las computadoras del equipo 1, utilice la id de usuario `ccna1`. A menos que el instructor indique lo contrario, la contraseña es `cisco`.

1. Desde el terminal de Windows, ejecute el comando de Telnet: **telnet** *destination-ip-address*:

```
C:/> telnet 172.16.254.1
```

Se mostrará un aviso de acceso, similar al que se muestra en la Figura 1.

```
 ************************************************************************
                This is Lab switch S1-Central.
                Authorized access only.
 ************************************************************************
User Access Verification
Username: ccna1
Password: cisco  (*hidden*)
S1-Central#
```

Figura 1. Cliente Telnet

2. Ingrese el nombre de usuario que corresponda. Cuando aparezca la petición de contraseña, ingrese `cisco <ENTER>`.

   Debe mostrarse el mensaje `S1-Central#`.

Tarea 2: Uso del comando `show mac-address-table` de Cisco IOS para examinar las direcciones MAC y las asociaciones de puerto.

Paso 1: Examinar la tabla de direcciones MAC del switch.

1. Emita el comando **`show mac-address-table ? <ENTER>`**. Se despliegan todas las opciones del comando.
2. Utilice la siguiente tabla para completar las opciones del comando:

Opción	Descripción

Paso 2: Examinar las entradas de la tabla de dirección MAC dinámica.

1. Emita el comando **`show mac-address-table`**.
   Con este comando se mostrarán las entradas estáticas (CPU) y dinámicas o aprendidas.

2. Enumere las direcciones MAC y los puertos del switch correspondientes:

Dirección MAC	Puerto del switch

Supongamos que había un hub con cinco host activos conectados al puerto del switch `gi0/0`. ¿Cuántas direcciones MAC se enumerarían en el puerto del switch `gi0/0`? _____

Paso 3: Examinar la expiración de la conexión en la tabla de direcciones MAC.

1. Emita el comando **`show mac-address-table aging-time`**.
   Con este comando se mostrará el tiempo predeterminado, en segundos, en que se almacenaron las entradas de la dirección MAC.
2. ¿Cuál es el tiempo de expiración predeterminado de VLAN 1? _____

Tarea 3: Desafío

¿Cuál sería el resultado si la tabla de dirección MAC estuviera llena de entradas dinámicas?

_____

_____

Tarea 4: Reflexión

Utilizando el protocolo Telnet, los ingenieros de redes pueden acceder a los dispositivos Cisco de forma remota en todas las LAN seguras. Esto tiene el beneficio de que permite el acceso a dispositivos remotos para resolución de problemas y monitoreo.

Un switch contiene una tabla de direcciones MAC en la que se enumera la dirección MAC conectada a cada puerto del switch. Cuando una trama ingresa al switch, éste busca la dirección MAC de destino de la trama. Si hay una coincidencia en la tabla de direcciones MAC, la trama se enruta por el puerto correspondiente. Sin la tabla de dirección MAC, el switch tendría que enviar la trama por cada puerto.

Tarea 5: Limpieza

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 9.8.3: Dispositivo intermediario como dispositivo final

Diagrama de topología

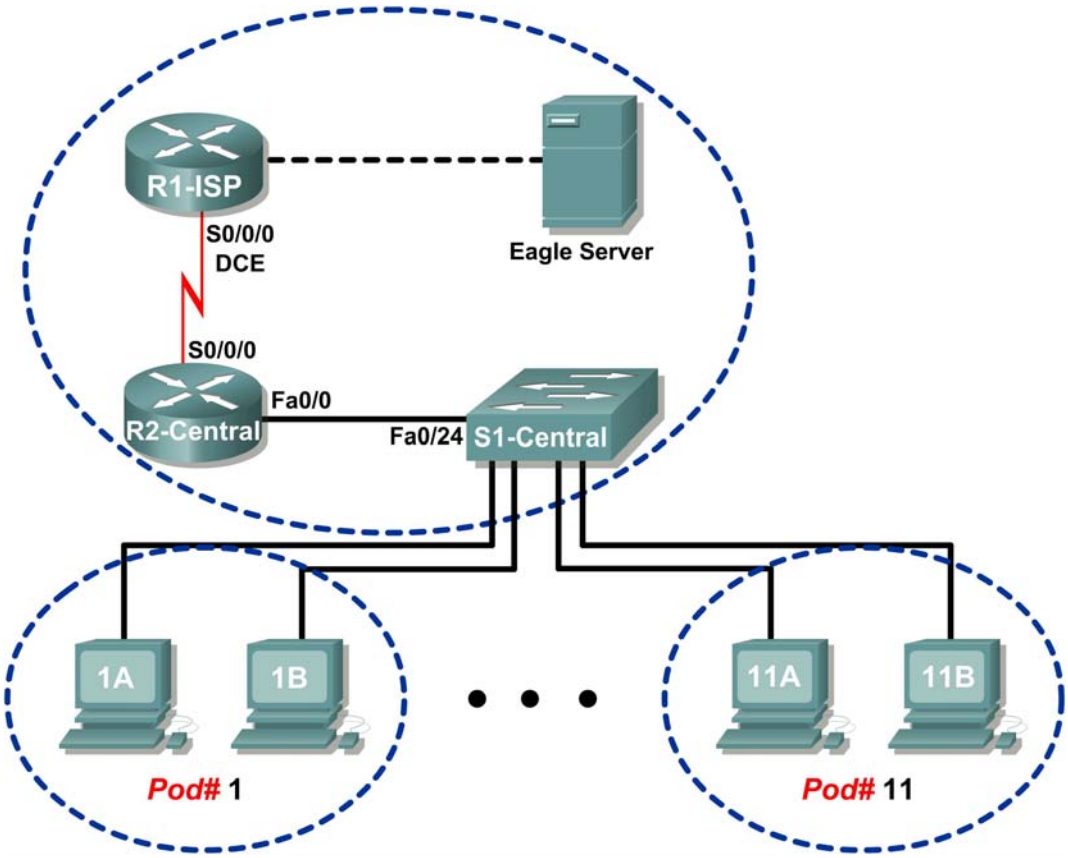


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod*#A	No aplicable	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	No aplicable	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Utilizar Wireshark para capturar y analizar tramas que se originen desde los nodos de la red.
- Examinar la manera en que se originan las tramas en una red pequeña.

Información básica

Se utiliza un switch para enrutar tramas entre los dispositivos de la red. Un switch por lo general no origina la trama hacia los dispositivos del nodo. En cambio, pasa eficientemente la trama desde un dispositivo a otro en la LAN.

Escenario

Se utiliza Wireshark para capturar y analizar las tramas de Ethernet. Si no se cargó Wireshark en la computadora host del módulo, lo puede descargar desde el URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/`, archivo `wireshark-setup-0.99.4.exe`.

En esta práctica de laboratorio se hace ping en la computadora host del módulo del compañero.

Tome nota de la dirección IP y de la conexión de puerto de S1-Central del equipo de la computadora host del módulo del compañero.

Dirección IP: _____ Número de puerto de S1-Central: _____

Tarea 1: Uso de Wireshark para capturar y analizar tramas que se originen desde los nodos de la red.

Paso 1: Configurar Wireshark para las capturas de paquetes.

Prepare Wireshark para las capturas.

1. Haga clic en **Captura > Opciones**.
2. Seleccione la interfaz que corresponda a la LAN.
3. Marque la casilla para Actualizar la lista de paquetes en tiempo real.
4. Haga clic en **Inicio**.

Con esta acción se inicia la captura de paquetes. Durante este proceso quizás haya más de 200 capturas, lo que torna el análisis bastante tedioso. La conversación Telnet crítica entre el equipo de la computadora host del módulo y S1-Central es fácil de filtrar.

Paso 2: Utilizar un cliente Telnet de Windows para acceder a S1-Central.

S1-Central se configura con 11 cuentas de estudiante, desde `ccna1` hasta `ccna11`. Para permitir el acceso a cada estudiante, utilice la id de usuario que corresponda a su equipo. Por ejemplo, para las computadoras del equipo 1, utilice la id de usuario `ccna1`. A menos que el instructor indique lo contrario, la contraseña es `cisco`.

1. Desde el terminal de Windows, ejecute el comando de Telnet: **`telnet`** *`destination-ip-address`*:

   C:/> **`telnet 172.16.254.1`**

2. Ingrese el nombre de usuario y la contraseña adecuados, **`cisco`**.
   Se debe devolver la petición de S1-Central, `S1-Central#`.

Paso 3: Limpie la tabla de direcciones MAC.

1. Examine la tabla de direcciones MAC con el comando: **`show mac-address-table`**. Además de varias entradas de CPU estáticas, debe haber numerosas entradas dinámicas en la tabla.
2. Para eliminar las entradas dinámicas de la tabla de direcciones MAC, utilice el comando: **`clear mac-address-table dynamic`**.
3. Enumere las entradas dinámicas de direcciones MAC:

Dirección MAC	Puerto del switch

4. Abra una segunda ventana terminal. Haga ping en la dirección IP de la computadora vecina, que se registró antes:

   `C:>\ ping –n 1` *`ip-address`*

5. La dirección MAC de esta computadora debe agregarse de manera dinámica a la tabla de direcciones MAC de S1-Central.
6. Enumere nuevamente las entradas dinámicas de direcciones MAC:

Dirección MAC	Puerto del switch

   ¿A qué conclusión puede arribar acerca de cómo un switch obtiene las direcciones MAC conectadas a interfaces de switch?

   _____

   _____

7. Cierre la captura de Wireshark.

   Se analizará la captura en la próxima tarea.

Tarea 2: Análisis de la manera en que se originan las tramas en una red pequeña.

Paso 1: Examinar una sesión Telnet con S1-Central.

1. Resalte uno de los paquetes de la sesión de Telnet. En el menú de Wireshark, haga clic en **Analizar | Seguir flujo TCP**. En este momento se abre una ventana de contenido de flujo, con una visualización predeterminada ASCII. Si no se ven el nombre de usuario y las contraseñas, cambie a HEX Dump.
2. Verifique el nombre de usuario y la contraseña ingresados:
   Username: _____ Contraseña: _____
3. Cierre la ventana de contenido de flujo.

Paso 2: Examinar el resultado del comando show `mac-address-table`.

1. Abra un Bloc de notas. Transfiera la información capturada al Bloc de notas para analizarla. Es posible que haya numerosos paquetes capturados.
2. En el panel superior de la Lista de paquetes de Wireshark, desplácese hasta la solicitud ICMP capturada. Si la ventana inferior donde se muestra la cantidad de bytes del paquete de Wireshark no se encuentra visible, haga clic en **Ver > Bytes del paquete**.

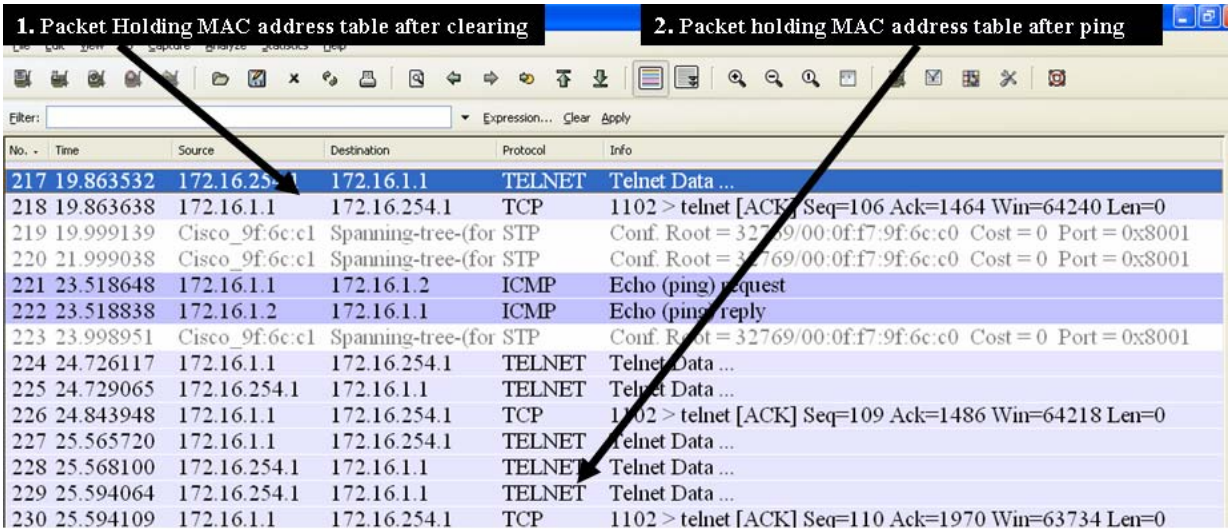


Figura 1. Captura Wireshark de Telnet

Vea la Figura 1, un resultado parcial de la captura de Wireshark:

1 Seleccione el último paquete de datos de Telnet de S1-Central anterior al comando **`ping`**. A continuación, seleccione la cantidad de bytes del paquete correspondiente. Haga clic con el botón derecho sobre el byte del paquete y haga clic en **Copiar > Sólo texto**. En el Bloc de notas, haga clic en **Editar > Pegar**. Las asignaciones dinámicas deben ser similares al siguiente resultado:

```
{_lEMaNL;RPC          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 5
S1-Central#
```

3. Tome nota de la dirección MAC y el número de puerto que se muestra en el resultado. ¿Se corresponde el puerto del switch con el equipo de la computadora host del módulo? _____

Dirección MAC	Tipo	Puerto

¿Por qué la asignación de la computadora host del módulo todavía se encuentra en la tabla de direcciones MAC, pese a que ya se eliminó? _____

_____

Ésta es la conexión para la computadora host del módulo mediante Telnet en S1-Central.

2 Seleccione el último paquete de datos Telnet inmediatamente después de la respuesta del ping. A continuación, seleccione la cantidad de bytes del paquete correspondiente. Haga clic con el botón derecho sobre el byte del paquete y haga clic en **Copiar > Sólo texto**. En el Bloc de notas, haga clic en **Editar > Pegar**. El texto debe ser similar a la siguiente acción de pegar:

```
{_lEPaNM;VP          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
   1    0016.76ac.a76a    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
S1-Central#
```

4. Tome nota de la dirección MAC y del número de puerto de la segunda dinámica que se muestra en el resultado. ¿Corresponde el puerto del switch con el equipo de la computadora host del módulo vecino? _____

Dirección MAC	Tipo	Puerto

Tarea 3: Reflexión

La captura de Wireshark de una sesión de Telnet entre una computadora host del módulo y S1-Central fue analizada para demostrar cómo un switch obtiene datos de manera dinámica sobre los nodos que tiene conectados.

Tarea 4: Desafío

Utilice Wireshark para capturar y analizar una sesión Telnet entre el la computadora host del módulo y el switch Cisco. Utilice la opción del menú de Wireshark **Analizar > Seguir flujo TCP** para visualizar la ID de usuario y la contraseña del inicio de sesión. ¿Cuán seguro es el protocolo Telnet? ¿Qué se puede hacer para que la comunicación entre los dispositivos Cisco sea más segura?

_____

_____

_____

_____

_____

Tarea 5: Limpieza

Se instaló Wireshark en la computadora host del módulo. Si debe desinstalarlo, haga clic en **Inicio > Panel de control**. Abra **Agregar o quitar programas**. Seleccione Wireshark y haga clic en **Quitar**.

Elimine todos los archivos creados durante la práctica de laboratorio en la computadora host del módulo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

9.9.1: Desafío de integración de capacidades: Ethernet conmutada

Diagrama de topología

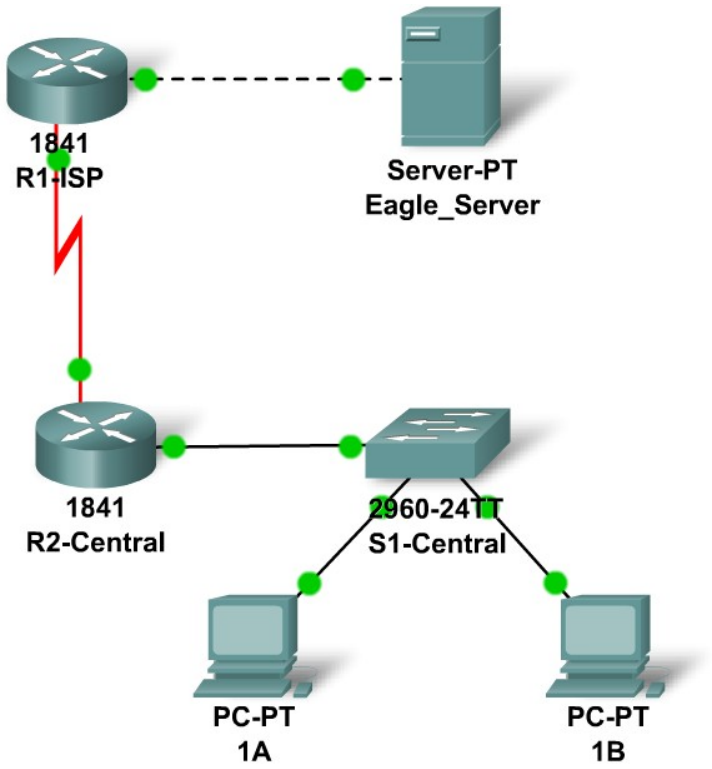


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	**Fa0/0**	192.168.111.134	255.255.255.248	No aplicable
	S0/0/0	192.168.111.138	255.255.255.252	No aplicable
R2-Central	**Fa0/0**			No aplicable
	S0/0/0	192.168.111.137	255.255.255.252	No aplicable
PC1A	**NIC**			
PC1B	**NIC**			
Eagle Server	**NIC**	192.168.111.133	255.255.255.248	192.168.111.134

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Determinar la planificación de subredes IP.
- Reparar temas de red relacionados a Ethernet.
- Probar la red.

Información básica

Se le pidió que resuelva algunos problemas en el modelo de red relacionados con la LAN Ethernet conectada a R2-Central.

Tarea 1: Planificación de subredes IP.

Se le ha asignado un bloque de direcciones IP de 192.168.111.0 /24. Debe tener en cuenta las tres redes existentes.

Las asignaciones de subred son:

- 1.ª subred, LAN de estudiantes actual, al menos 100 hosts (Fa0/0 en R2-Central);
- 2.ª subred, LAN ISP existente, al menos 5 hosts; (ya configurados)
- 3.ª subred, WAN existente, enlace punto a punto; (ya configurado)

Dirección IP de la interfaz:

- Las interfaces del servidor, de R1-ISP y de R2-Central ya han sido configuradas.
- Para la interfaz F0/0 de R2-Central use la dirección más utilizable en la subred LAN de estudiante existente.
- Para los hosts 1A y 1B use las dos primeras direcciones IP (las dos direcciones menos utilizables) de la subred LAN de estudiantes existente.
- Para los hosts 1A y 1B, el servidor DNS es 192.168.111.133.
- El router para el próximo salto (al cual debe apuntar a la ruta predeterminada), R1-ISP, tiene una dirección IP de 192.168.111.138 / 30.

Tarea 2: Reparación de problemas con la LAN Ethernet conmutada.

- La PC 1B tiene una tarjeta inalámbrica y no se puede conectar al switch; agregue la tarjeta de Interfaz Fast Ethernet PT-HOST-NM-1CFE a la PC 1B.
- Conecte el recién instalado NIC Fast Ethernet a la interfaz Fa0/2 del switch.
- Conecte la PC 1A a la interfaz Fa0/1 del switch.
- Conecte la interfaz Fa0/24 del switch a la interfaz Fa0/0 de R2-Central.

Aparentemente la configuración de velocidad y dúplex de Ethernet para la interfaz Fa0/0 de R2-Central, para las interfaces del switch S1-Central (Fa0/1, Fa0/2, y Fa0/24) y para las interfaces de la PC 1A son incorrectas. Configure todas las interfaces Ethernet para que autonegocien la velocidad y el duplex (que alcanzará un funcionamiento full duplex de 100 Mbps si ambos extremos del enlace pueden admitirlo). Para todos los dispositivos, asegúrese de que la energía eléctrica esté conectada al dispositivo y a las interfaces (asegúrese que las interfaces Ethernet no estén desconectadas). Agregue direcciones IP a la interfaz Fa0/0 del router y a las dos PC (la dirección de subred más utilizable debe asignarse al gateway y las dos direcciones menos utilizables deben asignarse a las PC). La ruta estática del R2-Central debería ser una ruta estática predeterminada que apunta a través de la dirección IP de la interfaz serial de

R1-ISP. Estos procedimientos se explicaron en los Desafíos de integración de aptitudes de los capítulos 5 y 6.

Tarea 3: Prueba de la red

Use ping, rastreo, tráfico Web y la herramienta **Inspeccionar** para rastrear el flujo de paquetes en el modo de simulación, con visualización de HTTP, DNS, TCP, UDP, ICMP y ARP para verificar si comprende cómo está funcionando la red.

Tarea 4: Reflexión

Las dos tecnologías de Capa 2 (y Capa 1) de este modelo constituyen una conexión serial (entre los routers) y las LAN Ethernet (para el servidor ISP y con el switch de S1-Central). Indique las similitudes y diferencias entre la conexión serial y Ethernet. En un próximo curso aprenderá mucho más sobre las tecnologías de Ethernet conmutada.

Práctica de laboratorio 10.3.2: ¿Cuántas redes?

Objetivos de aprendizaje

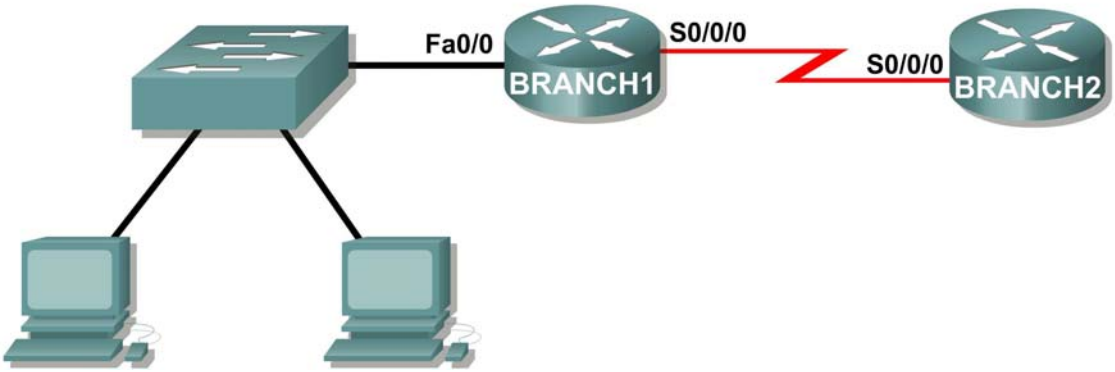
Al completar esta práctica de laboratorio, usted podrá:

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

Escenario

En esta práctica de laboratorio, se asignó la dirección de red 192.168.26.0/24 para la subred y la dirección IP de las redes que se muestran en los Diagramas de topología. Debe determinar la cantidad de redes necesarias para luego diseñar un esquema de direccionamiento adecuado. Coloque la dirección y la máscara correctas en la Tabla de direccionamiento. En este ejemplo, la cantidad de hosts no es importante. Sólo debe determinar la cantidad de subredes por ejemplo de topología.

Diagrama de topología A



Tarea 1: Determinar la cantidad de subredes del Diagrama de topología.

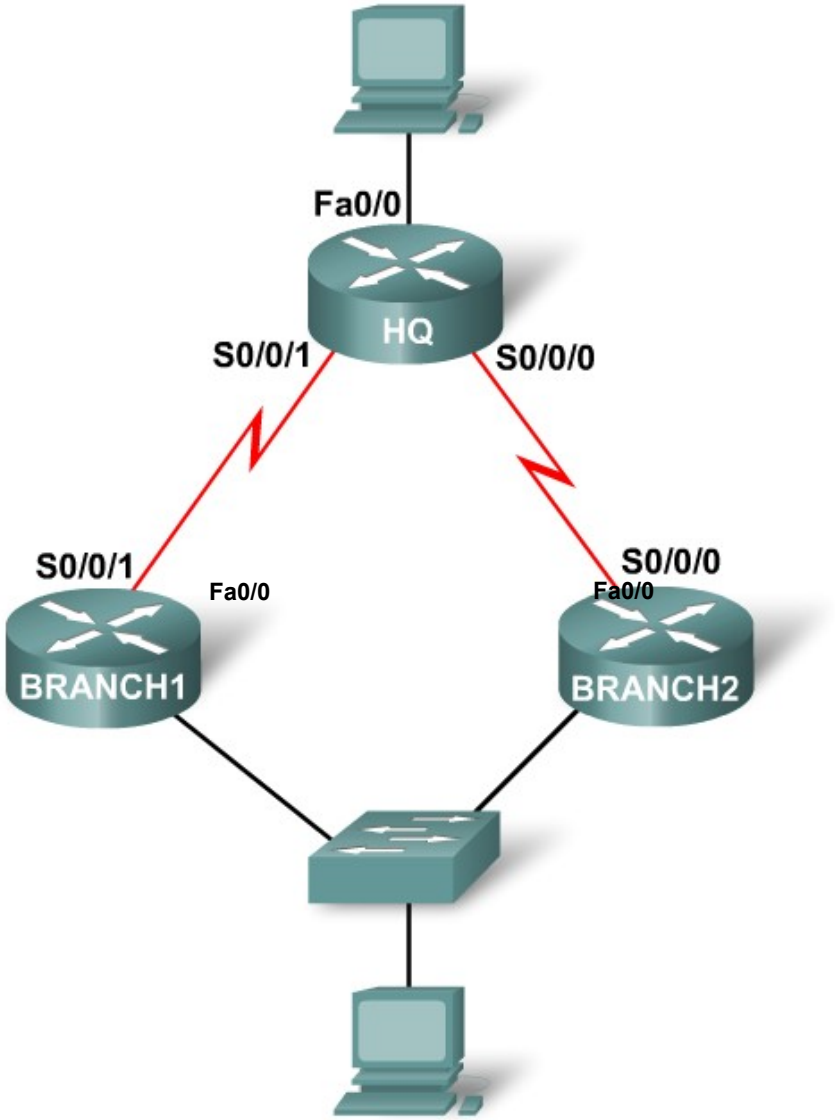
Paso 1: ¿Cuántas redes hay? _____
Paso 2: ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____
Paso 3: ¿Cuántas direcciones de host utilizables y subredes utilizables consiguió con esto? _____
Paso 4: ¿Cuál es la nueva máscara de subred en formato decimal? _____
Paso 5: ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

Tarea 2: Registrar información de la subred.

Paso 1: Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				

Diagrama de topología B



Tarea 3: Determinar la cantidad de subredes del Diagrama de topología.

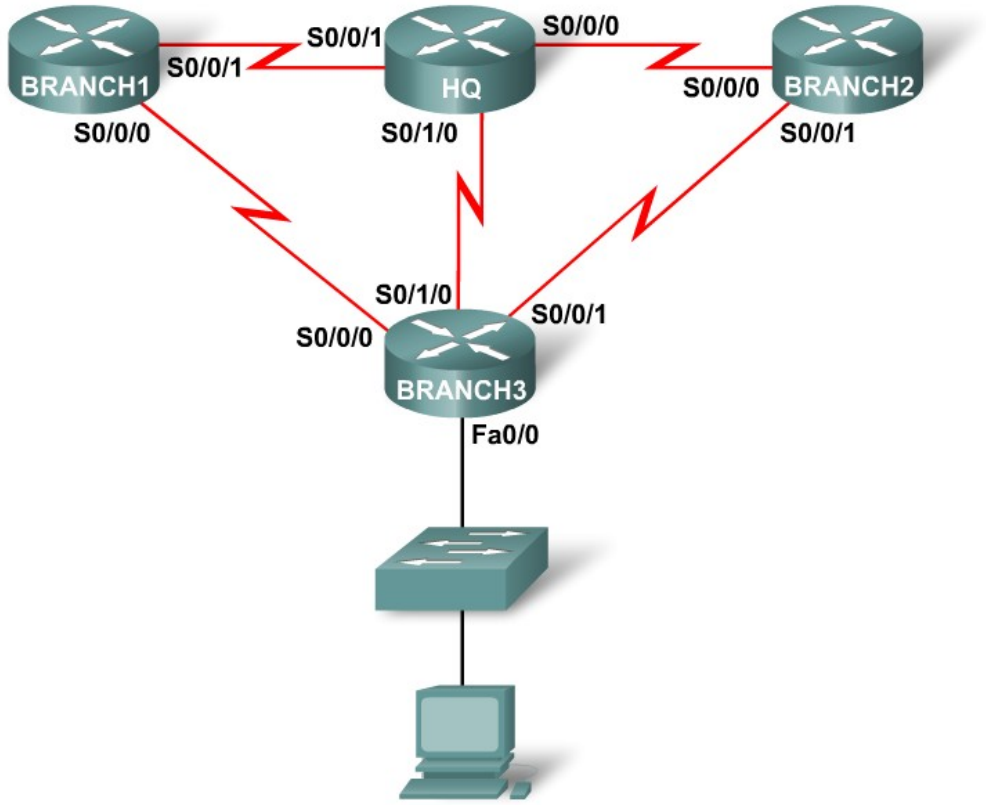
Paso 1: ¿Cuántas redes hay? _____
Paso 2: ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____
Paso 3: ¿Cuántas direcciones de host utilizables y subredes utilizables consiguió con esto? _____
Paso 4: ¿Cuál es la nueva máscara de subred en formato decimal? _____
Paso 5: ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

Tarea 4: Registrar información de la subred.

Paso 1: Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				

Diagrama de topología C



Tarea 5: Determinar la cantidad de subredes del Diagrama de topología.

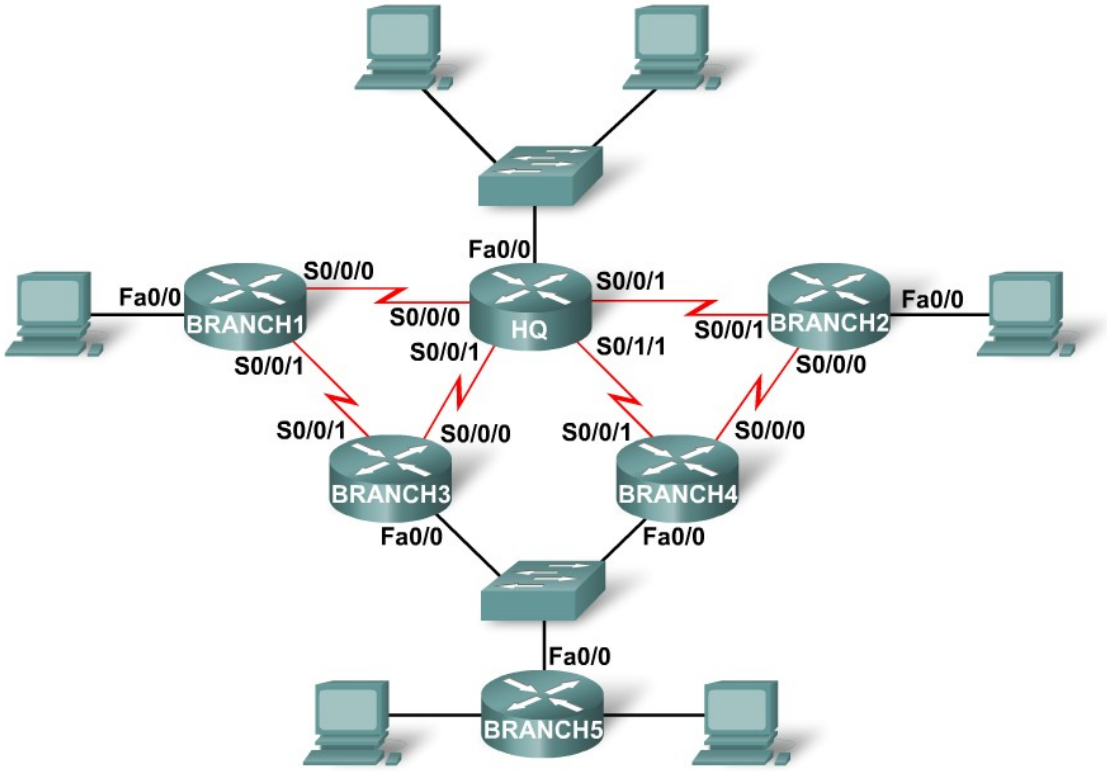
Paso 1: ¿Cuántas redes hay? _____
Paso 2: ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____
Paso 3: ¿Cuántas direcciones de host utilizables y subredes utilizables consiguió con esto? _____
Paso 4: ¿Cuál es la nueva máscara de subred en formato decimal? _____
Paso 5: ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

Tarea 6: Registrar información de la subred.

Paso 1: Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Diagrama de topología D



Tarea 7: Determinar la cantidad de subredes del Diagrama de topología.

Paso 1: ¿Cuántas redes hay? _____
Paso 2: ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? _____
Paso 3: ¿Cuántas direcciones de host utilizables y subredes utilizables consiguió con esto? _____
Paso 4: ¿Cuál es la nueva máscara de subred en formato decimal? _____
Paso 5: ¿Cuántas subredes quedan disponibles para usar en el futuro? _____

Tarea 8: Registrar información de la subred.

Paso 1: Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Tarea 9: Reflexión

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

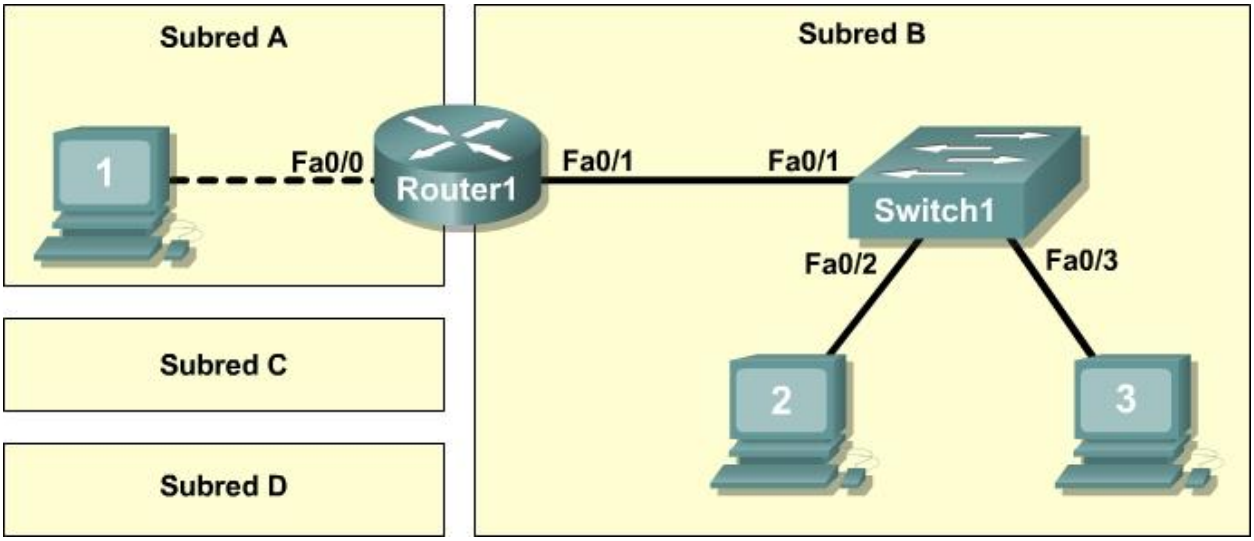
_____

_____

_____

Práctica de laboratorio 10.6.1: Creación de una pequeña topología de laboratorio

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Diseñar la red lógica.
- Configurar la topología física de laboratorio.
- Configurar la topología LAN lógica.
- Verificar la conectividad LAN.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA
Switch Cisco	1	Parte del equipo de laboratorio del CCNA
*Computadora (host)	3	Computadora del laboratorio
Cables UTP Cat-5 o cualquier cable UTP superior de conexión directa	3	Conecta el Router1 y los equipos Host1 y Host2 con el Switch 1
Cable UTP Cat -5 de conexión cruzada	1	Conecta el equipo Host1 con el Router1

Tabla 1. Equipo y hardware para el laboratorio

Reúna todos los equipos y cables necesarios. Para configurar el laboratorio, consulte la lista de equipos y hardware en la Tabla 1.

Escenario

En esta práctica de laboratorio podrá crear una red pequeña que requiere la conexión de dispositivos de red y la configuración de equipos host para lograr una conectividad básica de red. SubredA y SubredB son subredes que se necesitan en la actualidad. SubredC y la SubredD son subredes anticipadas, aún no conectadas a la red. Se utilizará la subred 0°.

Nota: El Apéndice 1 contiene una tabla de subred para último octeto de la dirección IP.

Tarea 1: Diseñar la red lógica.

Dada una dirección IP y máscara de `172.20.0.0 / 24 (dirección / máscara)`, diseñe un esquema de direccionamiento IP que cumpla con los siguientes requisitos:

Subred	Cantidad de hosts
SubredA	2
SubredB	6
SubredC	47
SubredD	125

Los equipos host de cada subred utilizarán la primera dirección IP disponible en el bloque de direcciones. Las interfaces del router utilizarán la última dirección IP disponible en el bloque de direcciones.

Paso 1: Diseñe un bloque de direcciones para la SubredD

Comience el diseño lógico de la red cumpliendo con el requisito de la SubredD, que requiere el bloque más grande de direcciones IP. Consulte la tabla de la subred y elija el primer bloque de direcciones que admitirá la SubredD.

Complete la siguiente tabla con la información sobre la dirección IP de la SubredD:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits? _____

Paso 2: Diseñe un bloque de direcciones para la SubredC

Cumpla con los requisitos de la SubredC, el siguiente bloque más grande de direcciones IP. Consulte la tabla de la subred y elija el primer bloque de direcciones disponibles que admitirá la SubredC.

Complete la siguiente tabla con la información sobre la dirección IP de la SubredC:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits? _____

Paso 3: Diseñe un bloque de direcciones para la SubredB

Cumpla con los requisitos de la SubredB, el siguiente bloque más grande de direcciones IP. Consulte la tabla de la subred y elija el primer bloque de direcciones disponibles que admitirá la SubredB.

Complete la siguiente tabla con la información sobre la dirección IP de la SubredB:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits? _____

Paso 4: Diseñe un bloque de direcciones para la SubredA

Cumpla con los requisitos de la SubredA. Consulte la tabla de la subred y elija el primer bloque de direcciones disponibles que admitirá la SubredB.

Complete la siguiente tabla con la información sobre la dirección IP de la SubredA:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits? _____

Tarea 2: Configurar la topología física del laboratorio.

Paso 1: Conecte físicamente los dispositivos.

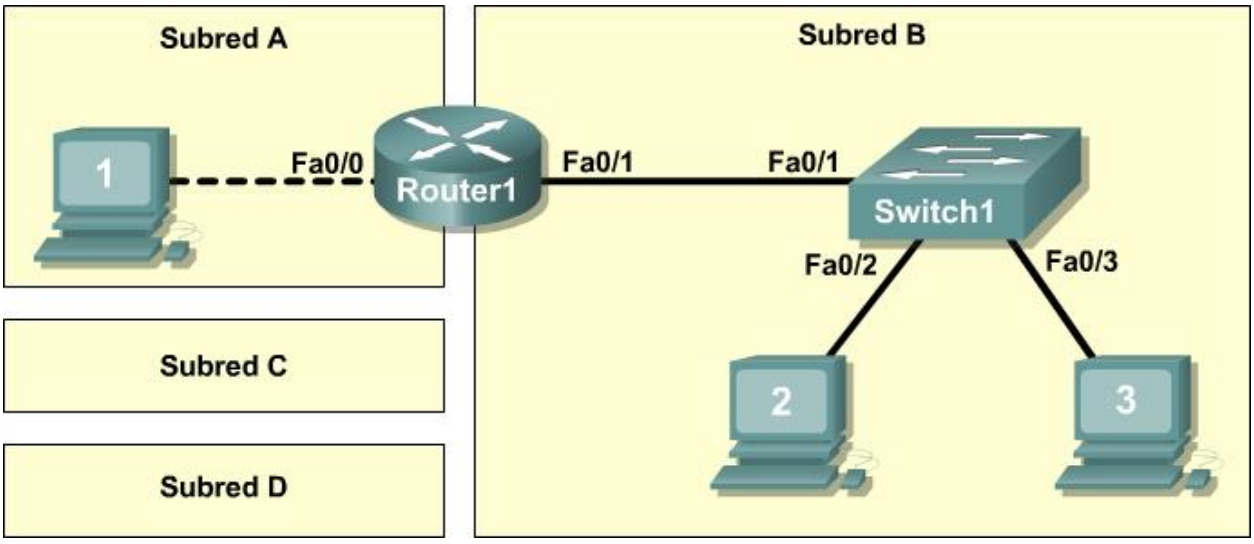


Figura 1. Cableado de la red

Realice el cableado de los dispositivos de red como se muestra en la Figura 1.

¿Qué tipo de cable necesita para conectar el Host1 con el Router1? ¿Por qué? _____ _____

_____

¿Qué tipo de cable necesita para conectar el Host1, el Host2 y el Router1 con el Switch1? ¿Por qué?

_____

_____

Si aún no está habilitada, suministre energía a todos los dispositivos.

Paso 2: Inspeccionar visualmente las conexiones de la red.

Después de realizar el cableado de los dispositivos de red, dedique unos minutos a verificar las conexiones. Prestar atención a los detalles ahora reducirá el tiempo necesario para diagnosticar un problema de conectividad más tarde. Asegúrese de que todas las conexiones del switch estén en verde. Cualquier conexión de switch que no cambie de ámbar a verde debe ser analizada. ¿Llega la energía de manera adecuada al dispositivo? ¿Empleó el cable correcto? ¿El cable correcto está en buenas condiciones?

¿Qué tipo de cable conecta la interfaz `Fa0/0` del Router1 con el Host1? _____

¿Qué tipo de cable conecta la interfaz `Fa0/1` del Router1 con el Switch1? _____

¿Qué tipo de cable conecta el Host2 con el Switch1? _____

¿Qué tipo de cable conecta el Host3 con el Switch1? _____

¿Están encendidos todos los equipos? _____

Tarea 3: Configurar la topología lógica.

Paso 1: Registre la configuración lógica de la red.

La dirección de IP del gateway del equipo host se utiliza para enviar paquetes IP a otras redes. Por lo tanto la dirección de gateway es la dirección IP asignada a la interfaz del router en esa subred.

A partir de la información sobre la dirección IP registrada en la Tarea 1, anote la información de la dirección IP de cada equipo:

Host1	
Dirección IP	
Máscara IP	
Dirección de puerta de enlace (gateway)	

Host2	
Dirección IP	
Máscara IP	
Dirección de puerta de enlace (gateway)	

Host3	
Dirección IP	
Máscara IP	
Dirección de puerta de enlace (gateway)	

Paso 2: Configure el equipo Host1.

En el Host1, haga clic en **Inicio > Panel de control > Conexiones de red**. Haga clic con el botón derecho en **Conexión de área local** y haga clic en **Propiedades**.

En la ficha **General**, seleccione **Protocolo de Internet (TCP/IP)** y luego haga clic en el botón **Propiedades**.

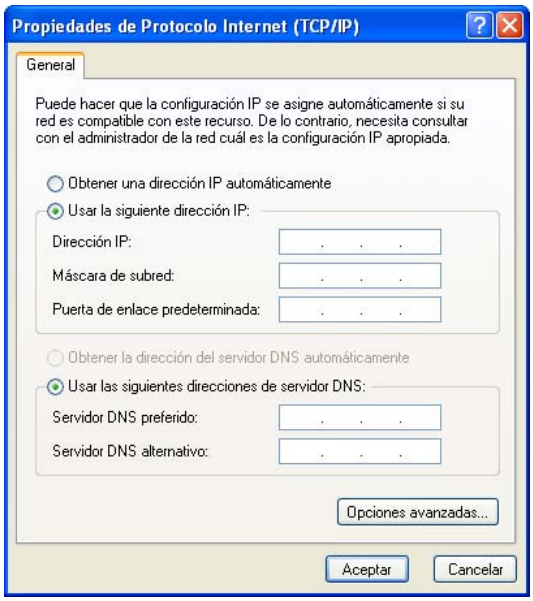


Figura 2. Configuración de dirección IP y gateway de Host1

Consulte la Figura 2 para determinar la configuración de dirección IP y gateway del Host1. Ingrese manualmente la siguiente información, registrada en el Paso 1 de arriba:

```
Dirección IP: Host1 IP address
Máscara de subred: Host1 subnet mask
Gateway por defecto: Gateway IP address
```

Cuando finalice, cierre la ventana de Propiedades del Protocolo de Internet (TCP/IP) haciendo clic en **Aceptar**. Cierre la ventana Conexión de área local. En función del sistema operativo de Windows, es posible que deba reiniciar el equipo para que se apliquen los cambios.

Paso 3: Configure los equipos Host2 y Host3.

Repita el Paso 2 con los equipos Host2 y Host3, utilizando la información de la dirección IP para dichos equipos.

Tarea 4: Verificar la conectividad de la red.

Verifique con el instructor que el Router1 haya sido configurado. De lo contrario, la conectividad entre las LAN estará interrumpida. El Switch1 debe tener una configuración predeterminada.

Se puede verificar la conectividad de la red con el comando **ping** de Windows. Abra una terminal de Windows haciendo clic en **Inicio > Ejecutar**. Escriba **cmd** y presione **Intro**.

Utilice la siguiente tabla para verificar y registrar de manera metódica la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Gateway (Router1, Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Host2		
Host1	Host3		
Host2	Host3		
Host2	Gateway (Router1, Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	Host2		
Host3	Gateway (Router1, Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

Detecte si hay alguna falla en la conectividad. El diagrama de topología puede ser muy útil para diagnosticar los problemas de conectividad.

En el escenario presentado, ¿cómo puede detectar un gateway que funciona mal?

_____

_____

Tarea 5: Reflexión

Repase los problemas de configuración física y lógica que hayan surgido durante la práctica de laboratorio. Asegúrese de que haya comprendido por completo los procedimientos utilizados para verificar la conectividad de la red.

Ésta es una práctica de laboratorio muy importante. Además de practicar cómo hacer subredes de IP, configuró equipos con direcciones de red y probó su conectividad.

Le recomendamos que practique varias veces la configuración del equipo host y la verificación. Esto afianzará las aptitudes que obtuvo en esta práctica de laboratorio y llegará a ser un mejor técnico de redes.

Tarea 6: Desafío

Solicite al instructor o a otro estudiante que presente uno o dos problemas en su red mientras usted no mira o se retira de la sala del laboratorio. Pueden ser físicos (cable UTP incorrecto), o lógicos (dirección IP o gateway incorrectos). Para solucionar los problemas:

1. Realice una buena inspección visual. Busque las luces de enlace verdes en el Switch1.

2. Utilice la tabla de la Tarea 3 para identificar la falla de conectividad. Enumere los problemas:

_____

_____

_____

_____

_____

3. Describa las soluciones propuestas:

_____

_____

_____

_____

_____

4. Pruebe la solución planteada. Si con esto se soluciona el problema, registre la solución. De lo contrario, continúe con la resolución del problema.

_____

_____

_____

_____

_____

_____

_____

_____

Tarea 7: Limpieza.

A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host.

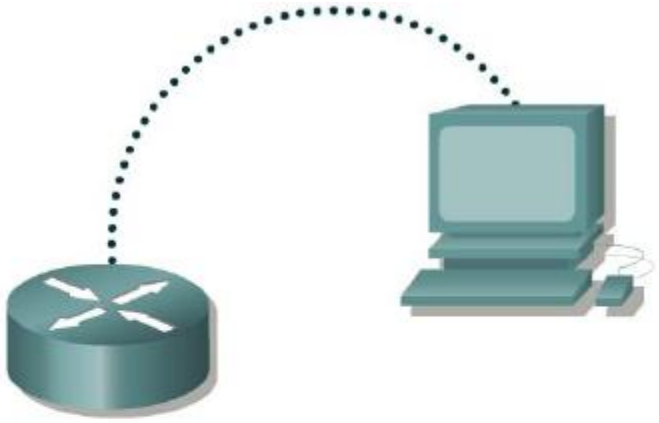
Retire con cuidado los cables y guárdelos de manera ordenada. Vuelva a conectar los cables que desconectó para esta práctica de laboratorio.

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Apéndice 1

Práctica de laboratorio 10.6.2: Cómo establecer una sesión de consola con HyperTerminal

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Conectar un router y un equipo utilizando un cable de consola.
- Configurar HyperTerminal para establecer una sesión de consola con el router IOS de Cisco.
- Configurar HyperTerminal para establecer una sesión de consola con el switch IOS de Cisco.

Información básica

HyperTerminal es un programa sencillo de emulación de terminal basado en Windows para comunicación serial, que se puede utilizar para conectarse al puerto de consola de los dispositivos IOS de Cisco. Se conecta una interfaz serial de una computadora con el dispositivo Cisco a través de un cable de consola. HyperTerminal es la forma más sencilla de acceder a un router para verificar o cambiar su configuración. Otra conocida utilidad de comunicación serial es TeraTerm Web. Las instrucciones para el uso de TeraTerm Web se describen en el Apéndice A.

Escenario

Establezca una red similar a la del Diagrama de topología. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Entre las posibles opciones están los routers 800, 1600, 1700, 2500, 2600 o una combinación de los mismos. Serán necesarios los siguientes recursos:

- Una computadora con una interfaz serial e HyperTerminal instalado
- Un router Cisco
- Un cable de consola (transpuesto) para conectar la estación de trabajo al router

Tarea 1: Conectar un router y una computadora con un cable de consola.

Paso 1: Establezca la conexión física básica.

Conecte el cable de consola (transpuesto) al puerto de consola del router. Conecte el otro extremo del cable al equipo host con un adaptador DB-9 o DB-25 al puerto COM 1.

Paso 2: Encienda los dispositivos.

Si todavía no están encendidos, encienda la computadora y el router.

Tarea 2: Configurar HyperTerminal para establecer una sesión de consola con el router IOS de Cisco.

Paso 1: Inicie la aplicación HyperTerminal.

Desde la barra de tareas de Windows, ejecute el programa HyperTerminal haciendo clic en **Inicio > Programas > Accesorios > Comunicaciones > HyperTerminal**.

Paso 2: Configure HyperTerminal.

Figura 1. Ventana de configuración de nombre de HyperTerminal

Consulte la Figura 1 para obtener una descripción de la ventana inicial de configuración de HyperTerminal. En la ventana Descripción de la conexión introduzca un nombre de sesión en el campo Nombre. Seleccione un ícono adecuado o deje el predeterminado. Haga clic en **Aceptar**.

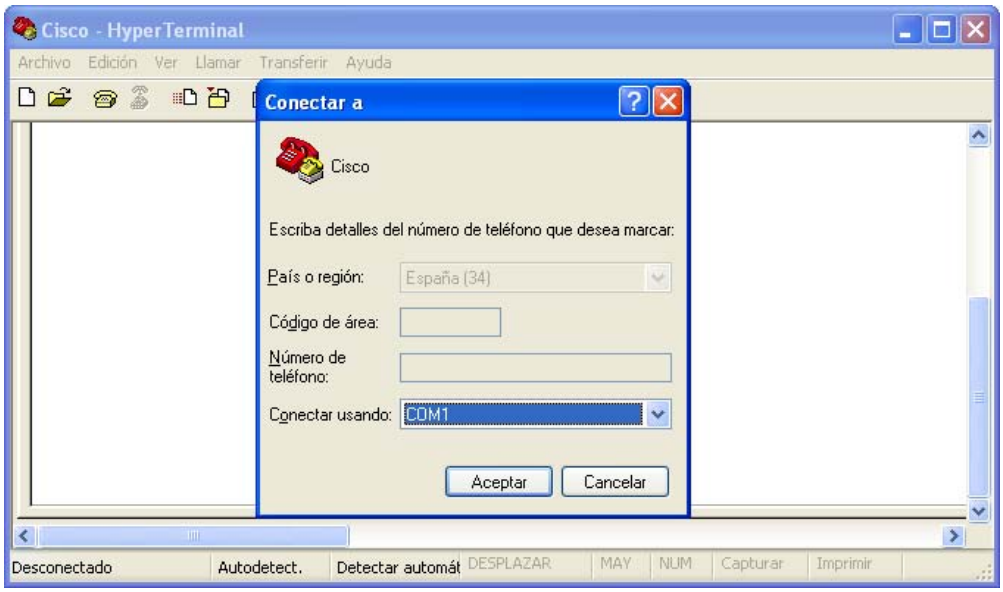


Figura 2. Tipo de conexión de HyperTerminal

Consulte la figura 2. Ingrese el tipo de conexión adecuado, COM 1, en el campo Conectar con. Haga clic en **Aceptar**.

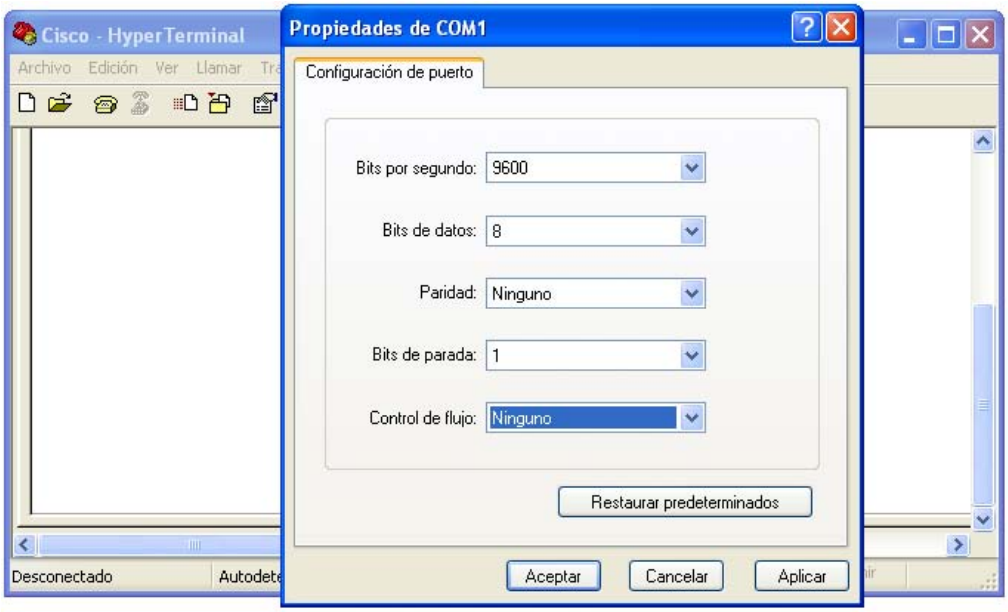


Figura 3. Configuración de puertos COM1 de HyperTerminal

Consulte la Figura 3. Cambie la configuración de puertos con los siguientes valores:

Configuración	**Valor**
Bits por segundo	**9600**
Bits de datos	**8**
Paridad	**Ninguno**
Bits de parada	**1**
Control del flujo	**Ninguno**

Haga clic en **Aceptar**.

Cuando inicie la ventana de sesión de HyperTerminal, presione la tecla **Intro**. Deberá haber una respuesta del router. Esto indica que la conexión se realizó de manera exitosa. Si no hay ninguna conexión, resuelva el problema según sea necesario. Por ejemplo, verifique que el router esté conectado. Compruebe la conexión hacia el puerto COM 1 correcto en la PC y el puerto de la consola en el router. Si todavía no se puede conectar, solicite asistencia del instructor.

Paso 3: Cierre HyperTerminal.

Cuando termine, cierre la sesión de HyperTerminal. Haga clic en **Archivo > Salir**. Cuando se le pregunta si desea guardar la sesión, haga clic en **Sí**. Ingrese un nombre para la sesión.

Paso 4: Reconecte la sesión HyperTerminal.

Reabra la sesión HyperTerminal como se describe en la Tarea 2 del Paso 1. Esta vez, cuando se abra la ventana de Descripción de la conexión (ver Figura 1), haga clic en **Cancelar**.

Haga clic en **Archivo > Abrir**. Seleccione la sesión guardada y luego haga clic en **Abrir**. Use esta técnica para reconectar la sesión de HyperTerminal con un dispositivo Cisco sin reconfigurar una nueva sesión.

Cuando termine, salga de TeraTerm.

Tarea 3: Configurar HyperTerminal para establecer una sesión de consola con el switch IOS de Cisco.

Las conexiones seriales entre routers y switches IOS de Cisco son muy similares. En esta tarea, usted creará una conexión serial entre el equipo host y un switch IOS de Cisco.

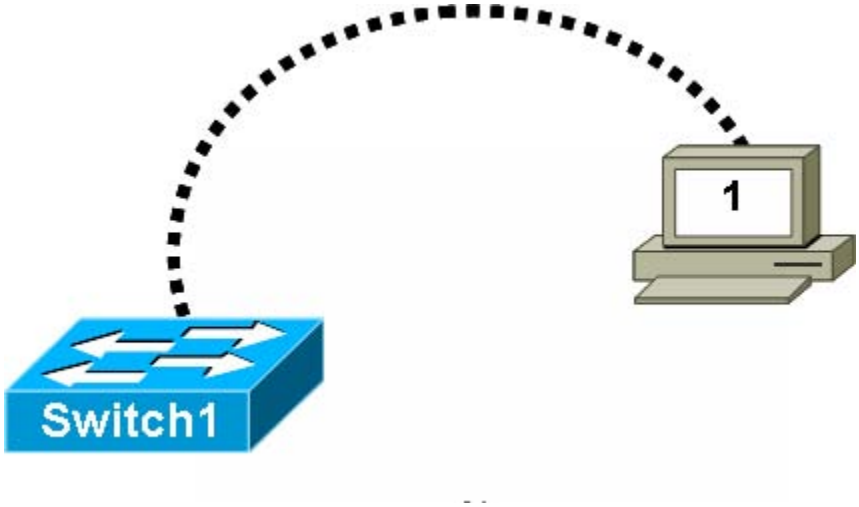


Figura 4. Conexión serial entre un equipo host y un switch Cisco

Paso 1: Establezca la conexión física básica.

Consulte la Figura 4. Conecte el cable de consola (transpuesto) al puerto de la consola en el router. Conecte el otro extremo del cable al equipo host con un adaptador DB-9 o DB-25 al puerto COM 1.

Paso 2: Encienda los dispositivos.

Si todavía no han sido encendidos, encienda el equipo y el switch.

Paso 3: Inicie la aplicación HyperTerminal.

Desde la barra de tareas de Windows, inicie el programa HyperTerminal haciendo clic en **Inicio > Programas > Accesorios > Comunicaciones > HyperTerminal**.

Paso 4: Configure HyperTerminal.

Use el procedimiento descrito en la Tarea 2, del Paso 2 para configurar HyperTerminal.

Consulte la Figura 1 de la ventana inicial de configuración de HyperTerminal. En la ventana Descripción de la conexión introduzca un nombre de sesión en el campo Nombre. Seleccione un ícono adecuado o deje el predeterminado. Haga clic en **Aceptar**.

Consulte la figura 2. Ingrese el tipo de conexión adecuado, COM 1, en el campo Conectar con. Haga clic en **Aceptar**.

Consulte la Figura 3. Cambie la configuración de puertos con los siguientes valores:

Configuración	Valor
Bits por segundo	**9600**
Bits de datos	**8**
Paridad	**Ninguno**
Bits de parada	**1**
Control del flujo	**Ninguno**

Haga clic en **Aceptar**.

Cuando inicie la ventana de sesión de HyperTerminal, presione la tecla **Intro**. Deberá haber una respuesta del switch. Esto indica que la conexión se realizó de manera exitosa. Si no hay ninguna conexión, resuelva el problema según sea necesario. Por ejemplo, verifique que el switch esté conectado. Compruebe la conexión hacia el puerto COM 1 correcto en la PC y el puerto de la consola en el switch. Si todavía no se puede conectar, solicite asistencia del instructor.

Paso 5: Cierre HyperTerminal.

Cuando termine, cierre la sesión de HyperTerminal. Haga clic en **Archivo > Salir**. Cuando se le pregunta si desea guardar la sesión, haga clic en **No**.

Tarea 3: Reflexión

En esta práctica de laboratorio se le brindó información para establecer una conexión de consola con un router y con un switch IOS de Cisco.

Tarea 4: Desafío

Dibuje las conexiones de pin para el cable de consola y para el cabe de conexión directa. Compare las diferencias y podrá identificar los diferentes tipos de cables.

Tarea 5: Limpieza

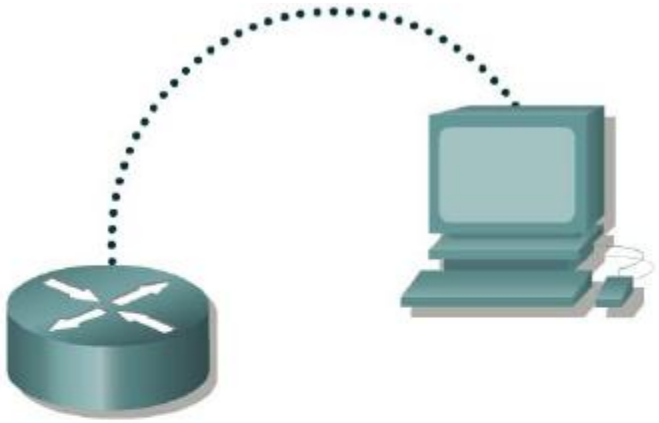
A menos que el instructor indique lo contrario, desconecte el equipo host y el router. Quite el cable transpuesto.

Llévese todo aquello que haya traído al laboratorio y deje la habitación lista para la próxima clase.

Apéndice A

Cómo establecer una sesión de consola con TeraTerm

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Conectar un router y un equipo utilizando un cable de consola.
- Configurar TeraTerm para establecer una sesión de consola con el router.

Información básica

TeraTerm Web es otro sencillo programa de emulación de terminal basado en Windows para comunicación serial, que se puede utilizar para conectarse al puerto de consola de los dispositivos IOS de Cisco.

Escenario

Cree una red con un cableado similar al del Diagrama de topología. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Entre las posibles opciones están los routers 800, 1600, 1700, 2500, 2600 o una combinación de los mismos. Serán necesarios los siguientes recursos:

- Un equipo con una interfaz serial y con TeraTerm Pro instalado
- Un router Cisco
- Un cable de consola (transpuesto) para conectar la estación de trabajo al router

Tarea 1: Conectar un router y una computadora con un cable de consola.

Paso 1: Establezca la conexión física básica.

Asegúrese de que esté apagada la energía del equipo y el router Cisco. Conecte el cable de consola (transpuesto) al puerto de consola del router. Conecte el otro extremo del cable a la PC con un adaptador DB-9 o DB-25 al puerto COM 1.

Paso 2: Encienda los dispositivos.

Encienda el equipo y el router.

Tarea 2: Configurar TeraTerm Web para establecer una sesión de consola con el router.

Paso 1: Inicie la aplicación TeraTerm Web.

Desde la barra de tareas de Windows, inicie el programa TeraTerm Web abriendo la carpeta TeraTerm Web e iniciando la aplicación TeraTerm Web, **`ttermpro`**.

Paso 2: Configure TeraTerm Web.

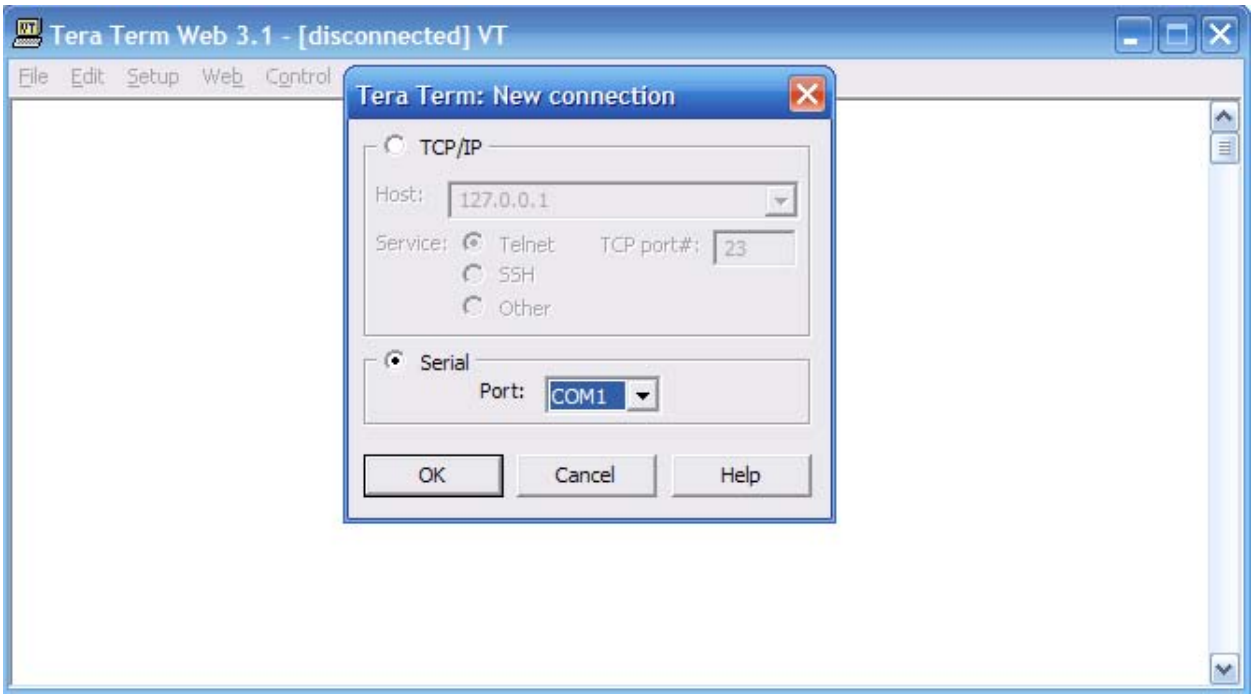


Figura 1. Ventana de configuración de conexión de TeraTerm Web

Haga clic en **Archivo > Conexión nueva**. Consulte la Figura 1. Seleccione el puerto serial COM adecuado. Haga clic en **Aceptar**.

Cuando inicie la ventana de sesión de TeraTerm Web, presione la tecla **Intro**. Deberá haber una respuesta del router. La conexión se realizó de manera exitosa. Si no hay ninguna conexión, resuelva el problema según sea necesario. Por ejemplo, verifique que el router esté conectado. Compruebe la conexión hacia el puerto COM 1 en la PC y el puerto de la consola en el router. Si todavía no se puede conectar, solicite asistencia del instructor.

Paso 3: Cierre TeraTerm Web.

Cuando termine, cierre la sesión de TeraTerm Web. Haga clic en **Archivo | Salir**. Cuando se le pregunta si desea guardar la sesión, haga clic en **Sí**. Ingrese un nombre para la sesión.

Paso 4: Reconecte la sesión TeraTerm Web.

Reabra la sesión TeraTerm Web como se describe en la Tarea 2 del Paso 1. Esta vez, cuando se abra la ventana de Descripción nueva (ver Figura 1), haga clic en **Cancelar**.

Haga clic en **Archivo > Abrir**. Seleccione la sesión guardada y luego haga clic en **Abrir**. Use esta técnica para reconectar la sesión de TeraTerm Web con un dispositivo Cisco sin reconfigurar una nueva sesión.

Tarea 3: Reflexión

En este laboratorio se le brindó información para establecer una conexión de consola con un router Cisco. Es posible acceder a los switches Cisco de la misma manera.

Tarea 4: Desafío

Dibuje las conexiones de pin para el cable de consola y para el cabe de conexión directa. Compare las diferencias y podrá identificar los diferentes tipos de cables.

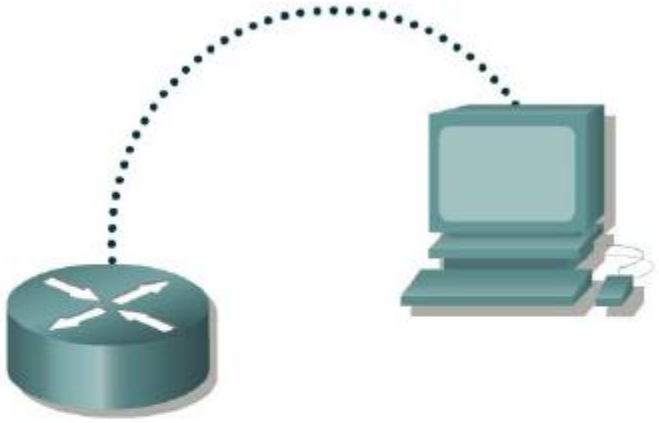
Tarea 5: Limpieza

A menos que el instructor indique lo contrario, desconecte el equipo host y el router. Quite el cable transpuesto.

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Práctica de laboratorio 10.6.3: Cómo establecer de una sesión de consola con Minicom

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Conectar un router y un equipo utilizando un cable de consola.
- Configurar Minicom para establecer una sesión de consola con el router.
- Ejecutar comandos básicos.

Información básica

Minicom es un programa UNIX de emulación de terminal basado en texto, similar al programa HyperTerminal de Windows. Se puede utilizar para distintos propósitos, como controlar un módem o acceder a un router Cisco mediante la conexión de consola serial. Se requiere el sistema operativo Linux o UNIX.

Escenario

Establezca una red similar a la del Diagrama de topología. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Entre las posibles opciones están los routers 800, 1600, 1700, 2500, 2600 o una combinación de los mismos. Serán necesarios los siguientes recursos:

- Computadora con Linux o UNIX con interfaz serial y Minicom cargado.

- Un router Cisco.
- Un cable de consola (transpuesto) para conectar la estación de trabajo al router.

Tarea 1: Conectar un router y una computadora con un cable de consola.

Paso 1: Establezca la conexión física básica.

Asegúrese de que esté apagada la energía del equipo y el router Cisco. Conecte el cable de consola (transpuesto) al puerto de consola del router. Conecte el otro extremo del cable a la PC con un adaptador DB-9 o DB-25 al puerto COM 1.

Paso 2: Encienda los dispositivos.

Encienda el equipo y el router.

Tarea 2: Configurar Minicom para establecer una sesión de consola con el router.

Paso 1: Inicie la aplicación de Minicom en el modo de configuración.

Nota: Para configurar Minicom, se requiere acceso a la raíz. Desde el indicador de comandos de Linux, inicie **`minicom`** con la opción **`-s`**. Esto ejecuta Minicom en el modo de configuración:

```
[root]# minicom -s <ENTER>
```

Paso 2: Configure Minicom para lograr comunicaciones seriales.

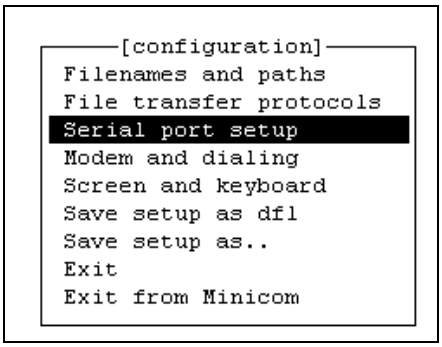


Figura 1. Ventana principal de configuración

Consulte la Figura 1. Para configurar el puerto serial, desplácese por la lista de configuración y seleccione **`Serial port setup`**. Presione **Intro**.

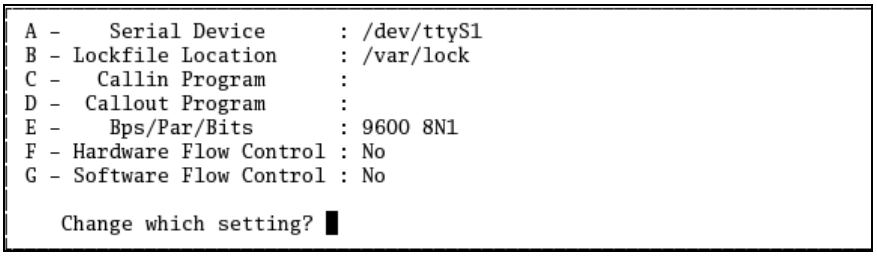


Figura 2. Ventana de configuración del puerto serial

Consulte la Figura 2. Utilice la letra por campo para cambiar una configuración. Consulte la Tabla 1 para determinar los valores correctos.

Opción	Campo	Valor
A	Dispositivo serial	/dev/ttyS0 para COM1 /dev/ttyS1 para COM2
E	Bps/Par/Bits	Bps- 9600 Paridad = Ninguna Bits- 8 Bits de parada- 1 (o bien, seleccione la opción "Q")
F	**Control del flujo del hardware**	Seleccione - No
G	**Control del flujo del software**	Seleccione - No

Tabla 1. Configuración del puerto serial

Regrese al menú de configuración presionando **Intro** o **Esc**.

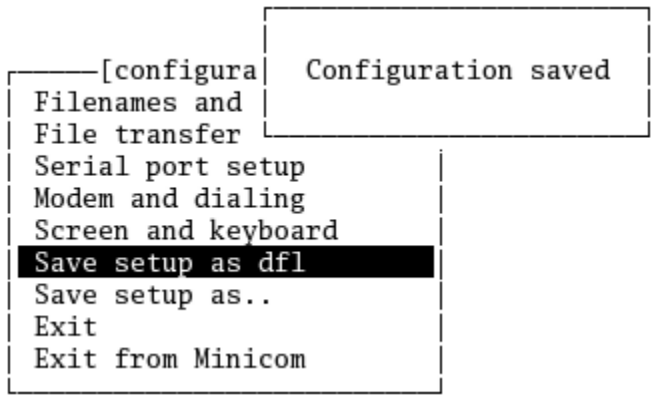


Figura 3. Ventana de configuración del puerto serial

Consulte la Figura 3. Seleccione **Save setup as dfl** (archivo predeterminado). Cuando reinicie Minicom, los valores predeterminados se volverán a cargar.

Paso 3: Cierre Minicom.

Cuando termine, cierre la sesión de Minicom. Seleccione **Exit from Minicom**.

Paso 4: Reinicie la sesión Minicom.

```
[root]# minicom <ENTER>
```

Cuando inicie la ventana de sesión, presione la tecla **Intro**. Deberá haber una respuesta del router. Esto indica que la conexión se realizó de manera exitosa. Si no hay ninguna conexión, resuelva el problema según sea necesario. Por ejemplo, verifique que el router esté conectado. Compruebe la conexión hacia el puerto COM1 correcto en la PC y el puerto de la consola en el router. Si todavía no se puede conectar, solicite asistencia del instructor.

Tarea 3: Ejecutar comandos básicos.

Minicom es una utilidad de comunicación serial, basada en texto y administrada con menú. Los comandos básicos no son intuitivos. Por ejemplo, los usuarios se comunican con dispositivos remotos dentro de la ventana de la terminal. Sin embargo, para controlar la utilidad utilice **<CTRL> A**. Para obtener ayuda, presione **<CTRL> A**, seguido por **Z**.

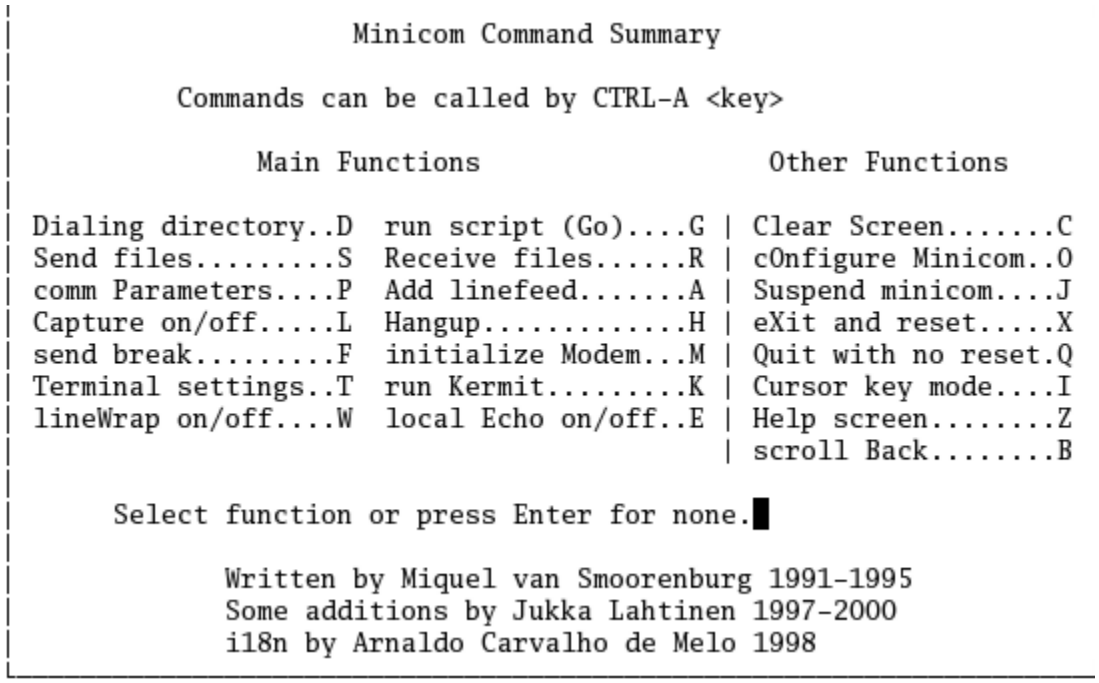


Figura 4. Pantalla de resumen de comandos de Minicom

En la Figura 4 encontrará una lista de funciones con las correspondientes teclas. Para salir de Minicom, presione **<CTRL> A**, seguido por **Q** o **X**.

Tarea 4: Reflexión

En este laboratorio se le brindó información para establecer una conexión de consola con un router Cisco mediante Minicom. Es posible acceder a los switches Cisco de la misma manera.

Tarea 5: Limpieza

A menos que el instructor indique lo contrario, desconecte el equipo host y el router. Quite el cable transpuesto.

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

10.7.1: Desafío de integración de aptitudes: Planificación de redes y configuración de interfaz

Diagrama de topología

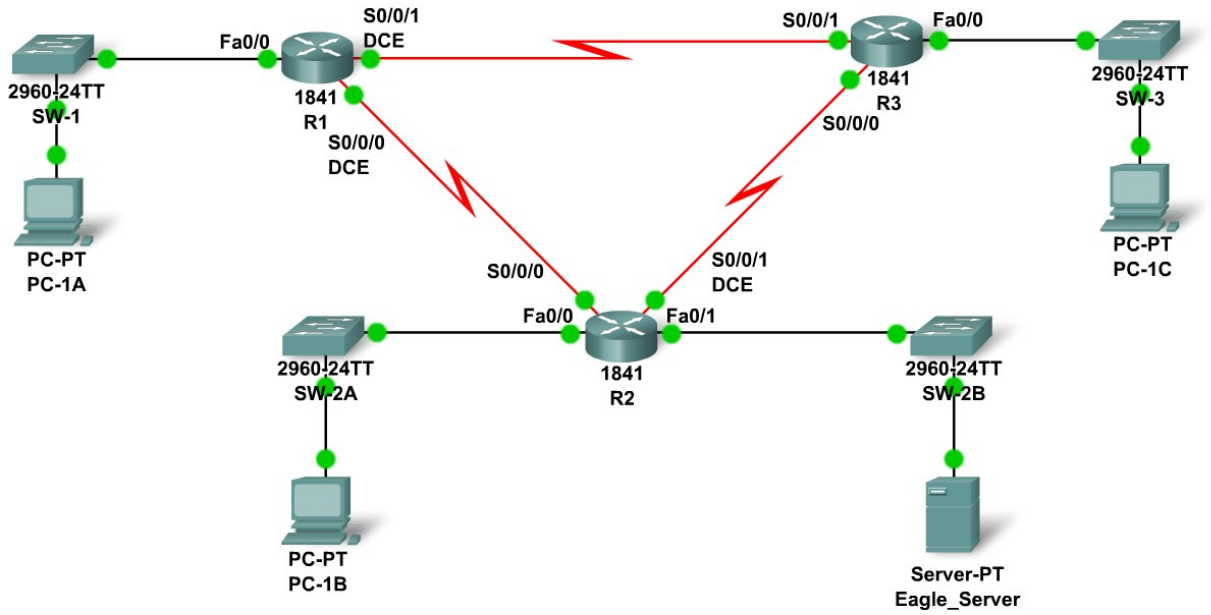


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/0			No aplicable
	S0/0/0			No aplicable
	S0/0/1			No aplicable
R2	Fa0/0			No aplicable
	Fa0/1			No aplicable
	S0/0/0			No aplicable
	S0/0/1			No aplicable
R3	Fa0/0			No aplicable
	S0/0/0			No aplicable
	S0/0/1			No aplicable
PC-1A	NIC			
PC-2A	NIC			
PC-3A	NIC			
Eagle_Server	NIC			

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Crear la topología de red.
- Planificar las direcciones IP.
- Configurar interfaces de routers y PC.
- Probar la red.

Información básica

Practique sus habilidades de creación, planificación y configuración de redes. Los nombres y el enrutamiento de los dispositivos ya han sido configurados.

Tarea 1: Creación de la topología de red.

Use los siguientes cuadros y los dispositivos del conjunto de dispositivos para crear la topología.

Routers:

Nombre de host	Interfaz	Conectar a	Interfaz
R1	Fa0/0	SW-1	Fa0/1
R1	S0/0/0 (DCE)	R2	S0/0/0
R1	S0/0/1 (DCE)	R3	S0/0/1
R2	Fa0/0	SW-2A	Fa0/1
R2	S0/0/1 (DCE)	R3	S0/0/0
R2	Fa0/1	SW-2B	Fa0/1
R3	Fa0/0	SW-3	Fa0/1

Switches:

Nombre de host	Interfaz	Conectar a	Interfaz
SW-1	Fa0/2	PC-1A	FastEthernet
SW-2A	Fa0/2	PC-1B	FastEthernet
SW-2B	Fa0/2	Eagle_Server	FastEthernet
SW-3	Fa0/2	PC-1C	FastEthernet

Tarea 2: Creación y asignación de un esquema de direcciones.

Se le pide que use el espacio de direcciones 192.168.1.0 /24. Se requieren siete redes en total; asigne las redes en orden decreciente de cantidad de hosts requeridos para un uso eficiente del espacio de direccionamiento. Use los siguientes cuadros para crear un esquema efectivo de direcciones.

LAN:

Nombre de host	Interfaz	Cantidad de hosts
R1	Fa0/0	60
R2	Fa0/0	10
	Fa0/1	30
R3	Fa0/0	7

WAN:

Nombre de host	Dirección que se asignará	Cantidad de hosts
R1-R2	R1: Primera dirección de host	2
R1-R3	R1: Primera dirección de host	2
R2-R3	R2: Primera dirección de host	2

Use las siguientes reglas para asignar direcciones IP.

- Las PC usarán la primera dirección de host de la subred, el servidor usará desde la segunda hasta la última dirección de su subred.
- Todos los puertos FastEthernet de un router usarán la última dirección de host de la subred asignada.
- El enlace R1-R2 utilizará la primera subred WAN, el enlace R1-R3 utilizará la segunda subred WAN y el enlace R2-R3 utilizará la tercera subred WAN. Las interfaces DCE de R1 y R2 deben tener frecuencia de reloj de 56000.

Tarea 3: Configuración de la interfaz

Realice la configuración de las interfaces de los routers R1, R2 y R3, las PC y el servidor, según el esquema de direccionamiento descrito anteriormente.

Tarea 4: Verificación de conectividad

Asegúrese de que todas las PC puedan realizar ping a sus gateways, otras PC y el servidor.

11.4.3.3: Documentación sobre la latencia de red con ping

Diagrama de topología

Objetivos de aprendizaje

- Usar el comando **`ping`** para documentar la latencia de red.
- Calcular diversas estadísticas a partir de los resultados de una captura **`ping`**.
- Medir los efectos de retardo en datagramas más grandes.

Información básica

Para obtener estadísticas reales sobre latencia, se debe realizar esta actividad en una red activa. Asegúrese de consultar con su instructor si existen restricciones locales de seguridad para el uso del comando **`ping`** en la red.

La computadora del servidor de destino debe enviar respuestas de ECO. De lo contrario, no se puede calcular el retardo. Algunas computadoras tienen esta característica deshabilitada a través de un firewall y algunas redes privadas bloquean el tránsito de datagramas de ECO. Para que este experimento resulte interesante, se debe escoger un destino bien distante. Por ejemplo, destinos en la misma LAN o a pocos saltos, pueden devolver una baja latencia que no es representativa. Con paciencia se puede encontrar un destino adecuado.

El objetivo de esta actividad de laboratorio es medir y evaluar la latencia de red en el tiempo y durante diferentes momentos del día para capturar una muestra representativa de la actividad típica de la red. Esto se logrará a través del análisis del retardo de retorno desde una computadora remota con un comando **`ping`**.

El análisis estadístico del retardo en la velocidad de transmisión (rendimiento) se realizará con la ayuda de una hoja de cálculo, como Microsoft Excel. Los tiempos de retardo de retorno, medidos en milisegundos, se resumirán a través del cálculo de la latencia promedio (media), teniendo en cuenta el valor de latencia del centro del rango ordenado de puntos de latencia (mediano) e identificando los retardos más frecuentes (modo). El Apéndice contiene una tabla que puede ser entregada al instructor una vez finalizado.

El retardo también se medirá cuando aumente el tamaño del datagrama ICMP.

Escenario

En el gráfico de topología anterior, la nube de red puede representar todos los dispositivos de red y el cableado entre la computadora del estudiante y la computadora del servidor de destino. Generalmente, son estos dispositivos los que presentan la latencia de red. Habitualmente, los ingenieros de redes dependen de redes fuera de la administración local para realizar la conectividad con redes externas. El monitoreo de la latencia de ruta también proporciona algunas mediciones de importancia administrativa que pueden ser usadas en la toma de decisiones cuando se evalúan aplicaciones adecuadas para la implementación de redes de área extensa (WAN).

Esta actividad demandará cinco días de pruebas. Se realizarán tres pruebas por día. Preferentemente, se realizará una prueba por la mañana temprano, una al mediodía y una a la tarde. La idea es identificar y documentar las diferencias de latencia durante diferentes momentos del día. Una vez finalizado, habrá un total de 15 grupos de estos datos.

Para comprender los efectos de retardo de datagramas más grandes, se enviarán y analizarán datagramas ICMP con datagramas cada vez más grandes.

Tarea 1: Uso del comando `ping` para documentar la latencia de red.

Paso 1: Verificar la conectividad entre la computadora del estudiante y la computadora del servidor de destino.

Para verificar la conectividad entre la computadora del estudiante y la computadora del servidor de destino, abra una ventana del terminal haciendo clic en inicio | ejecutar. Ingrese **`cmd`** y luego seleccione **`Aceptar`**. Intente enviar un ping a un destino lo suficientemente distante, como por ejemplo `www.yahoo.com`:

```
C:\> ping -n 1 www.yahoo.com
Pinging www.yahoo-ht3.akadns.net [209.191.93.52] with 32 bytes of data:
Reply from 209.191.93.52: bytes=32 time=304ms TTL=52
Ping  statistics for 209.191.93.5:
      Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
      Approximate round trip times in milli-seconds:
      Minimum = 304ms, Maximum = 304ms , Average = 304 ms
```

Use el comando **`ping /?`** para contestar las siguientes preguntas:

¿Cuál es el objetivo de la opción `-n` y el argumento `1`?

_____

_____

¿Qué opción y argumento cambiaría el tamaño predeterminado a 100 bytes? _____

Escoja una computadora del servidor de destino y escriba el nombre: _____

Use el comando **`ping`** para verificar la conectividad con el destino y escriba los resultados:

Paquetes enviados	Paquetes recibidos	Paquetes perdidos

Si hay paquetes perdidos use otro destino y vuelva a realizar la prueba.

Paso 2: Realizar una prueba de retardo.

Escriba el comando que enviará 100 solicitudes de ECO al destino:

_____

Use el comando ping para enviar 100 solicitudes de ECO al destino elegido. Cuando termine, copie las respuestas en un Bloc de notas. El Bloc de notas se puede abrir haciendo clic en Inicio | Programas | Accesorios y luego seleccionando Bloc de notas. Guarde el archivo con el formato de nombre *day-sample#.txt*, donde: *day* = el día en el cual se realizó la prueba (1 – 5), y *sample#* = el período de muestra (1 – 3).

También puede redireccionar el resultado a un archivo si agrega *> day-sample#.txt* al final del comando **ping**. NOTA: el terminal permanecerá en blanco hasta que el comando haya terminado.

Tarea 2: Cómputo de diversas estadísticas a partir de los resultados de una captura ping.

Paso 1: Abrir el archivo de texto en una hoja de cálculo Excel.

Si aún no está abierto, inicie Microsoft Excel. Seleccione las opciones del menú Archivo | Abrir. Use Explorar para llegar al directorio donde se encuentra el archivo de texto. Seleccione el nombre de archivo y elija Abrir. Para formatear un archivo de texto para usar en Excel, asegúrese de que todos los valores numéricos estén separados de los caracteres de texto. En el Asistente para importar texto, en el Paso 1, seleccione Ancho fijo. En el Paso 2, siga las instrucciones en la pantalla para separar los valores numéricos de los valores de texto. Consulte la Figura 1.

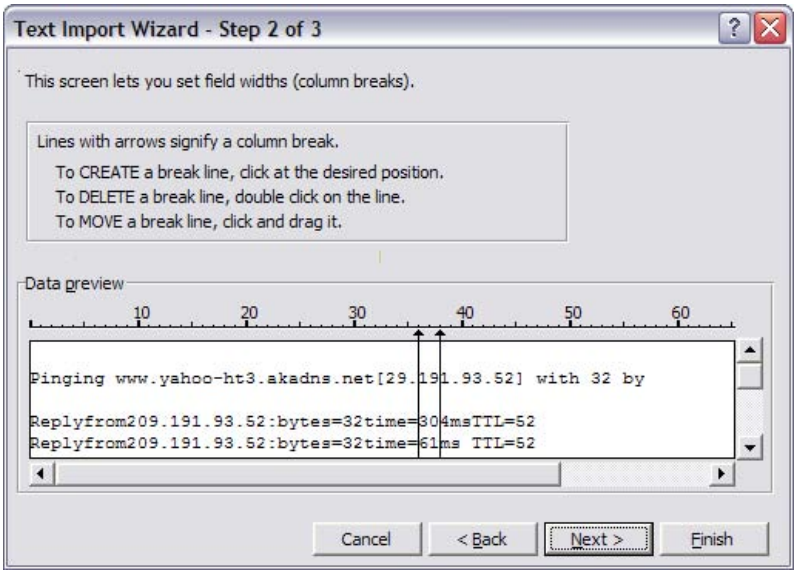


Figura 1. Asistente para importar texto de Excel.

Paso 2: Calcular los valores de retardo medio, mediano y de modo.

Cuando el formateo sea satisfactorio, seleccione **Finalizar**. Si la hoja de cálculo tiene números en campos diferentes, arregle manualmente los números. Una vez que haya abierto la hoja de cálculo, arregle el formato de las columnas para que sean más legibles. Cuando esté completo, usted debe tener una hoja de cálculo similar a la Figura 2.

	A	B	C	E	G	I
1				Bytes	Tiempo (ms	TTL
2	Respuesta	desde	209.191.93.52:	32	304	52
3	Respuesta	desde	209.191.93.52:	32	61	52
4	Respuesta	desde	209.191.93.52:	32	56	52
5	Respuesta	desde	209.191.93.52:	32	54	52
6	Respuesta	desde	209.191.93.52:	32	65	52
7	Respuesta	desde	209.191.93.52:	32	55	52

Figura 2. Hoja de cálculo parcial con formato correcto.

Anote en la tabla la cantidad de paquetes descartados, en la columna Paquetes descartados. Los paquetes descartados tendrán un valor de retardo consistentemente grande.

Finalmente, debe ordenar (clasificar) los valores de retardo cuando calcule los valores medianos y de modo. Esto se puede hacer con las opciones de menú Datos | Clasificar. Resalte todos los campos de datos. La Figura 3 muestra parte de una hoja de cálculo resaltada y el menú Datos | Clasificar abierto. Si se resaltó una fila de encabezado, haga clic en el botón de selección Fila de encabezado. Seleccione la columna que contenga los valores de Retardo. En la Figura 3 es la columna G. Cuando termine, haga clic en Aceptar.

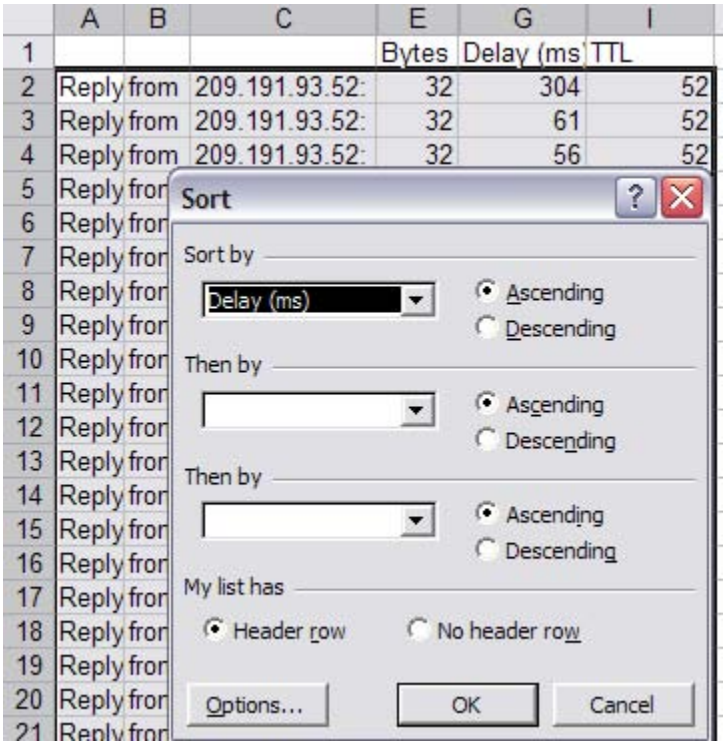


Figura 3. Ordenar la columna Retardo.

La formula que se usa para calcular el retardo medio, o promedio, es la suma de los retardos dividida por la cantidad de mediciones. Tomando el ejemplo anterior, ésta sería equivalente a la fórmula en la celda G102: `=promedio(G2:G101)`. Realice una “comprobación visual de validez” (sanity check) para verificar que el valor medio obtenido sea aproximado al valor mostrado. Anote este número en la tabla, debajo de la columna Medio.

La formula que se usa para calcular el retardo mediano, o el valor del retardo del centro del rango ordenado, es similar a la fórmula de promedio anterior. Para el valor mediano, la fórmula en la celda G103 sería `=mediano(G2:G101)`. Realice una ‘comprobación visual de validez’ para verificar que el

valor mediano obtenido sea similar al que se muestra en la mitad del rango de datos. Anote este número en la tabla, debajo de la columna Mediano.

La fórmula que se usa para calcular el retardo modal, o el valor de retardo que más se repite, también es similar. Para el valor modo, la fórmula en la celda G104 sería `=modo(G2:G101)`. Realice una "comprobación visual de validez" para verificar que el valor modo obtenido sea similar al valor que más se repite en el rango de datos. Anote este número en la tabla, debajo de la columna Modo.

Se puede guardar o desechar el nuevo archivo de hoja de cálculo, pero el archivo de datos de texto debe ser conservado.

Tarea 3: Medición de los efectos de retardo en datagramas más grandes.

Para determinar si un datagrama más grande afecta el retardo, se enviarán al destino solicitudes de ECO cada vez más grandes. En este análisis, se aumentarán 20 datagramas cada 100 bytes por petición de **`ping`**. Con los resultados de las respuestas se creará una hoja de cálculo y se generará un gráfico que compara el tamaño con el retardo.

Paso 1: Realizar una prueba de retardo de tamaño variable.

La forma más sencilla para realizar esta tarea es usar el comando incorporado de Windows PARA loop. La sintaxis es:

```
FOR /L %variable IN (start,step,end) DO command [command-parameters]

El conjunto es una secuencia de números de principio a fin, por cantidad
escalonada. Así, (1,1,5) produciría la secuencia 1 2 3 4 5 y (5,-1,1)
produciría la secuencia (5 4 3 2 1)
```

En el siguiente comando, *`destination`* es el destino. Emita el siguiente comando:
`FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i destination`

Copie el resultado en el Bloc de notas y guarde el archivo con el nombre `variablesizedelay.txt`.

Para redireccionar el resultado a un archivo, use el operador agregado de redireccionamiento, **>>**, como se muestra más abajo. El operador normal de redireccionamiento, **>**, destruirá el archivo cada vez que se ejecute el comando ping y sólo se guardará la última respuesta. NOTA: el terminal permanecerá en blanco hasta que el comando haya terminado.

`FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i destination >> variablesizedelay.txt`

A continuación se muestra el resultado de una línea. Las 20 respuestas se ordenan de forma similar:

```
C:\> FOR /L %i IN (100,100,2000) DO ping –n 1 –l %i www.yahoo.com

C:\> ping -n 1 -l 100 www.yahoo.com

Pinging www.yahoo-ht3.akadns.net [209.191.93.52] with 100 bytes of data:
Reply from 209.191.93.52: bytes=100 time=383ms TTL=52

Ping statistics for 209.191.93.52:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 383ms, Maximum = 383ms, Average = 383ms
```

Paso 2: Abrir el archivo de texto en una hoja de cálculo Excel.

Abra el nuevo archivo de texto en Excel. Consulte la Figura 4.

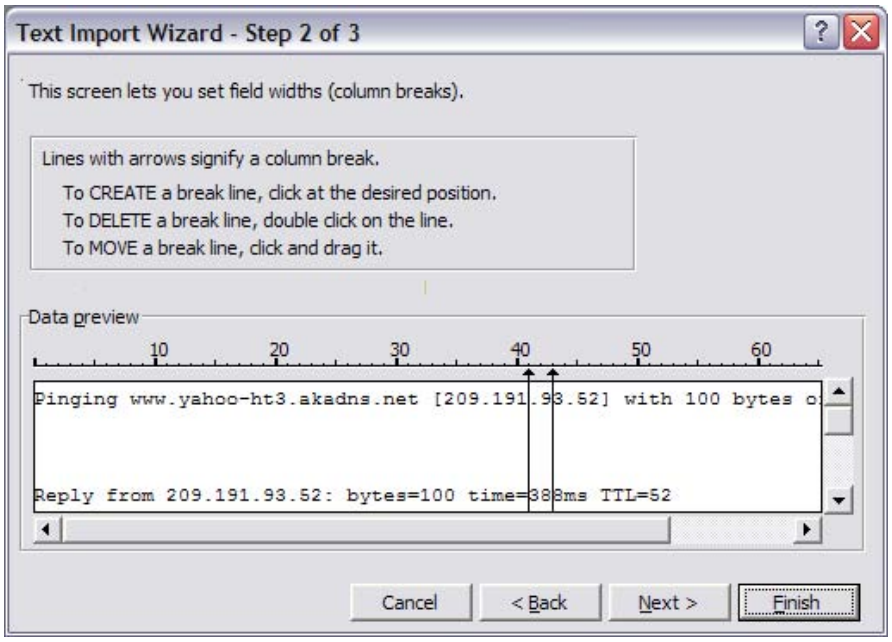
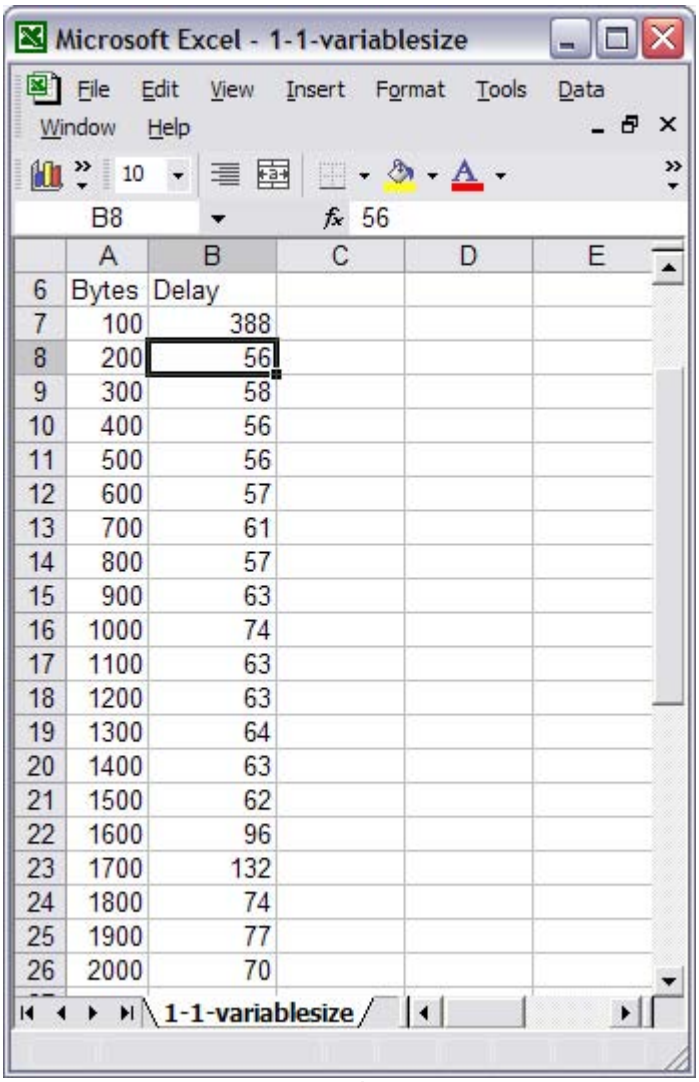


Figura 4. Asistente para importar texto de Excel.

La diferencia entre este archivo y el anterior es que el archivo de tamaño variable tiene mucha más información de la que es realmente necesaria.

Paso 3: Formatear la hoja de cálculo.

Limpie y organice los datos de la hoja de cálculo en dos columnas: Bytes y Retardo. Una vez que finalice, la hoja de cálculo debe parecerse a la Figura 5.

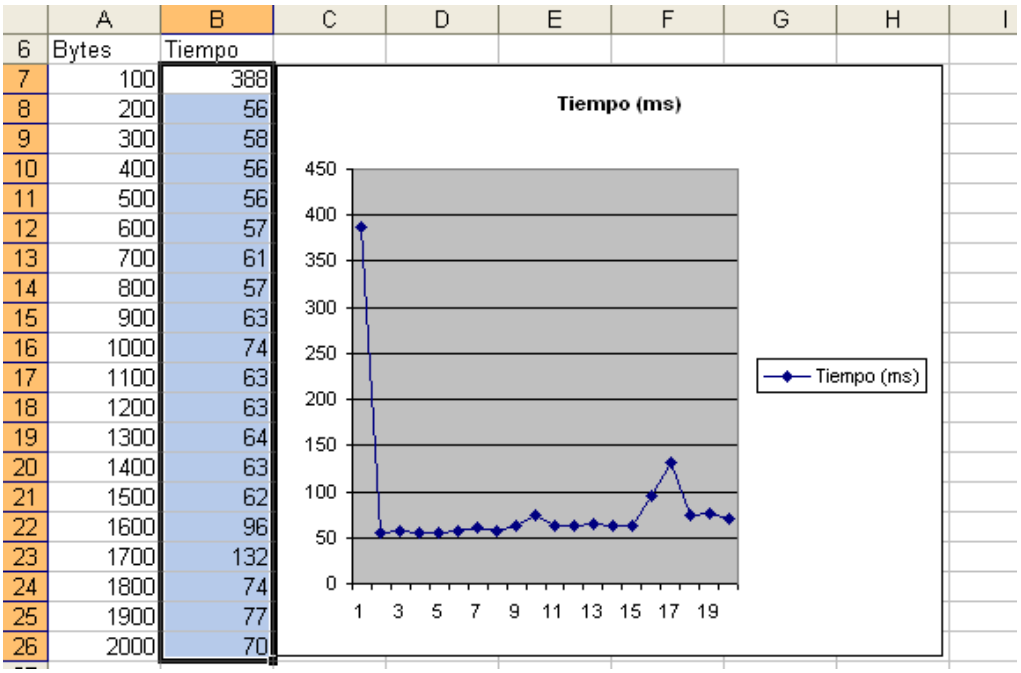


	A	B	C	D	E
6	Bytes	Delay			
7	100	388			
8	200	56			
9	300	58			
10	400	56			
11	500	56			
12	600	57			
13	700	61			
14	800	57			
15	900	63			
16	1000	74			
17	1100	63			
18	1200	63			
19	1300	64			
20	1400	63			
21	1500	62			
22	1600	96			
23	1700	132			
24	1800	74			
25	1900	77			
26	2000	70			

Figura 5. Hoja de cálculo formateada.

Paso 3: Crear un gráfico con los datos.

Resalte los datos de la columna Retardo. Seleccione las opciones del menú Insertar | Gráfico. Existen distintos gráficos que se pueden usar para presentar los datos de retardo, algunos mejores que otros. Aunque el gráfico debe ser claro, también hay lugar para la creatividad personal. El gráfico de la Figura 6 es un gráfico de Línea apilada.



	A	B
6	Bytes	Tiempo
7	100	388
8	200	56
9	300	58
10	400	56
11	500	56
12	600	57
13	700	61
14	800	57
15	900	63
16	1000	74
17	1100	63
18	1200	63
19	1300	64
20	1400	63
21	1500	62
22	1600	96
23	1700	132
24	1800	74
25	1900	77
26	2000	70

Figura 6. Esquema de comparación entre tamaño y datagrama.

Una vez que termine, guarde la hoja de cálculo y el gráfico, y entréguelo al instructor con el análisis de retardo final.

¿Se puede hacer alguna suposición en relación con el retardo cuando se envían datagramas más grandes a través de una red?

_____

_____

Tarea 4: Reflexión

El comando **ping** puede proporcionar información importante sobre la latencia de red. Un análisis detallado de retardo a través de días consecutivos durante distintos momentos del día puede alertar al ingeniero de redes sobre cambios en el rendimiento de la red. Por ejemplo, los dispositivos de red pueden saturarse durante determinados momentos del día y el retardo de red tendrá un pico. En este caso, las transferencias de datos de rutina deben programarse para las horas no pico, cuando el retardo es menor. Además, muchos usuarios se suscriben a aplicaciones punto a punto, como KaZaA y Napster. Cuando estas aplicaciones de archivos compartidos están activas, se deriva un valioso ancho de banda de importantes aplicaciones de negocios. Si los retardos son generados por eventos que se producen dentro de la organización, se pueden usar herramientas de análisis de redes para determinar el origen y para aplicar acciones correctivas. Cuando la fuente se origina en redes externas, que no tienen el control de la organización, la suscripción a través de un proveedor de servicios de Internet (ISP) diferente, o de uno adicional, puede ser una solución.

Tarea 5: Desafío

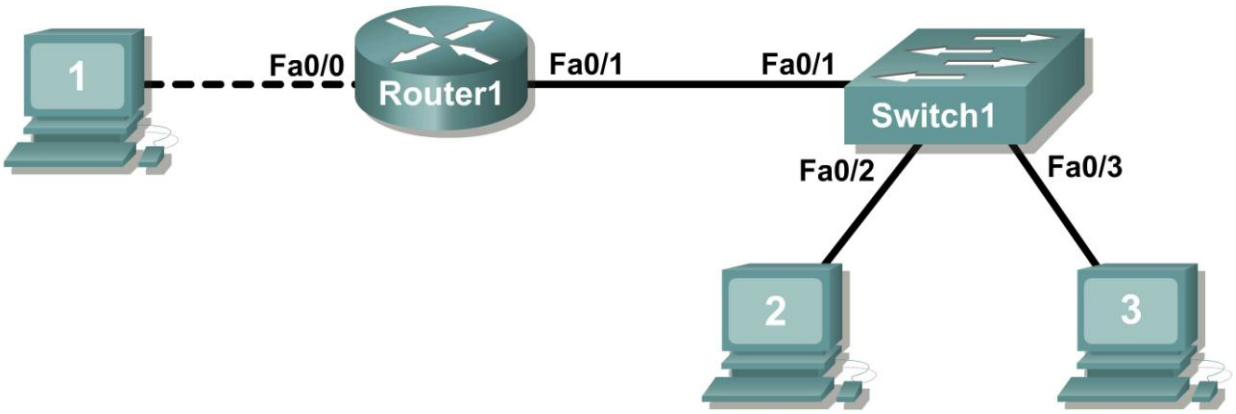
Si se puede, descargue un archivo grande y realice una prueba separada de retardo mientras se descarga el archivo. Escriba un análisis de uno o dos párrafos en el que compare estos resultados de retardo con una medición efectuada sin descarga.

Apéndice

NOMBRE: _____						**Documentación de retardo de red**
Dirección IP de origen: _____		**Dirección IP de destino:_____**			**TTL: _____**	
Análisis estadístico de latencia de red con datagramas de 32 bytes						
Día (1 – 5)	**Fecha (dd/mm/aaaa)**	**Hora (hh:mm)**	**MEDIO**	**MEDIANO**	**MODO**	**Paquetes descartados**
1						
2						
3						
4						
5						

Práctica de laboratorio 11.5.1: Configuración básica del dispositivo Cisco

Diagrama de topología



Objetivos de aprendizaje

- Establecer la configuración global del router Cisco.
- Configurar el acceso con contraseña al router Cisco.
- Configurar las interfaces del router Cisco.
- Guardar el archivo de configuración del router.
- Configurar un switch Cisco.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA.
Switch Cisco	1	Parte del equipo de laboratorio del CCNA.
*Computadora (host)	1	Computadora del laboratorio.
Cable de consola (transpuesto)	1	Conecta el equipo host 1 con el puerto de la consola del router.
Cable UTP Cat 5 de conexión cruzada	1	Conecta el equipo host 1 con la interfaz LAN del router Fa0/0
Cable de conexión directa	3	Conecta el equipo host con el switch y el switch con el router

Tabla 1. Equipo y hardware para el laboratorio.

Reúna todos los equipos y cables necesarios. Para configurar esta práctica de laboratorio, asegúrese de que los equipos enumerados en la Tabla 1 estén disponibles.

Las tareas de configuración comunes incluyen la configuración del nombre del host, las contraseñas de acceso y el banner MOTD.

La configuración de la interfaz es de suma importancia. Además de asignar una dirección IP de Capa 3, ingrese una descripción que indique el tiempo de diagnóstico de las velocidades de conexión de destino.

Los cambios de configuración se aplican de inmediato.

Los cambios se deben guardar en la NVRAM para que persistan luego de reiniciar.

Los cambios también se pueden guardar sin conexión en un archivo de texto para auditorías o reemplazo del dispositivo.

La configuración del switch Cisco IOS es similar a la del router Cisco IOS.

Escenario

En esta práctica de laboratorio, los estudiantes configurarán las preferencias comunes en un router y switch Cisco.

Dados una dirección IP de `198.133.219.0/24` y 4 bits prestados de las subredes, complete la siguiente información:

(Ayuda: complete el número de subred, luego la dirección de host. La información de dirección es fácil de calcular si el número de subred se completa primero)

Cantidad máxima de subredes: _____

Cantidad de hosts utilizables por subred: _____

	Dirección IP:		Máscara de subred:	
#	Subred	Primera dirección de host	Última dirección de host	Broadcast
0				

Antes de continuar, verifique las direcciones con el instructor. El instructor asignará subredes.

Tarea 1: Establecer la configuración global del router Cisco.

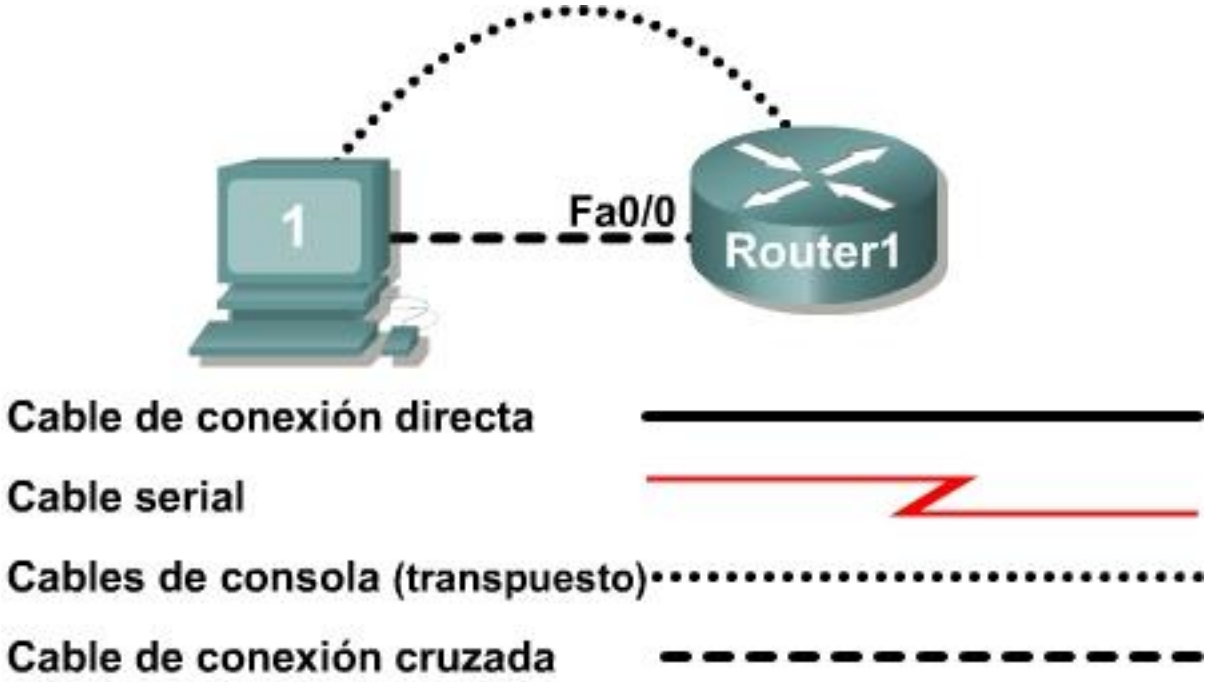


Figura 1. Cableado de la práctica de laboratorio.

Paso 1: Conecte físicamente los dispositivos.

Consulte la Figura 1. Conecte el cable de consola (transpuesto) al puerto de la consola en el router. Conecte el otro extremo del cable al equipo host con un adaptador DB-9 o DB-25 al puerto COM 1. Conecte el cable de conexión cruzada entre la tarjeta de interfaz de red (NIC) del equipo host y la interfaz Fa0/0 del Router. Conecte un cable de conexión directa entre la interfaz Fa0/1 del Router y cualquiera de las interfaces del switch (de la 1 a la 24).

Asegúrese de que se haya suministrado energía al equipo host, al switch y al router.

Paso 2: Conecte el equipo host al router mediante HyperTerminal.

Desde la barra de tareas de Windows, ejecute el programa HyperTerminal, haga clic en Inicio | Programas | Accesorios | Comunicaciones | HyperTerminal.

Configure HyperTerminal con las configuraciones adecuadas:

Descripción de la conexión

Nombre: **Práctica de laboratorio 11_2_11**

Ícono: **Elección personal**

Conectar a

Conectar mediante: **COM1** (o puerto COM adecuado)

```
Propiedades de COM1
    Bits por segundo: 9600
       Bits de datos: 8
             Paridad: None
      Bits de parada: 1
    Control de flujo: None
```

Cuando se muestre la ventana de sesión de HyperTerminal, presione la tecla **Intro** hasta recibir respuesta del router.

Si la terminal del router se encuentra en modo de configuración, salga ingresando **NO**.

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

Press RETURN to get started!
Router>
```

Cuando está en el modo exec privilegiado, el router intenta traducir todos los comandos que están mal escritos o que no se reconozcan, como nombres de dominio. Debido a que no hay un servidor de dominio configurado, hay una demora mientras la solicitud expira. Esto puede demorar algunos minutos. Para finalizar la espera, presione al mismo tiempo las teclas **<CTRL><SHIFT>6**, luego suelte y presione **x**:

```
Router>enabel
Traduciendo "enabel"...servidor de dominio (255.255.255.255) %
```

Presione brevemente las teclas **<CTRL><SHIFT>6**, suelte y presione **x**

```
Búsqueda del nombre interrumpida

Router>
```

En el modo exec de usuario, ingrese al modo exec privilegiado:

```
Router> enable
Router#
```

Verifique un archivo de configuración limpio con el comando exec privilegiado **show running-config**. Si previamente se guardó un archivo de configuración, deberá eliminarlo. En el Apéndice 1 se muestra la configuración predeterminada del router. Según cuál sea el modelo del router y la versión IOS, la configuración podría variar. Sin embargo, no debe haber contraseñas ni direcciones IP configuradas. Si el router no tiene una configuración predeterminada, solicite al instructor que elimine la configuración.

Paso 3: Establezca la configuración global del nombre de host.

¿Cuáles son los dos comandos que se pueden utilizar para salir del modo exec privilegiado? _____

¿Qué comando de atajo se puede utilizar para ingresar al modo exec privilegiado? _____

Examine los distintos modos de configuración que se pueden ingresar con el comando **configure?** Tome nota de la lista de modos de configuración y la descripción:

_____

_____

_____

_____

_____

_____

En el modo `exec privilegiado`, ingrese al modo de configuración global:

```
Router# configuration terminal
Router(config)#
```

¿Cuáles son los tres comandos que se pueden utilizar para salir del modo de configuración global y regresar al modo exec privilegiado?

_____

_____

¿Qué comando de atajo se puede emplear para ingresar al modo de configuración global? _____

Establezca el nombre de host del dispositivo en `Router1`:

```
router(config)# hostname Router1
             Router1(config)#
```

¿Cómo se puede eliminar el nombre de host?

_____

_____

Paso 4: Configure el banner MOTD.

En las redes de producción, el contenido del banner puede tener un impacto legal significativo en la organización. Por ejemplo, si el mensaje es “Bienvenido”, un juzgado puede interpretar que se ha otorgado permiso para que se acceda sin autorización al router. En un título se debe incluir información sobre la autorización, las penalidades por el acceso no autorizado, la conexión y las leyes locales aplicables. En la política de seguridad corporativa se debe incluir una cláusula sobre los mensajes del banner.

Cree un banner adecuado del MOTD. Sólo los administradores del sistema de la compañía ABC tienen acceso autorizado; se penaliza el acceso no autorizado y se registra toda la información de la conexión.

_____

_____

_____

_____

_____

_____

Examine los distintos modos de banners que se pueden ingresar. Tome nota de la lista de modos de banner y la descripción:

Router1(config)# banner ?

_____

_____

_____

_____

_____

_____

Elija un carácter de terminación que no se utilizará en el texto del mensaje. _____

Configure el banner MOTD. El banner MOTD se muestra en todas las conexiones antes del aviso de inicio de sesión. Utilice el carácter de terminación en la línea en blanco para finalizar la entrada del MOTD:

```
Router1(config)# banner motd %
Ingrese mensaje de TEXTO.  Finalice con el carácter '%'
***El usuario se encuentra conectado a un dispositivo de la red de ABC.
El acceso está autorizado sólo para los administradores del sistema de la
compañía ABC con aprobación anticipada por escrito. ***

*** El acceso no autorizado queda prohibido y será demandado. ***

*** Todas las conexiones se registran continuamente. ***

%
Router1(config)#
```

¿Cuál es el comando de configuración global que se utiliza para eliminar el banner MOTD?

_____

Tarea 2: Configurar el acceso con contraseña al router Cisco.

Las contraseñas de acceso se establecen en el modo exec privilegiado y el punto de ingreso del usuario como la consola, aux y las líneas virtuales. La contraseña del modo exec privilegiado es la más importante, debido a que controla el acceso al modo de configuración.

Paso 1: Configure la contraseña de exec privilegiado.

Cisco IOS admite dos comandos que establecen el acceso al modo exec privilegiado. Un comando, **`enable password`**, contiene criptografía débil y no debe usarse si el comando **`enable secret`** está disponible. El comando **`enable secret`** emplea un algoritmo hash de criptografía MD5. Cisco sostiene que "Hasta ahora, es imposible recuperar una contraseña secreta de enable a partir del contenido de un archivo de configuración (aparte de los obvios ataques de diccionario)". La seguridad con contraseña se basa en el algoritmo de contraseña y la contraseña. En los entornos de producción, se deben usar contraseñas fuertes en todo momento. Éstas consisten en nueve caracteres como mínimo, en minúsculas y mayúsculas, intercalados con números y símbolos. En un entorno de laboratorio, utilizaremos contraseñas débiles.

Establezca la contraseña del modo exec privilegiado en **`cisco.`**

```
Router1(config)# enable secret cisco
Router1(config)#
```

Paso 2: Configure la contraseña de consola.

Establezca la contraseña de acceso a la consola en **`class.`** La contraseña de consola controla el acceso al router.

```
Router1(config)# line console 0
Router1(config-line)# password class
Router1(config-line)# login
```

¿Cuál es el comando que se utiliza para eliminar la contraseña de consola? _____

Paso 3: Configure la contraseña de la línea virtual.

Establezca la contraseña de acceso a la línea virtual en **`class.`** La contraseña de la línea virtual controla el acceso de Telnet al router. En las primeras versiones de Cisco IOS, sólo se podían configurar cinco líneas virtuales, de la 0 a la 4. En las versiones más recientes, ha aumentado esta cantidad. A menos que haya una contraseña Telnet, el acceso a esa línea virtual está bloqueado.

```
Router1(config-line)# line vty 0 4
Router1(config-line)# password class
Router1(config-line)# login
```

Se cuenta con tres comandos que se pueden utilizar para salir del modo de configuración de la línea:

Comando	Efecto
	Vuelve al modo de configuración global.
	Sale de la configuración y regresa al modo exec privilegiado.

Emita el comando **exit**. ¿Qué indicador mostró el router? ¿Cuál es el modo?

```
Router1(config-line)# exit
```

_____

_____

Emita el comando **end**. ¿Qué indicador mostró el router? ¿Cuál es el modo?

_____

_____

Tarea 3: Configurar las interfaces del router Cisco.

Todas las interfaces cableadas deben contener documentación sobre la conexión. En las versiones más nuevas de Cisco IOS, la descripción máxima es de 240 caracteres.

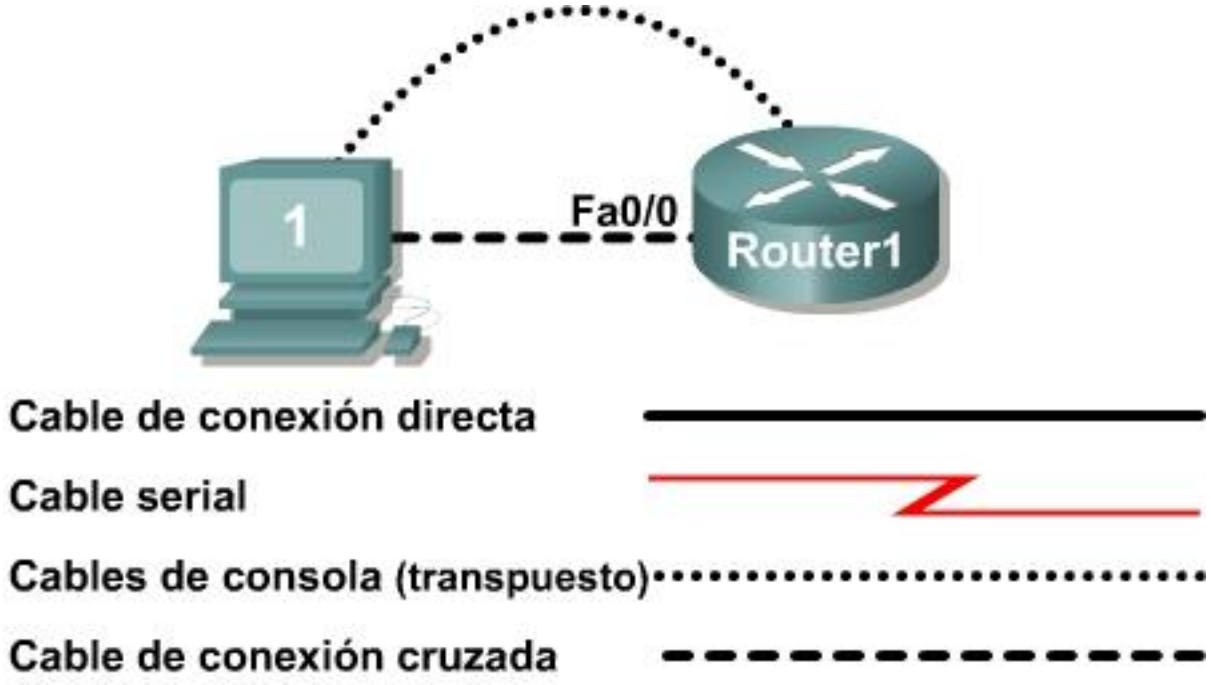


Figura 2. Topología física de la práctica de laboratorio.

En la Figura 2 se muestra una topología de red donde el equipo host está conectado al Router1, interfaz Fa0/0.

Tome nota del número de subred y la máscara: _____

La primera dirección IP se utiliza para configurar la LAN del equipo host. Tome nota de la primera dirección IP:

_____

La última dirección IP se utiliza para configurar la interfaz fa0/0 del router. Tome nota de la última dirección IP:

_____

Paso 1: Configure la interfaz fa0/0 del router.

Escriba una breve descripción de las conexiones del Router1:
Fa0/0 ->

_____

Aplique la descripción a la interfaz del router con el comando de configuración de la interfaz, **description**:

```
Router1(config)# interface fa0/0
Router1(config-if)# description Connection to Host1 with crossover cable
Router1(config-if)# ip address address mask
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Busque la interfaz para que se active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz
FastEthernet0/0, estado cambiado a "arriba"
```

Paso 2: Configure la interfaz Fa0/1 del router.

Escriba una breve descripción de las conexiones del Router1:
Fa0/1 ->

_____

Aplique la descripción a la interfaz del router con el comando de configuración de la interfaz, **description**:

```
Router1(config)# interface fa0/1
Router1(config-if)# description Connection to switch with straight-through
cable
Router1(config-if)# ip address address mask
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Busque la interfaz para que se active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz
FastEthernet0/1, estado cambiado a "arriba"
```

Paso 3: Configure el equipo host.

Configure el equipo host para que permita la conectividad LAN. Recuerde que se accede a la ventana de configuración LAN mediante el menú Inicio | Panel de control | Conexiones de red. Haga clic con el botón derecho en el ícono LAN y elija Propiedades. Resalte el campo Protocolo de Internet y seleccione Propiedades. Complete los siguientes campos:

Dirección IP: La primera dirección de host _____
Máscara de subred: La máscara de subred _____
Default Gateway: Dirección IP del router _____

Haga clic en Aceptar y luego Cerrar. Abra una ventana de la terminal y verifique las configuraciones con el comando **ipconfig**.

Paso 4: Verificar la conectividad de la red.

Utilice el comando **ping** para verificar la conectividad de la red con el router. Si las respuestas del ping no son exitosas, diagnostique la conexión:

¿Qué comando Cisco IOS se puede emplear para verificar el estado de la interfaz?

¿Qué comando de Windows se puede utilizar para verificar la configuración del equipo host?

_____

¿Cuál es el cable LAN correcto para conectar el host1 y el Router1? _____

Tarea 4: Guardar el archivo de configuración del router.

Cisco IOS se refiere al almacenamiento de la configuración RAM como configuración activa y al almacenamiento NVRAM como configuración de inicio. Para que las configuraciones se mantengan luego de reiniciar o suministrar energía, la configuración RAM se debe copiar en la RAM no volátil (NVRAM). Esto no ocurre de manera automática; se debe actualizar la NVRAM manualmente luego de los cambios realizados.

Paso 1: Compare las configuraciones RAM y NVRAM del router.

Utilice el comando **show** de Cisco IOS para ver las configuraciones RAM y NVRAM. La configuración se muestra de a una pantalla por vez. Si una línea contiene En la siguiente lista se describen las respuestas de teclas aceptables:

Tecla	Descripción
<BARRA ESPACIADORA>	Mostrar la siguiente página.
<REGRESAR>	Mostrar la siguiente línea.
Q	Salir
<CTRL> c	Salir

Tome nota de un comando de atajo posible que muestre los contenidos de NVRAM.

Muestra el contenido de la NVRAM. Si falta el resultado de la NVRAM, se debe a que no se ha guardado ninguna configuración:

```
Router1# show startup-config
 startup-config is not present
Router1#
```

Muestra el contenido de la RAM.

```
Router1#show running-config
```

Utilice el resultado para responder las siguientes preguntas:

¿Qué tamaño tiene el archivo de configuración? _____

¿Cuál es la contraseña secreta de enable? _____

¿El banner MOTD contiene la información que ingresó antes? _____

¿Las descripciones de la interfaz contienen la información que ingresó antes? _____

Tome nota de un comando de atajo posible que muestre los contenidos de la RAM._____

Paso 2: Guarde la configuración en la NVRAM

Se debe guardar la configuración en NVRAM para utilizarla la próxima vez que el router se encienda o recargue. Guarde la configuración en la NVRAM:

```
Router1# copy running-config startup-config
Destination filename [startup-config]? <INTRO>
Building configuration...
[OK]
Router1#
```

Tome nota de un comando de atajo posible que copie la configuración de RAM en NVRAM.

_____

Revise los contenidos de NVRAM y verifique que la configuración sea la misma que la configuración en la RAM.

Tarea 5: Configurar un switch Cisco.

La configuración del switch Cisco IOS (afortunadamente) es similar a la configuración del router Cisco IOS. El beneficio de aprender los comandos IOS es que son parecidos a diferentes dispositivos y versiones IOS.

Paso 1: Conecte el host con el switch.

Mueva el cable de la consola, o transpuesto, al puerto de la consola en el switch. Asegúrese de que haya suministrado energía al switch. En HyperTerminal, presione Intro hasta que el switch responda.

Paso 2: Establezca la configuración global del nombre de host.

En el Apéndice 2 se muestra la configuración predeterminada del switch. Según cuál sea el modelo del router y la versión IOS, la configuración podría variar. Sin embargo, no debe haber contraseñas configuradas. Si el router no tiene una configuración predeterminada, solicite al instructor que elimine la configuración.

En el modo exec del usuario, ingrese al modo de configuración global:

```
Switch> en
Switch# config t
Switch(config)#
```

Establezca el nombre de host del dispositivo en Switch1.

```
Switch(config)# hostname Switch1
Switch1(config)#
```

Paso 3: Configure el banner MOTD.

Cree un banner adecuado del MOTD. Sólo los administradores del sistema de la compañía ABC tienen acceso autorizado; se penaliza el acceso no autorizado y se registra toda la información de la conexión.

Configure el banner MOTD. El banner MOTD se muestra en todas las conexiones antes del aviso de inicio de sesión. Utilice el carácter de terminación en la línea en blanco para finalizar la entrada del MOTD. Si necesita asistencia, repase el paso similar de la configuración del banner MOTD del router.

```
Switch1(config)# banner motd %
```

Paso 4: Configure la contraseña de exec privilegiado.

Establezca la contraseña del modo exec privilegiado en **cisco.**

```
Switch1(config)# enable secret cisco
Switch1(config)#
```

Paso 5: Configure la contraseña de consola.

Establezca la contraseña de acceso a la consola en **class.**

```
Switch1(config)# line console 0
Switch1(config-line)# password class
Switch1(config-line)# login
```

Paso 6: Configure la contraseña de la línea virtual.

Establezca la contraseña de acceso a la línea virtual en **class.** Hay 16 líneas virtuales que se pueden configurar en un switch Cisco IOS: del 0 al 15.

```
Switch1(config-line)# line vty 0 15
Switch1(config-line)# password class
Switch1(config-line)# login
```

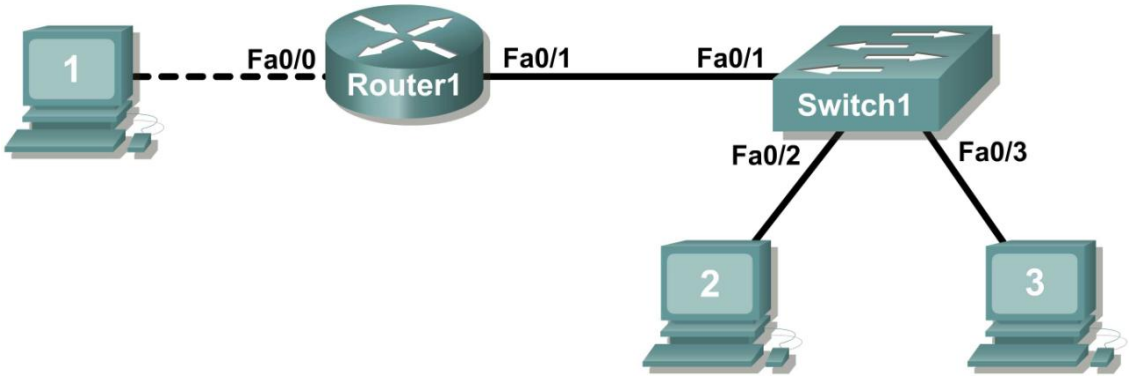


Figura 3. Topología de la red.

Paso 7: Configure la descripción de la interfaz.

En la Figura 3 se muestra la topología de la red, donde el Router1 está conectado al Switch1, interfaz Fa0/1. El Switch1 interfaz Fa0/2 está conectado al equipo host 2 y la interfaz Fa0/3 está conectada al equipo host 3.

Escriba una breve descripción de las conexiones del Switch1:

Interfaz del Router1	Descripción
Fa0/1	
Fa0/2	
Fa0/3	

Aplique las descripciones a la interfaz del switch con el comando de configuración de la interfaz, **`description`**:

```
Switch1(config)# interface fa0/1
Switch1(config-if)# description Connection to Router1
Switch1(config)# interface fa0/2
Switch1(config-if)# description Connection to host computer 2
Switch1(config)# interface fa0/3
Switch1(config-if)# description Connection to host computer 3
Switch1(config-if)# end
Switch1#
```

Paso 8: Guarde la configuración en la NVRAM

Se debe guardar la configuración en NVRAM para utilizarla la próxima vez que el switch se encienda o recargue. Guarde la configuración en la NVRAM:

```
Switch1# copy run start
Destination filename [startup-config]? <INTRO>
Building configuration...
[OK]
Switch1#
```

Revise los contenidos de NVRAM y verifique que la configuración sea la misma que la configuración en la RAM.

Tarea 6: Reflexión

Cuanto más practique los comandos, más rápido logrará configurar los router y switch Cisco IOS. Es aceptable que al principio utilice notas para auxiliarse en la configuración de un dispositivo, pero un ingeniero de redes profesional no necesita un “ayuda memoria” para realizar tareas de configuración frecuentes. En la siguiente tabla se enumeran los comandos que se abarcaron en esta práctica de laboratorio:

Propósito	Comando
Ingresar al modo de configuración global.	**`configure terminal`** Ejemplo: Router> **`enable`** Router# configure terminal Router(config)#

Propósito	Comando
Especificar el nombre del router.	**hostname** *name* Ejemplo: Router(config)# **hostname Router1** Router(config)#
Especificar una contraseña encriptada para evitar el ingreso no autorizado al modo exec privilegiado.	**enable secret** *password* Ejemplo: Router(config)# **enable secret cisco** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a la consola.	**password** *password* **login** Ejemplo: Router(config)#**line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a Telnet. Líneas vty del router: 0 4 Líneas vty del switch: 0 15	**password** *password* **login** Ejemplo: Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** router (config)#
Configure el banner MOTD.	**Banner motd %** Ejemplo: Router(config)# **banner motd %** Router(config)#
Configurar una interfaz. Router: la interfaz está APAGADA de manera predeterminada Switch: la interfaz está ENCENDIDA de manera predeterminada	Ejemplo: Router(config)# **interface fa0/0** Router(config-if)# **description** *description* Router(config-if)# **ip address** *address mask* Router(config-if)#**no shutdown** Router (config-if)#
Guardar la configuración en la NVRAM.	**copy running-config startup-config** Ejemplo: Router# **copy running-config startup-config** Router#

Tarea 7: Desafío

A menudo es necesario, y siempre útil, guardar el archivo de configuración en un archivo de texto sin conexión. Una manera de hacerlo es utilizar la opción Capturar del menú Transferir de HyperTerminal.

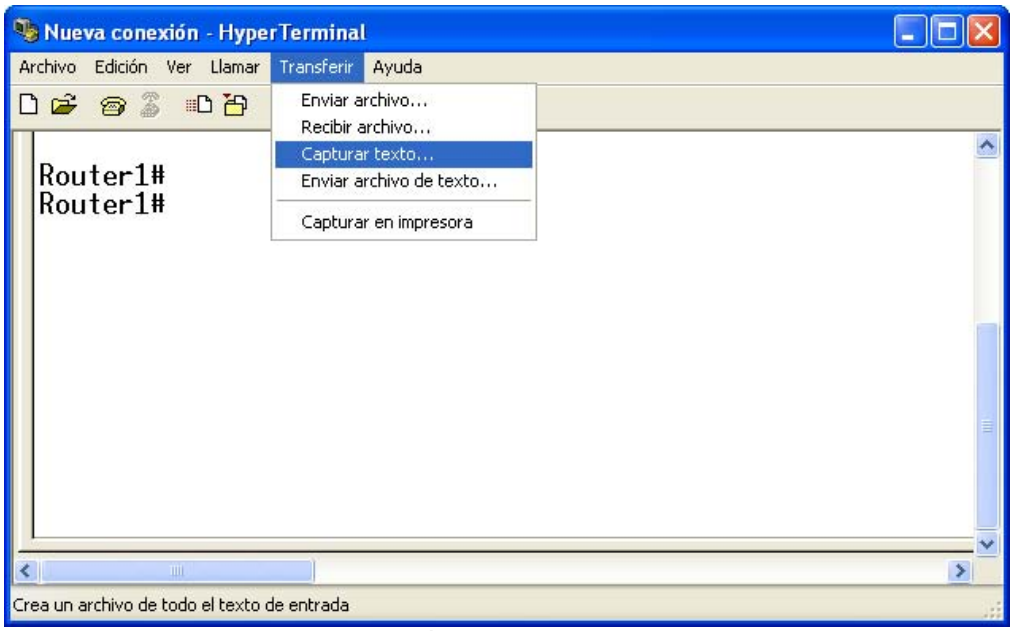


Figura 2. Menú Captura de Hyperterminal.

Consulte la Figura 2. Toda la comunicación entre el equipo host y el router se guarda en un archivo. El archivo se puede editar y guardar. También se puede modificar, copiar y pegar en el router.

Para iniciar una captura, seleccione la opción del menú de Hyperterminal: Transferir | Capturar texto. Ingrese una ruta de acceso y un nombre de archivo, luego seleccione Iniciar.

Ejecute el comando exec privilegiado **`show running-config`** y presione la tecla de la barra espaciadora hasta que se haya mostrado toda la configuración.

Detenga la captura. Seleccione la opción del menú Transferencia | Capturar texto | Detener.

Abra el archivo de texto y repase los contenidos. Elimine las líneas que no sean comandos de configuración como el mensaje more. Corrija de manera manual todas las líneas que estaban mezcladas u ocupe la misma línea. Luego de verificar el archivo de configuración, resalte las líneas y seleccione en el menú del Bloc de notas: Editar | Copiar. Esto ubica la configuración en la memoria del equipo host.

Para cargar el archivo de configuración, SIEMPRE es mejor comenzar con una configuración RAM limpia. De lo contrario, los comandos de configuración antiguos pueden permanecer tras pegarlos y tener consecuencias no intencionales (también conocidas como Ley de las consecuencias no intencionales):

Elimine el archivo de configuración NVRAM:

```
Router1# erase start
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] <ENTER>
[OK]
Erase of nvram: complete
```

Recargue el router:

```
Router1# reload
Proceed with reload? [confirm] <ENTER>
```

Una vez que se reinicie, ingrese al modo de configuración global:

```
Router> en
Router# config t
Router(config)#
```

Con el mouse, haga clic con el botón derecho en la ventana de Hyperterminal y seleccione Pegar en el host. La configuración se cargará rápidamente en el router. Analice todos los mensajes de error con detenimiento; cada uno se debe investigar y corregir.

Verifique la configuración y guarde en NVRAM.

Tarea 8: Limpieza

Antes de desconectar la energía del router y el switch, elimine el archivo de configuración de la NVRAM de cada dispositivo con el comando exec privilegiado: **erase startup-config.**

Elimine los archivos de configuración guardados en los equipos host.

A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host. Llévese todo aquello que haya traído al laboratorio y deje la aula lista para la próxima clase.

Apéndice 1: Configuración predeterminada del router Cisco IOS

```
Configuración actual: 824 bytes
!
versión 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Vlan1
 no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

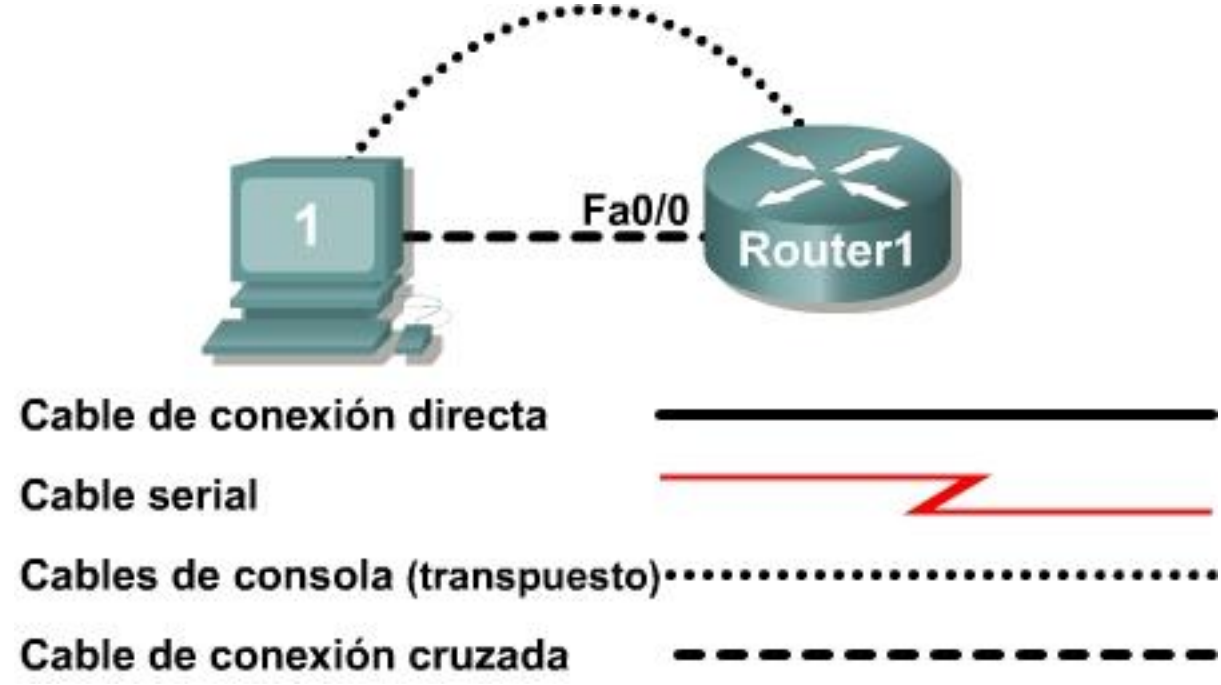
Apéndice 2: Configuración predeterminada del switch Cisco IOS

```
Configuración actual: 1519 bytes
!
versión 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 no ip address
!
interface FastEthernet0/4
 no ip address
!
interface FastEthernet0/5
 no ip address
!
interface FastEthernet0/6
 no ip address
!
interface FastEthernet0/7
 no ip address
!
interface FastEthernet0/8
 no ip address
!
interface FastEthernet0/9
 no ip address
!
interface FastEthernet0/10
 no ip address
!
interface FastEthernet0/11
 no ip address
!
```

```
interface FastEthernet0/12
 no ip address
!
interface FastEthernet0/13
 no ip address
!
interface FastEthernet0/14
 no ip address
!
interface FastEthernet0/15
 no ip address
!
interface FastEthernet0/16
 no ip address
!
interface FastEthernet0/17
no ip address
!
interface FastEthernet0/18
 no ip address
!
interface FastEthernet0/19
 no ip address
!
interface FastEthernet0/20
 no ip address
!
interface FastEthernet0/21
 no ip address
!
interface FastEthernet0/22
 no ip address
!
interface FastEthernet0/23
 no ip address
!
interface FastEthernet0/24
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
ip http server
!
!
line con 0
line vty 5 15
!
end
```

Práctica de laboratorio 11.5.2: Administración de la configuración de dispositivos

Diagrama de topología



Objetivos de aprendizaje

- Configurar la conectividad de la red.
- Utilizar TFTP para guardar y restablecer la configuración de Cisco IOS.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA.
Equipo (host)	1	Computadora del laboratorio.
Cable de consola (transpuesto)	1	Conecta el equipo host 1 con el puerto de la consola del router.
Cable de conexión cruzada	1	Conecta la tarjeta de interfaz de red (NIC) del host1 con el Router1 Fa0/1

Tabla 1. Equipo y hardware para el laboratorio.

Reúna todos los equipos y cables necesarios. Para configurar esta práctica de laboratorio, asegúrese de que los equipos enumerados en la Tabla 1 estén disponibles.

El equipo host se utiliza como servidor TFTP. En esta práctica de laboratorio se emplea el software de servidor TFTP SolarWinds. SolarWinds es una aplicación TFTP gratis para Windows.

Escenario

En esta práctica de laboratorio, los estudiantes establecerán las configuraciones del router Cisco, guardarán la configuración en un servidor TFTP y luego restablecerán la configuración desde un servidor TFTP.

Dada una dirección IP de `10.250.250.0/24` y 6 bits utilizados para las subredes. Utilice la ÚLTIMA subred. El Host1 debe utilizar la PRIMERA dirección de host válida y el Router1 debe utilizar la ÚLTIMA dirección de host válida.

Dirección IP: `10.250.250.0`		Máscara de subred:	
Subred	Primera dirección de host	Última dirección de host	Broadcast

Tarea 1: Configurar la conectividad de la red.

Paso 1: Conecte físicamente los dispositivos.

Consulte el diagrama de topología. Conecte el cable de la consola, o transpuesto, al puerto de la consola del router y el otro extremo al equipo host con un adaptador DB-9 o DB-25 en el puerto COM 1. Asegúrese de que se haya suministrado energía al equipo host y al router.

Paso 2: Conecte de manera lógica los dispositivos.

Con la información sobre la dirección IP presentada en el escenario, configure el equipo host1.

Paso 3: Conecte el equipo host al router mediante HyperTerminal.

Desde la barra de tareas de Windows, ejecute el programa HyperTerminal, haga clic en Inicio | Programas | Accesorios | Comunicaciones | HyperTerminal.

Cuando se muestre la ventana de sesión de HyperTerminal, presione la tecla **Intro** hasta recibir respuesta del router.

Paso 4: Configurar el Router1.

Configurar el Router1. Las tareas de configuración para el Router1 incluyen lo siguiente:

Tarea: Consulte el Apéndice 1 para obtener ayuda con los comandos
Especificar el nombre del router: `Router1`
Especificar una contraseña encriptada para el modo exec privilegiado: `cisco`
Especificar una contraseña de acceso a la consola: `class`
Especificar una contraseña de acceso a Telnet: `class`
Configure el banner MOTD.
Configurar la interfaz Fa0/0 del Router1: establecer la descripción establezca la dirección de la Capa 3 ejecute **`no shutdown`**

NOTA **NO GUARDE LA CONFIGURACIÓN EN NVRAM.

Paso 5: verifique la conectividad.

Verifique la conectividad entre el host1 y el Router1:

```
Router1# ping 10.250.250.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.250.250.253, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Router1#
```

Tarea 2: Utilizar el TFTP para guardar y restablecer una configuración de Cisco IOS.

Paso 1: Instale la aplicación de TFTP SolarWinds.

Haga doble clic en la aplicación de TFTP SolarWinds para comenzar la instalación. Seleccione Siguiente. Acepte el acuerdo de la licencia y las configuraciones predeterminadas. Una vez instalado SolarWinds, haga clic en Finalizar.

Paso 2: Inicie el servidor TFTP.

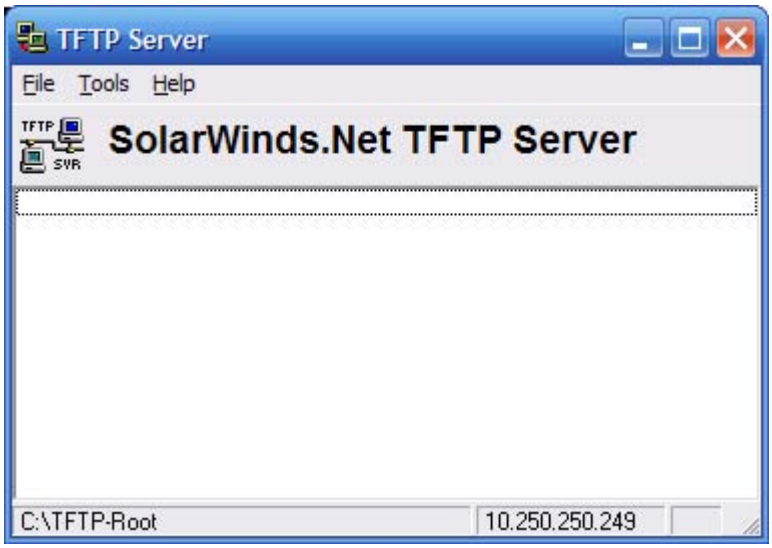


Figura 2. Ventana del servidor TFTP.

Inicie el servidor TFTP haciendo clic en Inicio | Programas | SolarWinds Free Tools | TFTP Server. En la Figura 2 se muestra una ventana activa del servidor TFTP.

Paso 3: Configure el servidor TFTP.

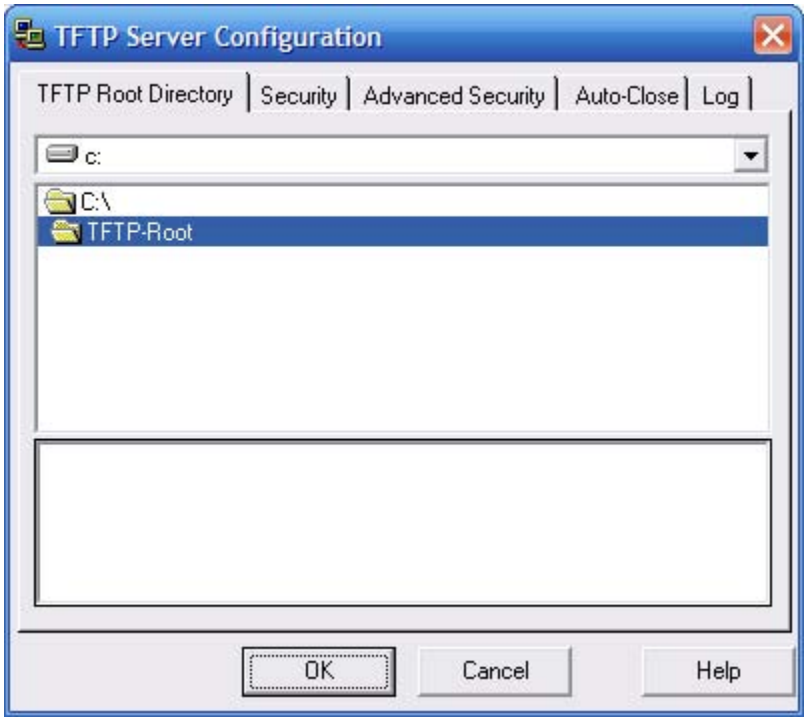


Figura 3. Ventana del servidor TFTP.

Para configurar el servidor TFTP, seleccione la opción del menú Archivo | Configurar. Consulte la Figura 3. Verifique las siguientes configuraciones:

Configuración	Valor
Directorio raíz del TFTP:	Raíz TFTP
Seguridad	Transmitir y recibir archivos
Seguridad avanzada	10.250.250.254 a 10.250.250.254
Cerrar automáticamente	Nunca
Registro	Permitir las solicitudes de registro para el siguiente archivo. Dejar el archivo predeterminado.

Cuando finalice, seleccione Aceptar.

Paso 4: Guarde la configuración del Router1 al servidor TFTP.

Desde HyperTerminal, comience a subir al servidor TFTP:

```
Router1#copy running-config tftp:
Address or name of remote host []? 10.250.250.253
Destination filename [router1-confg]? <INTRO>
!!
1081 bytes copied in 2.008 secs (538 bytes/sec)
Router1#
```

Verifique que la transferencia se haya realizado correctamente. Abra el archivo de registro: c:\Program Files\SolarWinds\Free Tools\TFTP-Server.txt. El contenido del archivo debe ser similar al siguiente:

```
3/25/2007 12:29 :Receiving router1-confg from  (10.250.250.254)
3/25/2007 12:29 :Received router1-confg from  (10.250.250.254), 1081 bytes
```

Verifique el archivo transferido. Utilice Microsoft Word o Bloc de notas para analizar el contenido del archivo c:\TFTP-Root\router1-confg. Éste debe ser similar a la siguiente configuración:

```
!
versión 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$D02B$AuX05n0HPT239yYRoQ0oE.
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 description connection to host1
 ip address 10.250.250.254 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd
*** ABC COMPANY NETWORK DEVICE ****
*** Authorized access only *****
```

```
*** Logging is enabled ****
!
line con 0
 password class
 login
line aux 0
line vty 0 4
 password class
 login
!
scheduler allocate 20000 1000
Fin
```

Paso 5: Restablezca la configuración del Router1 desde el servidor TFTP.

Verifique que la NVRAM esté despejada, luego reinicie el Router1:

```
Router1# show startup-config
 startup-config is not present
Router1# reload
Proceed with reload? [confirm] <ENTER>
```

Se debe establecer la conectividad con el servidor TFTP. El Router1 fa0/0 debe configurarse con una dirección IP y la interfaz activada:

```
Router> enable
Router# conf t
Enter configuration commands, one per line.  Finalice con CNTL/Z.
Router(config)# interface fa0/0
Router(config-if)# ip address 10.250.250.254 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit

*Mar 25 16:43:03.095: %SYS-5-CONFIG_I: Configurado desde la consola por la
consola
*Mar 25 16:43:04.967: %LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz
FastEthernet0/0, estado cambiado a "arriba"
```

Configurar el nombre de host del router para realizar una PRUEBA

```
Router(config-if)#exit
Router(config)#hostname TEST
Router(config-if)#end
TEST#
```

Verifique la conectividad con el comando ping:

```
Router# ping 10.250.250.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.250.250.253, timeout is 2 seconds:
.!!!!
Success rate is 80 percent(4/5), round-trip min/avg/max = 1/1/1ms
Router#
```

Descargue el archivo de configuración del Router1 desde el servidor TFTP:

```
Router# copy tftp startup-config
Address or name of remote host []? 10.250.250.253
Source filename []? router1-confg
Destination filename [startup-config]? <INTRO>
Accessing tftp://10.250.250.253/router1-confg...
Loading router1-confg from 10.250.250.253 (via FastEthernet0/0): !
[OK - 1081 bytes]

1081 bytes copied in 9.364 secs (115 bytes/sec)
Router1#
*Mar 25 16:55:26.375: %SYS-5-CONFIG_I: Configured from
tftp://10.250.250.253/router1-confg by console
Router1#
```

Analice la configuración que se encuentra en la NVRAM para comprobar que se haya transferido bien el archivo. La configuración debe ser igual a la indicada en la Tarea 1, Paso 4.

Vuelva a cargar el router, seleccione NO en el aviso que dice “Se ha modificado la configuración”. Debe restablecer la configuración anterior y el nombre de host del router ahora debe ser: Router1.

Tarea 3: Reflexión

El TFTP es una forma rápida y eficiente de guardar y cargar archivos de configuración de Cisco IOS.

Tarea 4: Desafío

Al igual que la acción de cargar un archivo de configuración, el IOS también se puede guardar sin conexión para utilizarlo cuando lo necesite. Para determinar el nombre de archivo del IOS, ejecute el comando Cisco IOS **show version**. Se resalta el nombre del archivo a continuación:

```
Router1# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(10b),
RELEASE SOFTWARE (fc3)
Soporte técnico: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

Tiempo de actividad de Router1 de 17 minutos
System returned to ROM by reload at 16:47:54 UTC Sun Mar 25 2007
El archivo de imagen de sistema es "flash:c1841-advipservicesk9-mz.124-
10b.bin"

Este producto contiene características criptográficas y está sujeto a las leyes
de los Estados Unidos y del país local concernientes a importación, exportación,
transferencia y uso. El envío de productos criptográficos de Cisco no brinda
autorización a terceros para importar, exportar, distribuir o utilizar tal
encriptación. Los importadores, exportadores, distribuidores y usuarios son
responsables del cumplimiento de las leyes de EE. UU. y locales. Al utilizar
este producto, acepta cumplir con las leyes y regulaciones aplicables. Si no
```

```
puede cumplir con las leyes de los EE. UU. y locales, devuelva este producto
inmediatamente.

Puede encontrarse un resumen de las leyes estadounidenses que rigen los
productos criptográficos de Cisco en:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

Para obtener asistencia adicional, contáctenos enviando un e-mail
a export@cisco.com.

Cisco 1841 (revisión 6.0) con 174080K/22528K bites de memoria.
Processor board ID FHK110918KJ
2 Serial(sync/async) interfaces
La configuración DRAM es de 64 bits con paridad desactivada.
191K bytes de NVRAM.
62720K bytes de ATA CompactFlash (Lectura/Escritura)

Configuration register is 0x2102

Router1#
```

Los comandos para cargar el IOS son parecidos a los necesarios para subir un archivo de configuración:

```
Router1# copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Address or name of remote host []? 10.250.250.253
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
22063220 bytes copied in 59.564 secs (370412 bytes/sec)
Router1#
```

Tarea 5: Limpieza

Antes de apagar el router, elimine el archivo de configuración de la NVRAM si lo había cargado. Utilice el comando de exec privilegiado **erase startup-config.**

Elimine el servidor TFTP de SolarWinds del equipo host. Seleccione Inicio | Panel de control. Abra Agregar o quitar programas. Seleccione SolarWinds, luego haga clic en Quitar. Acepte las opciones predeterminadas.

Elimine los archivos de configuración guardados en los equipos host.

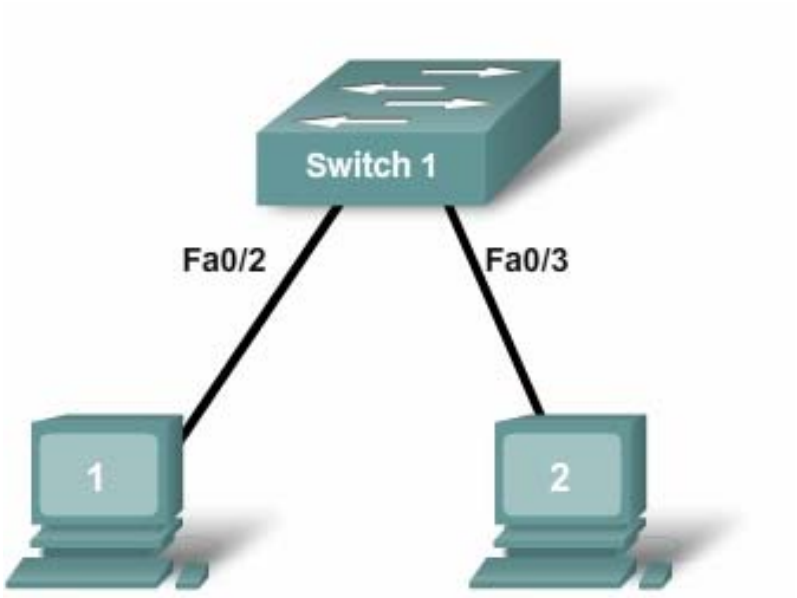
A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Apéndice 1

Propósito	Comando
Ingresar al modo de configuración global.	**configure terminal** Ejemplo: Router> **enable** Router# configure terminal Router(config)#
Especificar el nombre del router.	**hostname** *name* Ejemplo: Router(config)# **hostname Router1** Router(config)#
Especificar una contraseña encriptada para evitar el ingreso no autorizado al modo exec privilegiado.	**enable secret** *password* Ejemplo: Router(config)# **enable secret cisco** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a la consola.	**password** *password* **login** Ejemplo: Router(config)#**line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a Telnet. Líneas vty del router: 0 4 Líneas vty del switch: 0 15	**password** *password* **login** Ejemplo: Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** router (config)#
Configure el banner MOTD.	**Banner motd %** Ejemplo: Router(config)# **banner motd %** Router(config)#
Configurar una interfaz. Router: la interfaz está APAGADA de manera predeterminada Switch: la interfaz está ENCENDIDA de manera predeterminada	Ejemplo: Router(config)# **interface fa0/0** Router(config-if)# **description** *description* Router(config-if)# **ip address** *address mask* Router(config-if)#**no shutdown** Router (config-if)#
Guardar la configuración en la NVRAM.	**copy running-config startup-config** Ejemplo: Router# **copy running-config startup-config** Router#

Práctica de laboratorio 11.5.3: Configuración de equipos host para redes IP

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Diseñar la topología lógica del laboratorio.
- Configurar la topología física de laboratorio.
- Configurar la topología LAN lógica.
- Verificar la conectividad LAN.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA
Switch Cisco	1	Parte del equipo de laboratorio del CCNA
*Equipo (Host)	3	Computadora del laboratorio
Cable UTP CAT-5 o cualquier cable UTP superior de conexión directa	3	Conecta el Router1 y los equipos Host1 y Host2 con el switch 1

Tabla 1. Equipo y hardware para el laboratorio

Reúna todos los equipos y cables necesarios. Para configurar esta práctica de laboratorio, asegúrese de que los equipos enumerados en la Tabla 1 estén disponibles.

Escenario

En esta práctica de laboratorio, los estudiantes podrán crear una red pequeña que necesita dispositivos de red para conexión y equipos host de configuración para lograr una conectividad de red básica. En el Apéndice se encuentra una referencia para la configuración de la red lógica.

Tarea 1: Diseñar la topología lógica del laboratorio.

1. Dados una dirección IP de `192.168.254.0/24` y 5 bits utilizados para subredes, complete la siguiente información:

   Cantidad máxima de subredes: _____

   Cantidad de hosts utilizables por subred: _____

	Diriección IP: 192.168.254.0		**Máscara de subred:**	
#	**Subred**	**Primera dirección de host**	**Última dirección de host**	**Broadcast**
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				

2. Antes de continuar, verifique las direcciones con el instructor. El instructor asigna una subred por estudiante o equipo.

Tarea 2: Configurar la topología física del laboratorio.

Paso 1: Conecte físicamente los dispositivos.

1. Realice el cableado de los dispositivos de red como se muestra en la Figura 1.

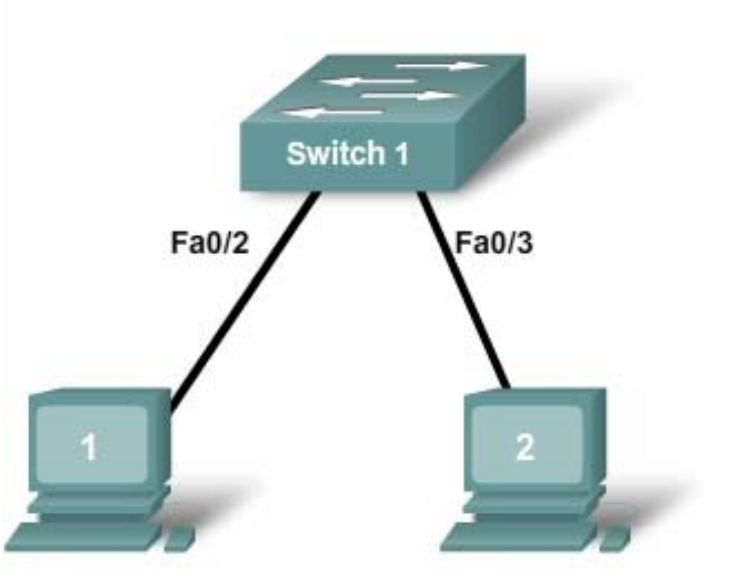


Figura 1. Cableado de la red

¿Se necesita un cable de conexión cruzada para conectar los equipos host con el switch? ¿Por qué? _____

_____

Si aún no está habilitada, suministre energía a todos los dispositivos.

Paso 2: Inspeccionar visualmente las conexiones de la red.

Después de realizar el cableado de los dispositivos de red, dedique unos minutos a verificar las conexiones. Prestar atención a los detalles ahora reducirá el tiempo necesario para diagnosticar un problema de conectividad más tarde.

Tarea 3: Configurar la topología lógica.

Paso 1: Registre la configuración lógica de la red.

1. Los equipos host utilizan las dos primeras direcciones IP de la subred. Anote la información de la dirección IP de cada dispositivo:

Dispositivo	Subred	Dirección IP	Máscara
Host1			
Host2			

Figura 2. Topología lógica

2. A partir de la información dada en la Figura 2, tome nota del direccionamiento de red IP de cada equipo:

Host 1	
Dirección IP	
Máscara IP	

Host 2	
Dirección IP	
Máscara IP	

Paso 2: Configure el equipo Host1.

1. En Equipo1, haga clic en **Inicio > Panel de control > Conexiones de red**. Haga clic con el botón derecho en el ícono LAN y elija **Propiedades**. En la ficha **General**, seleccione **Protocolo de Internet (TCP/IP)** y luego haga clic en el botón **Propiedades**.

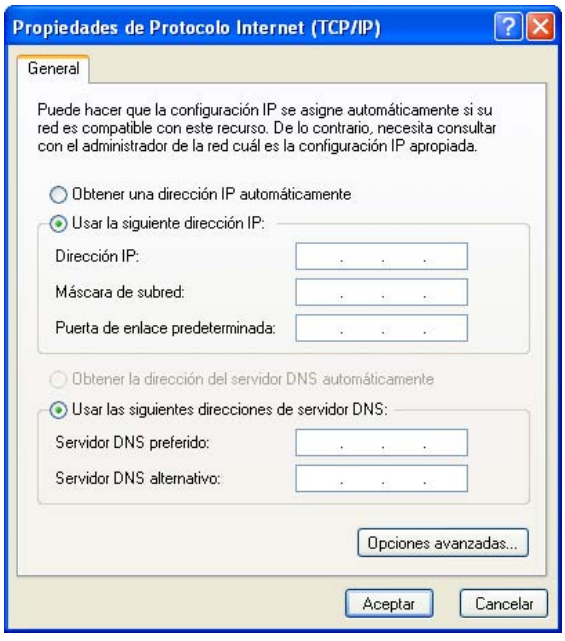


Figura 3. Configuración de dirección IP y gateway de Host1

2. Consulte la Figura 3 para determinar la configuración de dirección IP y gateway del Host1.
3. Cuando finalice, haga clic en **Aceptar** y luego en **Cerrar**. Es posible que se deba reiniciar la computadora para que los cambios tengan efecto.
4. Verifique la configuración del Host1 con el comando **`ipconfig /all`**.

5. Registre el resultado a continuación:

Configuración	Valor
Dispositivo Ethernet	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway por defecto	

Paso 3: Configure el Host2.

1. Repita el Paso 2 para el Host2, con la información de la dirección IP de la tabla completada en el Paso 1.
2. Verifique la configuración del Host1 con el comando **`ipconfig /all`**.
3. Registre el resultado a continuación:

Configuración	Valor
Dispositivo Ethernet	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway por defecto	

Tarea 4: Verificar la conectividad de la red.

Se puede verificar la conectividad de la red con el comando **`ping`** de Windows.

1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red:

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Host2		
Host2	Host1		

2. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

   Nota: Si los pings a los equipos hosts fallan, deshabilite temporalmente el firewall de la computadora y vuelva a realizar la verificación. Para deshabilitar el firewall de Windows, haga clic en **Inicio > Panel de control > Firewall de Windows**, marque **Desactivado** y luego haga clic en **Aceptar**.

Tarea 5: Reflexión

Repase los problemas de configuración física y lógica que hayan surgido durante la práctica de laboratorio. Asegúrese de que ha comprendido por completo los procedimientos utilizados para configurar un equipo host de Windows.

Tarea 6: Desafío

Solicite al instructor o a otro estudiante que presente uno o dos problemas en su red mientras usted no mira o se retira de la sala del laboratorio. Pueden ser físicos (cable UTP incorrecto), o lógicos (dirección IP incorrecta). Para solucionar los problemas:

1. Realice una buena inspección visual. Busque las luces de enlace verdes en el Switch1.
2. Utilice la tabla de la Tarea 3 para identificar la falla de conectividad. Enumere los problemas:

   _____

   _____

   _____

   _____

   _____

3. Describa las soluciones propuestas:

   _____

   _____

   _____

   _____

   _____

4. Pruebe la solución planteada. Si con esto se soluciona el problema, registre la solución. De lo contrario, continúe con la resolución del problema.

   _____

   _____

   _____

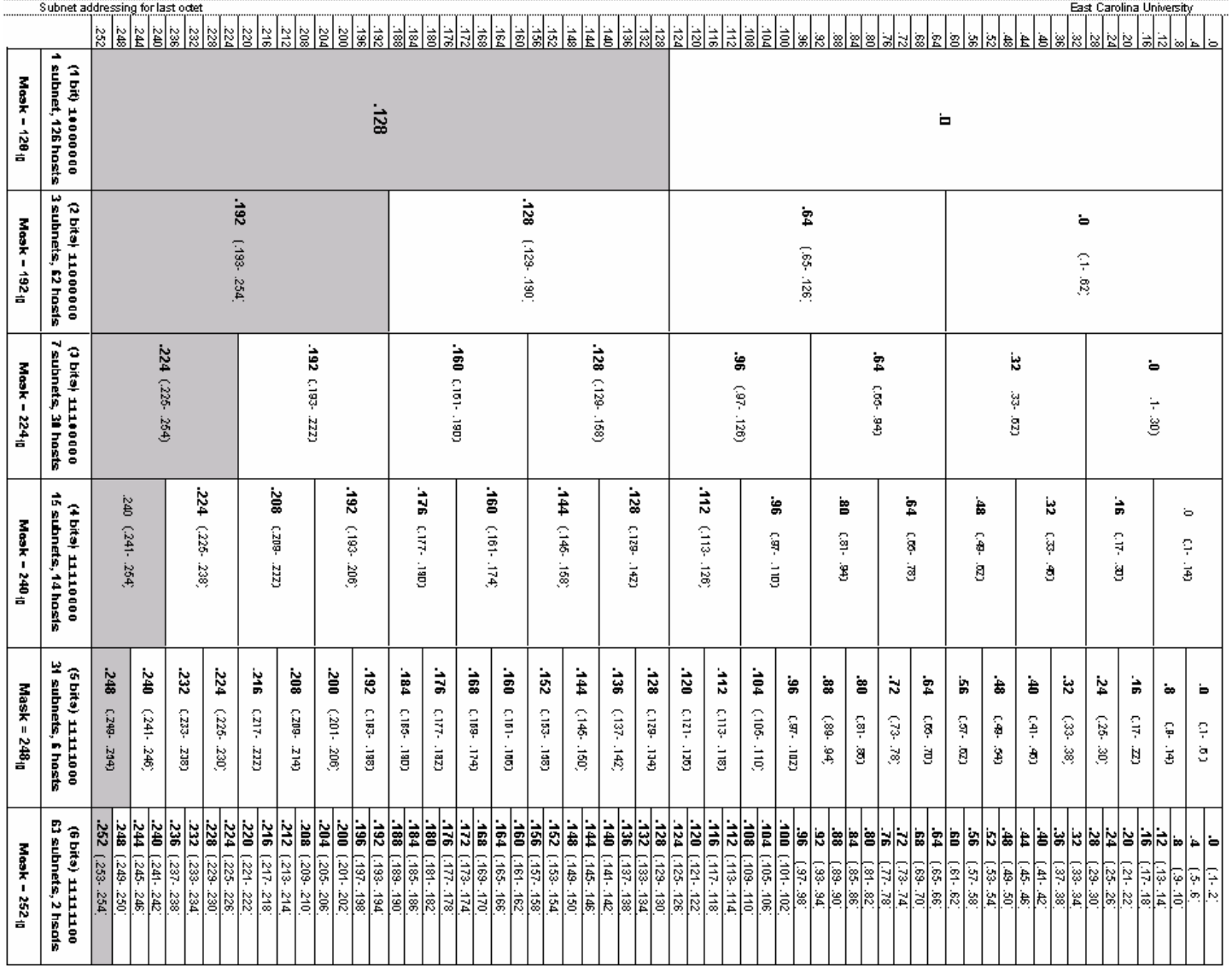
   _____

   _____

Tarea 7: Limpieza

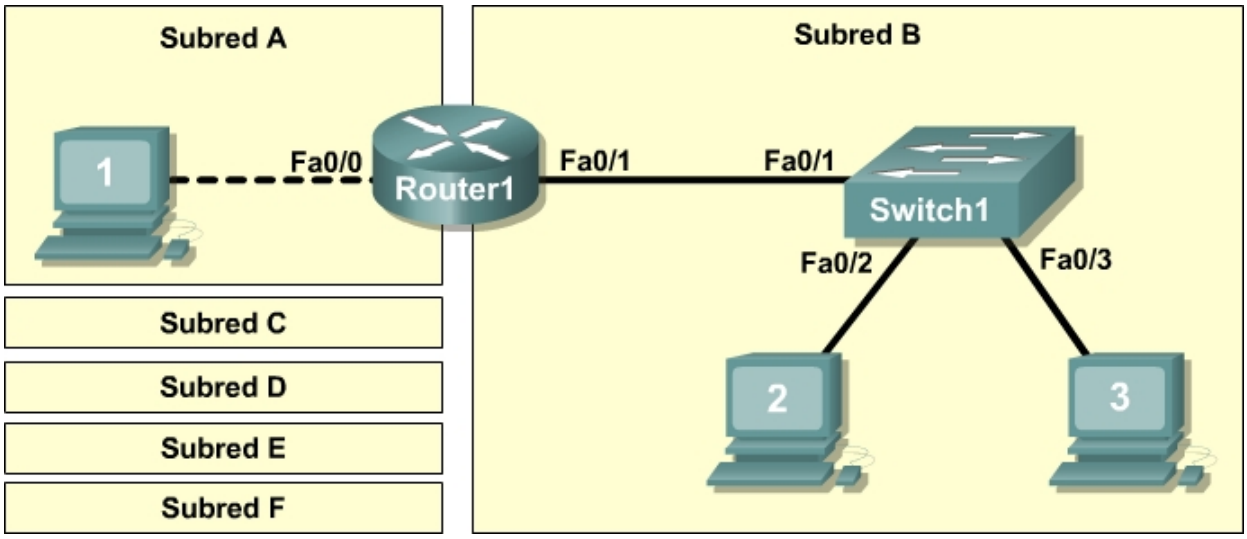
A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Apéndice



Práctica de laboratorio 11.5.4: Pruebas de red

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Diseñar la topología lógica del laboratorio.
- Configurar la topología física de laboratorio.
- Configurar la topología LAN lógica.
- Verificar la conectividad LAN.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA
Switch Cisco	1	Parte del equipo de laboratorio del CCNA
*Equipo (Host)	3	Computadora del laboratorio
Cable UTP CAT-5 o cualquier cable UTP superior de conexión directa	3	Conecta el Router1, el Host1 y el Host2 con el switch1
Cable UTP CAT -5 de conexión cruzada	1	Conecta el Host 1 con el Router1
Cable de consola (transpuesto)	1	Conecta el Host1 a la consola del Router1

Tabla 1. Equipo y hardware para el laboratorio

Reúna todos los equipos y cables necesarios. Para configurar esta práctica de laboratorio, asegúrese de que los equipos enumerados en la Tabla 1 estén disponibles.

En el Apéndice se encuentra la sintaxis de configuración de Cisco IOS para esta práctica de laboratorio.

Escenario

En esta práctica de laboratorio podrá crear una red pequeña que requiere la conexión de dispositivos de red y la configuración de equipos host para lograr una conectividad básica de red. SubredA y SubredB son subredes que se necesitan en la actualidad. SubnetC, SubnetD, SubnetE y SubnetF son subredes anticipadas, que aún no se han conectado a la red.

Tarea 1: Diseñar la topología lógica del laboratorio.

Dada una dirección IP y máscara de `172.20.0.0 / 24 (dirección / máscara)`, diseñe un esquema de direccionamiento IP que cumpla con los siguientes requisitos:

Subred	Cantidad de hosts
SubredA	Como se observa en el diagrama de topología
SubredB	Entre 80 y 100
SubredC	Entre 40 y 52
SubredD	Entre 20 y 29
SubredE	12
SubredF	5

Nota: Siempre comience con la subred con la mayor cantidad de hosts y trabaje en orden descendente. Por lo tanto, debería comenzar con la SubredB y terminar con la SubredA.

Paso 1: Diseñe un bloque de direcciones para la SubredB

Comience el diseño lógico de la red cumpliendo con el requisito de la SubredB, que requiere el bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el primer bloque de direcciones que admitirá la SubredB.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredB:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Paso 2: Diseñe un bloque de direcciones para la SubredC

Cumpla con los requisitos de la SubredC, el siguiente bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la SubredC.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredC:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Paso 3: Diseñe un bloque de direcciones para la SubredD

Cumpla con los requisitos de la SubredD, el siguiente bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la SubredD.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredD:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Paso 4: Diseñe un bloque de direcciones para la SubredE

Cumpla con los requisitos de la SubredE, el siguiente bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la SubredE.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredE:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Paso 5: Diseñe un bloque de direcciones para la SubredF

Cumpla con los requisitos de la SubredF, el siguiente bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la SubredF.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredF:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Paso 6: Diseñe un bloque de direcciones para la SubredA

Cumpla con los requisitos de la SubredA, el bloque más pequeño de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la SubredA.

1. Complete la siguiente tabla con la información sobre la dirección IP de la SubredA:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

2. ¿Cuál es la máscara de bits en números binarios? _____

Tarea 2: Configurar la topología física del laboratorio.

Paso 1: Conectar físicamente los dispositivos de la práctica de laboratorio.

1. Realice el cableado de los dispositivos de red como se observa en la Figura 1. Preste atención especialmente al cable de conexión cruzada que se necesita entre el Host1 y el Router1.

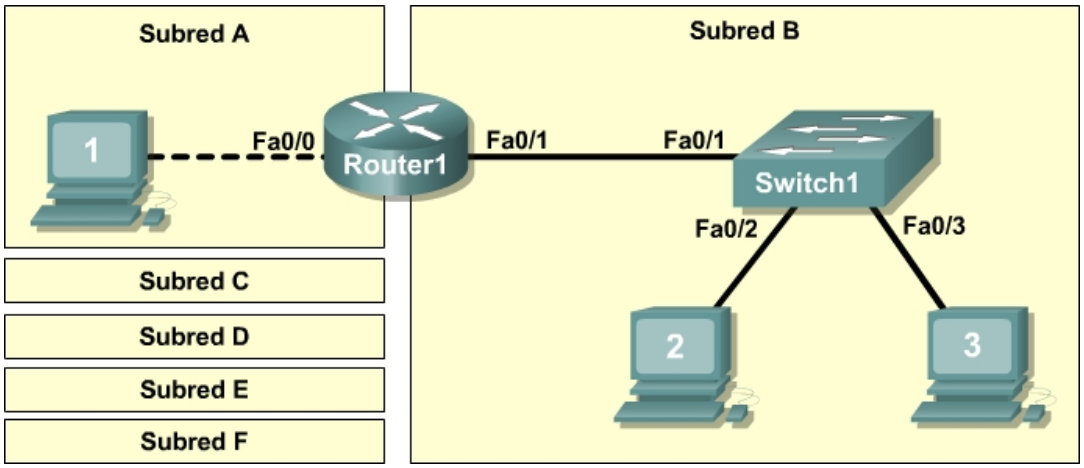


Figura 1. Cableado de la red

2. Si aún no está habilitada, suministre energía a todos los dispositivos.

Paso 2: Inspeccionar visualmente las conexiones de la red.

Después de realizar el cableado de los dispositivos de red, dedique unos minutos a verificar las conexiones. Prestar atención a los detalles ahora reducirá el tiempo necesario para diagnosticar más tarde un problema de conectividad de red de Capa 1.

Tarea 3: Configurar la topología lógica.

Paso 1: Registre la configuración lógica de la red.

En la SubredA, Host1 utilizará la primera dirección IP de la subred. Router1, interfaz Fa0/0, utilizará la última dirección host. En la SubredB, los equipos host utilizan la primera y la segunda dirección IP de la subred, respectivamente. Router1, interfaz Fa0/1, utilizará la última dirección host de red.

Para enrutar de manera adecuada las tramas de la Capa2 entre los dispositivos de la LAN, Switch1 no necesita configuración de Capa 3. La dirección IP asignada al Switch1, la interfaz VLAN 1, se emplea para establecer la conectividad de Capa 3 entre los dispositivos externos y el switch. Sin una dirección IP, los protocolos de la capa superior, como TELNET y HTTP, no funcionan. La dirección de gateway por defecto permite que el switch responda a las solicitudes del protocolo desde dispositivos de redes distantes. Por ejemplo, la dirección IP del gateway extiende la conectividad de Capa 3 más allá de la SubredB. El Switch1 utiliza la anteúltima dirección de host.

Anote la información de la dirección IP de cada dispositivo:

Dispositivo	Subred	Dirección IP	Máscara	Gateway
Host1				
Router1-Fa0/0				
Host2				
Host3				

Dispositivo	Subred	Dirección IP	Máscara	Gateway
Switch1				
Router1-Fa0/1				

Paso 2: Configurar los equipos host.

1. En cada equipo, sucesivamente, haga clic en **Inicio > Panel de control > Conexiones de red**. Haga clic con el botón derecho en el ícono LAN y elija **Propiedades**. En la ficha **General**, seleccione **Protocolo de Internet (TCP/IP)** y luego haga clic en el botón **Propiedades**.
2. Verifique que la dirección IP de la Capa 3 del Host1 se encuentre en una subred diferente que Host2 y Host3. Configure cada equipo host con la información de dirección IP registrada en el Paso 1.
3. Verifique que la configuración sea adecuada en todos los equipos host con el comando **`ipconfig`** y complete la siguiente tabla:

Dispositivo	Dirección IP	Máscara	Gateway por defecto
Host1			
Host2			
Host3			

Paso 3: Configurar el Router1.

1. Desde la barra de tareas de Windows, ejecute el programa HyperTerminal haciendo clic en **Inicio > Programas > Accesorios > Comunicaciones > HyperTerminal**. Configure HyperTerminal para acceder a Router1. Las tareas de configuración para el Router1 incluyen lo siguiente:

Tarea: **(Consulte el Apéndice para obtener ayuda con los comandos)**
Especificar el nombre del router: `Router1`
Especificar una contraseña encriptada para el modo EXEC privilegiado: `cisco`
Especificar una contraseña de acceso a la consola: `class`
Especificar una contraseña de acceso telnet: `class`
Configurar el banner MOTD
Configurar la interfaz Fa0/0 del Router1: • Establezca la descripción • Establezca la dirección de la Capa 3 • Ejecute **`no shutdown`**
Configurar la interfaz Fa0/1 del Router1: • Establezca la descripción • Establezca la dirección de la Capa 3 • Ejecute **`no shutdown`**

2. Guardar la configuración en la NVRAM.
3. Muestra el contenido de la RAM:
4. Escriba las especificaciones de la configuración a continuación:

Nombre de host: _____

Contraseña secreta de enable: _____

Contraseña de acceso a la consola: _____

Contraseña de acceso Telnet: _____

Banner MOTD: _____

5. Visualice la información sobre la configuración de la interfaz Fa0/0: **`show interface Fa0/0`**

   Estado de FastEthernet 0/0 (arriba / abajo): _____

   Protocolo de línea: _____

   Dirección MAC: _____

6. Visualice la información sobre la configuración de la interfaz Fa0/1: **`show interface Fa0/1`**

   Estado de FastEthernet 0/0 (arriba / abajo): _____

   Protocolo de línea: _____

   Dirección MAC: _____

7. Visualice la información breve de la dirección IP sobre cada interfaz: **`show ip interface brief`**

```
Interface         IP-Address     OK?     Method Status       Protocol
FastEthernet0/0
FastEthernet0/1
```

8. Tome medidas correctivas para los problemas y vuelva a probar.

Paso 4: Configure el Switch1.

1. Pase el cable de la consola del Router1 al Switch1.
2. Presione **Intro** hasta que se reciba respuesta.
3. La configuración para el Switch1 incluye las siguientes tareas:

Tarea: **(Consulte el Apéndice para obtener ayuda con los comandos)**
Especificar el nombre del Switch1
Especificar una contraseña encriptada para el modo exec privilegiado: `cisco`
Especificar una contraseña de acceso a la consola: `class`
Especificar una contraseña de acceso a Telnet: `class`
Configurar el banner MOTD
Configure la interfaz Fa0/1 del Switch1: Establezca la descripción
Configure la interfaz Fa0/2 del Switch1: Establezca la descripción
Configure la interfaz Fa0/3 del Switch1: Establezca la descripción

Tarea: (Consulte el Apéndice para obtener ayuda con los comandos)
Configure la dirección IP de la VLAN 1de administración: • Establezca la descripción • Establezca la dirección de la Capa 3 • Ejecute **`no shutdown`**
Configure la dirección IP del gateway por defecto

4. Muestra el contenido de la RAM:
5. Escriba las especificaciones de la configuración a continuación:

   Nombre de host: _____

   Contraseña secreta de enable: _____

   Contraseña de acceso a la consola: _____

   Contraseña de acceso Telnet: _____

   Banner MOTD: _____

   Interfaz VLAN 1: _____

   Dirección IP del gateway por defecto: _____
6. Visualice la información sobre la configuración de la interfaz VLAN 1: **`show interface vlan1`**

   Estado de VLAN 1 (arriba/abajo): _____

   Protocolo de línea: _____

Tarea 4: Verificar la conectividad de la red.

Paso 1: Usar el comando `ping` para verificar la conectividad de la red.

Puede verificarse la conectividad de la red mediante el comando **`ping`**. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla.

1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red:

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Host local (127.0.0.1)		
Host1	Dirección IP de la NIC		
Host1	Gateway (Router1, Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Switch1		
Host1	Host2		
Host1	Host3		
Host2	Host local (127.0.0.1)		
Host2	Dirección IP de la NIC		

Desde	Hacia	Dirección IP	Resultados de ping
Host2	Host3		
Host2	Switch1		
Host2	Gateway (Router1, Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	Host local (127.0.0.1)		
Host3	Dirección IP de la NIC		
Host3	Host2		
Host3	Switch1		
Host3	Gateway (Router1, Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

2. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

   Nota: Si los pings a los equipos hosts fallan, deshabilite temporalmente el firewall de la computadora y vuelva a realizar la verificación. Para deshabilitar el firewall de Windows, haga clic en **Inicio > Panel de control > Firewall de Windows**, marque **Desactivado** y luego haga clic en **Aceptar**.

Paso 2: Use el comando `tracert` para verificar la conectividad local.

1. Desde el Host1, ejecute el comando tracert a Host2 y Host3.
2. Registre los resultados:

   De Host1 a Host2: _____

   De Host1 a Host3: _____

Paso 3: Verificar la conectividad de la Capa 2.

1. Si aún no está conectado, pase el cable de consola del Router1 al Switch1.
2. Presione la tecla **Intro** hasta que haya respuesta desde el Switch1.
3. Emita el comando **`show mac-address-table.`** Con este comando se mostrarán las entradas estáticas (CPU) y dinámicas o aprendidas.
4. Enumere las direcciones MAC dinámicas y los puertos del switch correspondientes:

Dirección MAC	Puerto del switch

5. Verifique que se hayan obtenido tres direcciones MAC dinámicas, una para cada interfaz, desde la Fa0/1, Fa0/2 y Fa0/3.

Tarea 5: Reflexión

Repase los problemas de configuración física y lógica que hayan surgido durante la práctica de laboratorio. Asegúrese de que haya comprendido por completo los procedimientos utilizados para verificar la conectividad de la red.

Tarea 6: Desafío

Solicite al instructor o a otro estudiante que presente uno o dos problemas en su red mientras usted no mira o se retira de la sala del laboratorio. Pueden ser físicos (cable UTP incorrecto), o lógicos (dirección IP o gateway incorrectos). Para solucionar los problemas:

1. Realice una buena inspección visual. Busque las luces de enlace verdes en el Switch1.
2. Utilice la tabla de la Tarea 3 para identificar la falla de conectividad. Enumere los problemas:

   _____

   _____

   _____

   _____

   _____

3. Describa las soluciones propuestas:

   _____

   _____

   _____

   _____

   _____

4. Pruebe la solución planteada. Si con esto se soluciona el problema, registre la solución. De lo contrario, continúe con la resolución del problema.

   _____

   _____

   _____

   _____

   _____

Tarea 7: Limpieza

A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host.

Antes de desconectar la energía del router y el switch, elimine el archivo de configuración de la NVRAM de cada dispositivo con el comando exec privilegiado: **`erase startup-config.`**

Retire con cuidado los cables y guárdelos de manera ordenada. Vuelva a conectar los cables que desconectó para esta práctica de laboratorio.

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

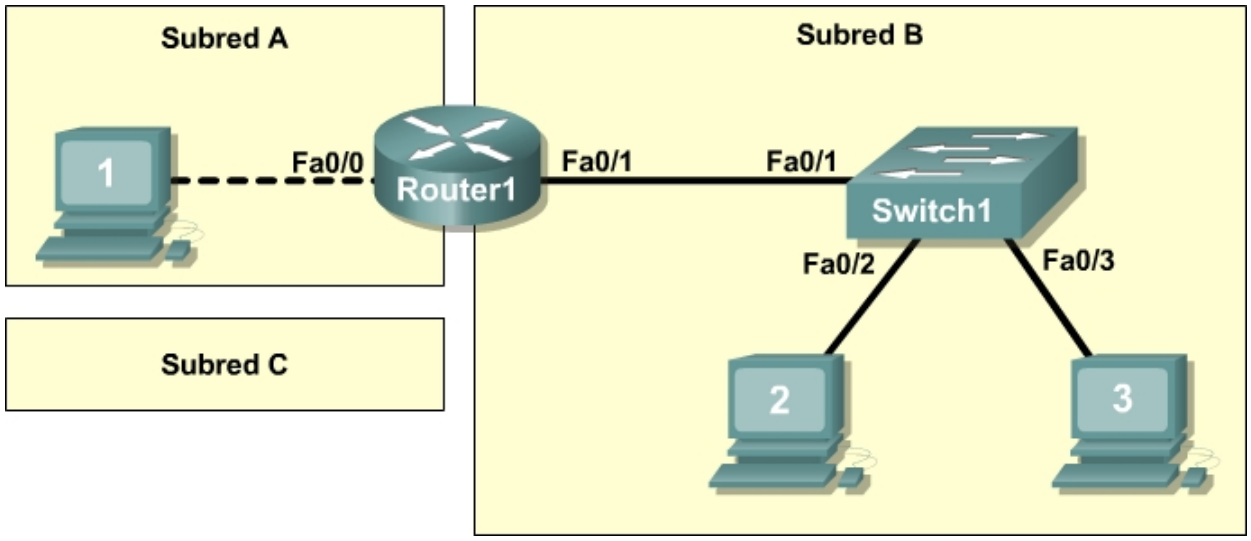
Apéndice: Lista de comandos Cisco IOS utilizados en esta práctica de laboratorio

Propósito	Comando
Ingresar al modo de configuración global.	**configure terminal** Ejemplo: Router>**enable** Router#**configure terminal** Router(config)#
Especificar el nombre del dispositivo Cisco.	**hostname** *name* Ejemplo: Router(config)# **hostname Router1** Router(config)#
Especificar una contraseña encriptada para evitar el ingreso no autorizado al modo EXEC privilegiado.	**Enable secret** *password* Ejemplo: Router(config)# **enable secret cisco** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a la consola.	**password** *password* **login** Ejemplo: Router(config)#**line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Especificar una contraseña para evitar el acceso no autorizado a Telnet. Líneas vty del router: 0 4 Líneas vty del switch: 0 15	**password** *password* **login** Ejemplo: Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** router (config)#
Configure el banner MOTD.	**Banner motd %** Ejemplo: Router(config)# **banner motd %** Router(config)#
Configure una interfaz de router. La interfaz de router está APAGADA de manera predeterminada	Ejemplo: Router(config)#**interface Fa0/0** Router(config-if)#**description** *description* Router(config-if)# **ip address** *address mask* Router(config-if)#**no shutdown** Router (config-if)#
La interfaz del switch está ACTIVADA de manera predeterminada (interfaz VLAN DESACTIVADA de manera predeterminada)	Ejemplo: Switch(config)#**interface Fa0/0** Switch(config-if)#**description** *description* Switch(config)#**interface vlan1** Switch(config-if)#**ip address** *address mask* Switch(config-if)#**no shutdown** Switch(config-if)#

Propósito	Comando
Switch: crea un gateway IP por defecto	`Switch(config)#ip default-gateway address`
Guardar la configuración en la NVRAM.	**copy running-config startup-config** Ejemplo: `Router#copy running-config startup-config`

Práctica de laboratorio 11.5.5: Documentación de la red con comandos de utilidades

Diagrama de topología



Objetivos de aprendizaje

- Diseñar la topología lógica del laboratorio.
- Configurar la topología física de laboratorio.
- Designar y configurar la topología LAN lógica.
- Verificar la conectividad LAN.
- Documentar la red.

Información básica

Hardware	Cantidad	Descripción
Router Cisco	1	Parte del equipo de laboratorio del CCNA.
Switch Cisco	1	Parte del equipo de laboratorio del CCNA.
*Computadora (host)	3	Computadora del laboratorio.
Cable UTP CAT-5 o cualquier cable UTP superior de conexión directa	3	Conecta el Router1, el Host1 y el Host2 al Switch1.
Cable UTP CAT -5 de conexión cruzada	1	Conecta el Host1 al Router1
Cable de consola (transpuesto)	1	Conecta el Host1 a la consola del Router1

Tabla 1. Equipos y hardware para prácticas de laboratorio de Eagle 1.

Reúna todos los equipos y cables necesarios. Para configurar esta práctica de laboratorio, asegúrese de que los equipos enumerados en la Tabla 1 estén disponibles.

En esta práctica de laboratorio, se copiará en un Bloc de notas el resultado del router y el host desde los dispositivos para utilizarlo en la documentación de la red. En el Apéndice 1 se encuentran las tablas que puede utilizar para copiar el resultado o diseñar sus propias tablas.

Escenario

La documentación de la red es una herramienta muy importante para la organización. Los ingenieros de red, al contar con una buena documentación de la red, pueden ahorrarse tiempo en el diagnóstico de problemas y en la planificación del crecimiento de la red.

En esta práctica de laboratorio, los estudiantes podrán crear una red pequeña que necesita dispositivos de red para conexión y equipos host de configuración para lograr una conectividad de red básica. La Subred A y la Subred B son subredes que actualmente se necesitan. La SubredC es una subred anticipada, que aún no se ha conectado a la red.

Tarea 1: Configurar la topología lógica de la práctica de laboratorio.

Dada una dirección de IP y una máscara de 209.165.200.224 / 27 (dirección / máscara), diseñe un esquema de direccionamiento IP que cumpla con los siguientes requisitos:

Subred	Cantidad de hosts
Subred A	2
Subred B	Entre 2 y 6
Subred C	Entre 10 y 12

Paso 1: Diseñe un bloque de direcciones para la Subred C

Comience el diseño lógico de la red cumpliendo con el requisito de la Subred C, el bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la Subred C.

Complete la siguiente tabla con la información sobre la dirección IP de la Subred C:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits en números binarios? _____

Paso 2: Diseñe un bloque de direcciones para la Subred B

Cumpla con los requisitos de la Subred B, el siguiente bloque más grande de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el primer bloque de direcciones que admitirá la Subred B.

Complete la siguiente tabla con la información sobre la dirección IP de la Subred B:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits en números binarios? _____

Paso 3: Diseñe un bloque de direcciones para la Subred A

Cumpla con los requisitos de la Subred A, el bloque más pequeño de direcciones IP. Usando números binarios para crear la tabla de la subred, elija el siguiente bloque de direcciones disponible que admitirá la Subred A.

Complete la siguiente tabla con la información sobre la dirección IP de la Subred A:

Dirección de red	Máscara	Primera dirección de host	Última dirección de host	Broadcast

¿Cuál es la máscara de bits en números binarios? _____

Tarea 2: Configurar la topología física del laboratorio.

Paso 1: Conectar físicamente los dispositivos de la práctica de laboratorio.

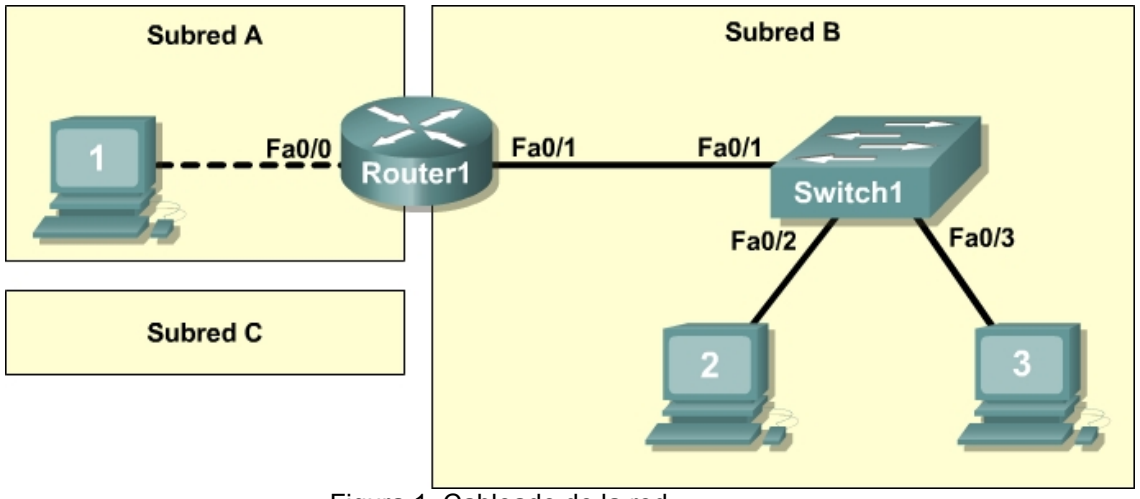


Figura 1. Cableado de la red.

Realice el cableado de los dispositivos de red como se observa en la Figura 1. Preste atención especialmente al cable de conexión cruzada que se necesita entre el Host1 y el Router1.

Si aún no está habilitada, suministre energía a todos los dispositivos.

Paso 2: Inspeccionar visualmente las conexiones de la red.

Después de realizar el cableado de los dispositivos de red, dedique unos minutos a verificar las conexiones. Prestar atención a los detalles ahora reducirá el tiempo necesario para diagnosticar un problema de conectividad más tarde.

Tarea 3: Configurar la topología lógica.

Paso 1: Registre la configuración lógica de la red.

Los equipos host utilizan las dos primeras direcciones IP de la subred. El router de la red utilizará la ÚLTIMA dirección host de red. Anote la información de la dirección IP de cada dispositivo:

Dispositivo	Subred	Dirección IP	Máscara	Gateway
Router1-Fa0/0				
Host1				
Router1-Fa0/1				
Host2				
Host3				
Switch1	No aplicable	No aplicable	No aplicable	No aplicable

Paso 2: Configurar los equipos host.

En cada equipo, sucesivamente, haga clic en Inicio | Panel de control | Conexiones de red. Identifique el ícono del dispositivo de Conexión de área local. Utilice el puntero del mouse para resaltar el ícono, haga clic con el botón derecho y seleccione Propiedades. Resalte Protocolo de Internet (TCP/IP) y seleccione Propiedades.

Verifique que la dirección IP de la Capa 3 del Host1 se encuentre en una subred diferente que Host2 y Host3. Configure cada equipo host con la información de dirección IP registrada en el Paso 1.

Verifique la configuración correcta de cada equipo host con el comando **`ipconfig /all`**. Registre la información en el Apéndice 1: Documentación de la red:

Paso 3: Configurar el Router1.

Desde la barra de tareas de Windows, ejecute el programa HyperTerminal, haga clic en Inicio | Programas | Accesorios | Comunicaciones | HyperTerminal. Configure HyperTerminal para acceder a Router1. Las tareas de configuración para el Router1 incluyen lo siguiente:

Tarea
Especificar el nombre del router: Router1
Especificar una contraseña encriptada para el modo exec privilegiado: `cisco`
Especificar una contraseña de acceso a la consola: `class`
Especificar una contraseña de acceso a Telnet: `class`
Configure el banner MOTD.
Configurar la interfaz Fa0/0 del Router1: establecer la descripción establezca la dirección de la Capa 3 ejecute **`no shutdown`**
Configurar la interfaz Fa0/1 del Router1: establecer la descripción establezca la dirección de la Capa 3 ejecute **`no shutdown`**

Guardar la configuración en la NVRAM.

Muestra el contenido de la RAM:

Copie el resultado de la configuración en la tabla de configuración del Router1, que se encuentra en el Apéndice 1.

Copie el resultado de los comandos show interface fa0/0 y show interface fa0/1 en las tablas de configuración de interfaz del Router1 que se encuentran en el Apéndice 1.

Copie el resultado del comando show ip interface brief en la tabla de configuración de la dirección IP del Router1 en el Apéndice 1.

Paso 4: Configure el Switch1.

Pase el cable de la consola del Router1 al Switch1. Presione Intro hasta que se reciba respuesta. La configuración para el Switch1 incluye las siguientes tareas:

Tarea
Especificar el nombre del `Switch1`
Especificar una contraseña encriptada para el modo exec privilegiado: `cisco`
Especificar una contraseña de acceso a la consola: `class`
Especificar una contraseña de acceso a Telnet: `class`
Configure el banner MOTD.
Configurar la interfaz Fa0/1 del Switch1: establecer la descripción
Configurar la interfaz Fa0/2 del Switch1: establecer la descripción
Configurar la interfaz Fa0/3 del Switch1: establecer la descripción

Muestra el contenido de la RAM:

Copie el resultado de la configuración en la tabla de configuración del Switch1, que se encuentra en el Apéndice 1.

Copie el resultado del comando **`show mac address-table`** en la tabla de dirección MAC del Switch1, que se encuentra en el Apéndice 1.

Tarea 4: Verificar la conectividad de la red.

Paso 1: Usar el comando ping para verificar la conectividad de la red.

Puede verificarse la conectividad de la red mediante el comando **`ping`**. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla.

**NOTA: Si los pings a los equipos hosts fallan, deshabilite temporalmente el firewall de la computadora y vuelva a realizar la verificación. Para deshabilitar el firewall de Windows, seleccione Inicio | Panel de control | Firewall de Windows, seleccione Desactivado y luego Aceptar.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Host local (127.0.0.1)		
Host1	Dirección IP de la NIC		
Host1	Gateway (Router1, Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Host2		
Host1	Host3		
Host2	Host local (127.0.0.1)		
Host2	Dirección IP de la NIC		
Host2	Host3		
Host2	Gateway (Router1, Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	Host local (127.0.0.1)		
Host3	Dirección IP de la NIC		
Host3	Host2		
Host3	Gateway (Router1, Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

Paso 2: Use el comando tracert para verificar la conectividad local.

Además de verificar la conectividad, el comando tracert se puede utilizar para probar el rendimiento básico de la línea de base de red. Es decir, con tráfico mínimo, los resultados de tracert se pueden comparar con los períodos de mucho tráfico. Los resultados sirven para justificar las actualizaciones de los equipos o las nuevas compras.

Desde el Host1, ejecute el comando tracert para el Router1, el Host2 y el Host3. Registre los resultados en la parte de resultados de Tracert del Host1, que se encuentra en el Apéndice A.

Desde el Host2, ejecute el comando tracert para el Host3, el Router1 y el Host1. Registre los resultados en la parte de resultados de Tracert del Host2, que se encuentra en el Apéndice A.

Desde el Host3, ejecute el comando tracert para el Host2, el Router1 y el Host1. Registre los resultados en la parte de resultados de Tracert del Host3 que se encuentra en el Apéndice A.

Tarea 5: Documentar la red.

Con todo el trabajo realizado hasta ahora, parecería que no queda mucho más por hacer. Se configuró la red de manera física y lógica, se verificó y se copió el resultado del comando en las tablas.

El último paso en la documentación de la red es organizar el resultado. Mientras lo haga, piense en lo que podría llegar a necesitar dentro de seis meses o un año. Por ejemplo:

¿Cuándo se creó la red?
¿Cuándo se documentó la red?
¿Hubo desafíos significativos que tuvo que superar?
¿Quién realizó la configuración (vale la pena conocer ese talento)?
¿Quién realizó la documentación (vale la pena conocer ese talento)?

Debe responder a estas preguntas en la documentación. Si lo desea, redáctelo a modo de carta de presentación.

No se olvide de incluir la siguiente información:
Una copia de la topología física.
Una copia de la topología lógica.

Prepare la documentación en un formato profesional y entréguela al instructor.

Tarea 6: Reflexión

Repase los problemas de configuración física y lógica que hayan surgido durante la práctica de laboratorio. Asegúrese de que comprende por completo los procedimientos utilizados para verificar la conectividad de la red.

Tarea 7: Desafío

Solicite al instructor o a otro estudiante que presente uno o dos problemas en su red mientras usted no mira o se retira de la sala del laboratorio. Pueden ser físicos (cables que se cambiaron de lugar en el switch) o lógicos (dirección IP o gateway incorrectos).

Utilice la documentación de la red para diagnosticar y solucionar los problemas:

1. Realice una buena inspección visual. Busque las luces de enlace verdes en el Switch1.

2. Utilice la documentación de la red para comparar cómo debería estar la red y cómo lo está en realidad:
   _____
   _____
   _____
   _____
   _____

3. Describa las soluciones propuestas:
   _____
   _____
   _____
   _____
   _____

4. Pruebe la solución planteada. Si con esto se soluciona el problema, registre la solución. De lo contrario, continúe con la resolución del problema.

_____
_____
_____
_____
_____
_____

Tarea 8: Limpieza.

A menos que el instructor le indique lo contrario, restaure la conectividad de red del equipo host y luego desconecte la alimentación de los equipos host.

Antes de desconectar la energía del router y el switch, elimine el archivo de configuración de la NVRAM de cada dispositivo con el comando exec privilegiado: **`erase startup-config`**.

Retire con cuidado los cables y guárdelos de manera ordenada. Vuelva a conectar los cables que desconectó para esta práctica de laboratorio.

Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

Apéndice 1: Documentación de la red

Tablas del host confeccionadas para la Tarea 3, Paso 2:

Configuración de red del Host1	
Nombre de Host	
Enrutamiento IP habilitado	
Adaptador Ethernet	
Descripción	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway por defecto	

Configuración de red del Host2	
Nombre de Host	
Enrutamiento IP habilitado	
Adaptador Ethernet	
Descripción	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway por defecto	

Configuración de red del Host3	
Nombre de Host	
Enrutamiento IP habilitado	
Adaptador Ethernet	
Descripción	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway por defecto	

Configuración del Router1 de la Tarea 3, Paso 3:

Configuración del Router1

Configuración de la interfaz Fa0/0 del Router1 de la Tarea 2, Paso 3:

Configuración de la interfaz fa0/1 del Router1 de la Tarea 3, Paso 3:

Configuración de la dirección IP del Router1 de la Tarea 3, Paso 3:

Configuración del Switch1 de la Tarea 3, Paso 4:

Configuración de la tabla de dirección MAC del Switch1 de la Tarea 3, Paso 4:

Resultados de traceroute del Host1 obtenidos en la Tarea 4, Paso 2:

Resultados de traceroute del Host2 obtenidos en la Tarea 4, Paso 2:

Resultados de traceroute del Host3 obtenidos en la Tarea 4, Paso 2:

Práctica de laboratorio 11.5.6: Estudio de caso final: Análisis de datagrama con Wireshark

Objetivos de aprendizaje

Al completar este ejercicio, los estudiantes podrán demostrar lo siguiente:

- cómo se construye un segmento TCP y explicar los campos del segmento;
- cómo se construye un paquete IP y explicar los campos del paquete;
- cómo se construye una trama de Ethernet II y explicar los campos de la trama;
- los contenidos de una SOLICITUD DE ARP y de una RESPUESTA DE ARP.

Información básica

Esta práctica de laboratorio requiere dos archivos de paquetes capturados y Wireshark, un analizador de protocolos de red. Descargar los siguientes archivos de Eagle server e instalar Wireshark en su computadora si es que aún no se ha instalado:

- eagle1_web_client.pcap (ya mencionado)
- eagle1_web_server.pcap (sólo referencia)
- wireshark.exe

Escenario

Este ejercicio detalla la secuencia de datagramas que se crean y envían a través de una red entre un cliente Web, PC_Client, y un servidor Web, eagle1.example.com. Comprender el proceso que se utiliza para ubicar los paquetes en secuencia en la red permitirá al estudiante diagnosticar las fallas de red de manera lógica cuando se interrumpe la conectividad. Para una mayor rapidez y claridad, se ha omitido de las capturas el sonido de los paquetes de la red. Antes de ejecutar un analizador de protocolos de red en una red que no le pertenece, debe asegurarse de obtener el permiso (por escrito).

La Figura 1 muestra la topología de esta práctica de laboratorio.

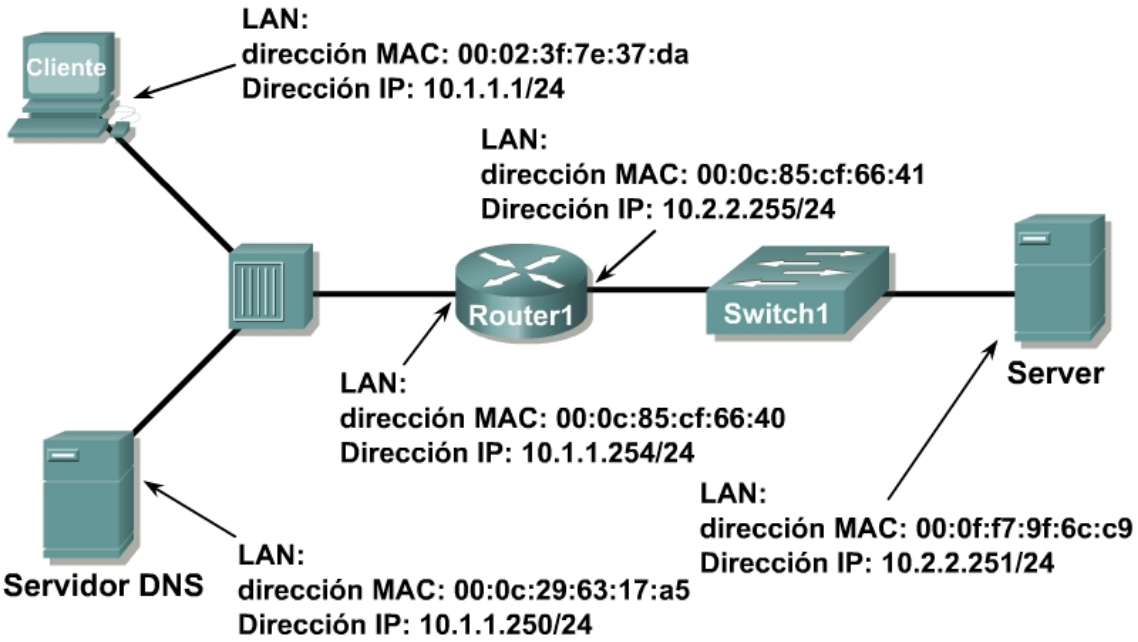


Figura 1. Topología de la red.

A través de las herramientas de la línea de comandos de Microsoft ®, se muestra la información de configuración IP y el contenido de la caché ARP. Consulte la Figura 2.

```
C: > ipconfig / all
Configuración IP de Windows
Conexión de área local del adaptador Ethernet:
     Sufijo de conexión específica DNS. :
     Descripción. . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                          Conexión de red
     Dirección física . . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp habilitado. . . . . . . . . . : No
     Dirección IP . . . . . . . . . . . : 10.1.1.1
     Máscara de subred. . . . . . . . . : 255.255.255.0
     Gateway por defecto. . . . . . . . : 10.1.1.254
     Servidores DNS . . . . . . . . . . : 10.1.1.250
C: > arp -a
No se encontraron entradas de ARP
C: >
```

Figura 2. Estado de red inicial de PC Client.

Se inicia un cliente Web y se ingresa el URL eagle1.example.com, como se observa en la Figura 3. Aquí comienza el proceso de comunicación con el servidor Web, que es donde comienzan los paquetes capturados.

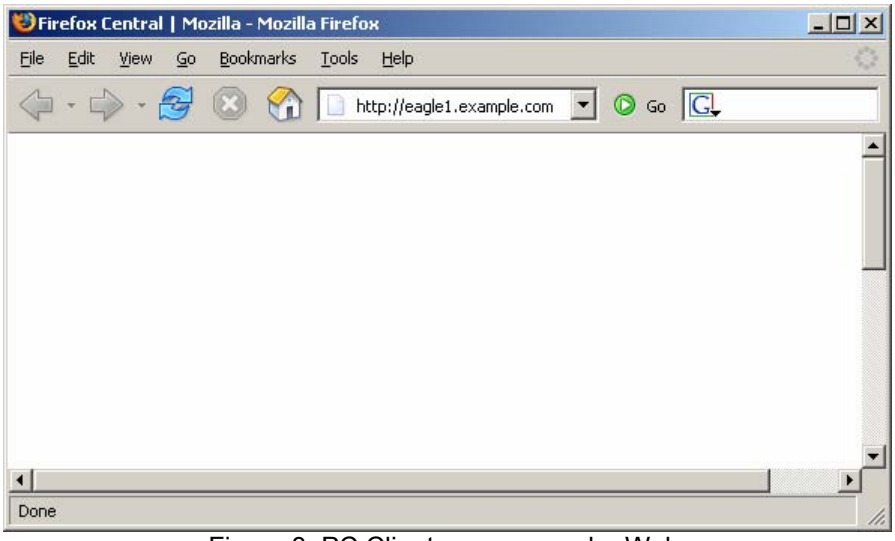


Figura 3. PC Client con navegador Web.

Tarea 1: Preparar el laboratorio.

Paso 1: Inicie Wireshark en el equipo.

Consulte la Figura 4 para realizar cambios en los resultados predeterminados. Desmarque `Barra de herramientas principal`, `Barra de herramientas de filtro` y `Bytes del paquete`. Verifique que `Lista de paquetes` y `Detalles del paquete` estén marcados. Para asegurarse de que no haya traducción automática de las direcciones MAC, desmarque `Resolución de nombres` para `Capa de MAC` y `Capa de Transporte`.

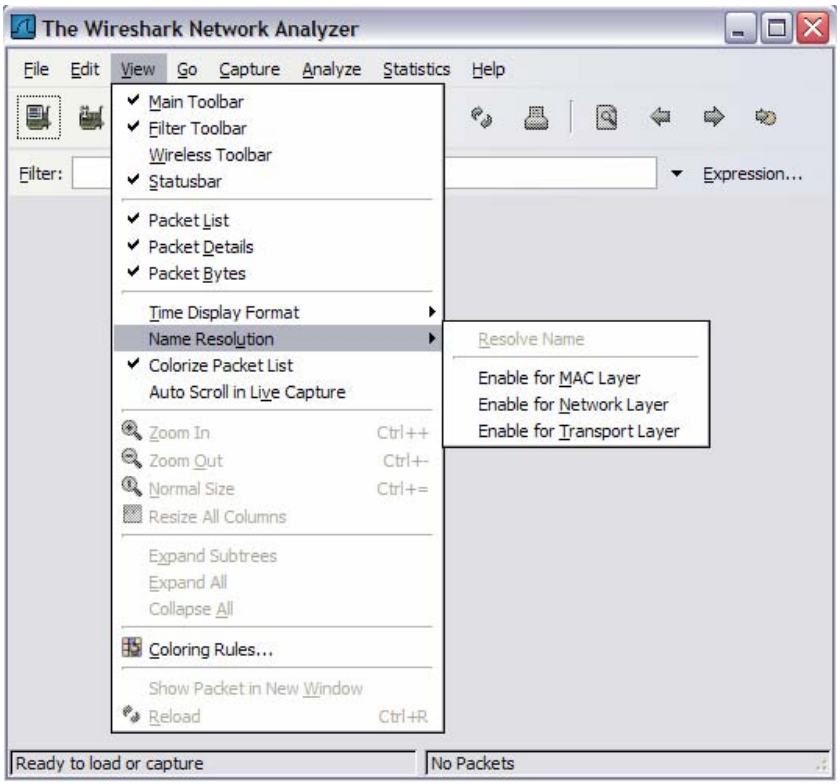


Figura 4. Cambios a la vista predeterminada de Wireshark.

Paso 2: Cargue la captura del cliente Web, `eagle1_web_client.pcap`.

Se muestra una pantalla similar a la de la Figura 5. Hay varios menús y submenús desplegables disponibles. También hay dos ventanas de datos separadas. La ventana Wireshark de arriba muestra todos los paquetes capturados. La ventana inferior contiene los detalles de los paquetes. En la ventana inferior, cada línea que contiene una casilla de verificación ☒ indica que hay información adicional disponible.

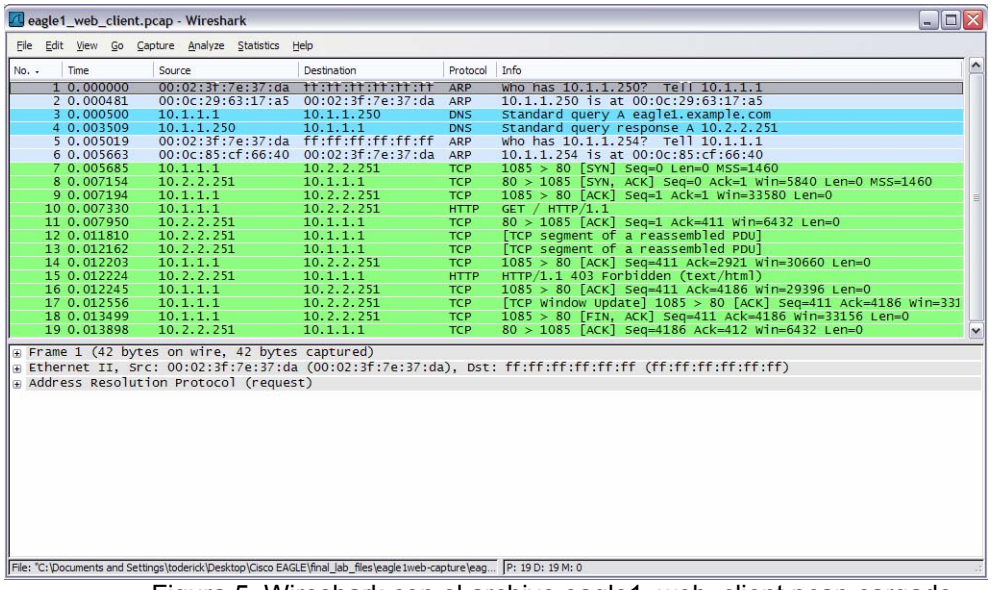


Figura 5. Wireshark con el archivo eagle1_web_client.pcap cargado.

Tarea 2: Revisar el proceso de flujo de datos a través de la red.

Paso 1: Revise el funcionamiento de la capa de Transporte.

Cuando PC_Client crea el datagrama para una conexión con eagle1.example.com, el datagrama viaja a través de las distintas capas de red. En cada capa se agrega la información de encabezado importante. Dado que esta comunicación es desde un cliente Web, el protocolo de la capa de Transporte será TCP. Vea el segmento TCP que se muestra en la Figura 6. PC_Client genera una dirección de puerto TCP interna, en esta conversación 1085, y reconoce la dirección de puerto del servidor Web conocida, 80. De la misma forma, se ha generado internamente un número de secuencia. Se incluye información suministrada por la capa de Aplicación. Habrá ciertos tipos de información que PC_Client no conocerá, y que por lo tanto deberán averiguarse utilizando otros protocolos red.

No hay número de acuse de recibo. Antes de que este segmento pueda pasar a la capa de Red, debe realizarse el protocolo de enlace de tres vías de TCP.

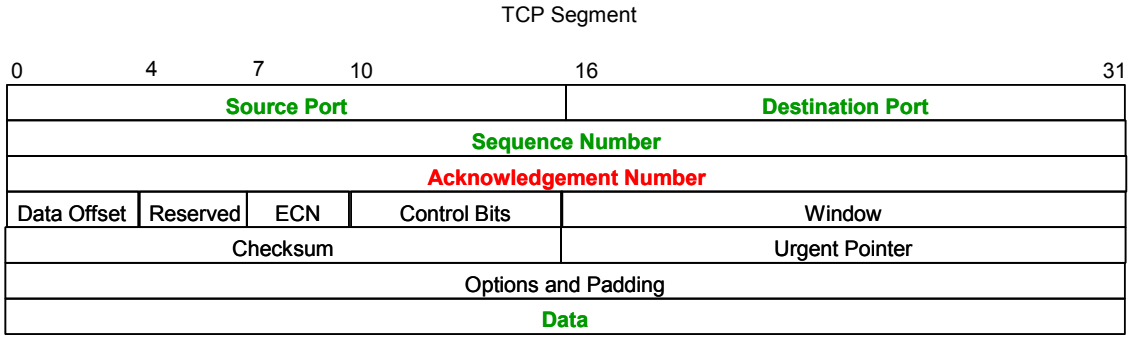


Figura 6. Campos del segmento TCP.

Paso 2: Revise el funcionamiento de la capa de Red.

En la capa de Red, el PAQUETE (IP) IPv4 tiene varios campos completados con información. Esto se ilustra en la Figura 7. Por ejemplo: se observa la Versión del paquete (IPv4), al igual que la dirección IP de origen.

El destino para este paquete es eagle1.example.com. La dirección IP correspondiente se debe averiguar a través del DNS (Sistema de nombres de dominio). Los campos relacionados con los protocolos de la capa superior permanecen vacíos hasta que se recibe el datagrama de la capa superior.

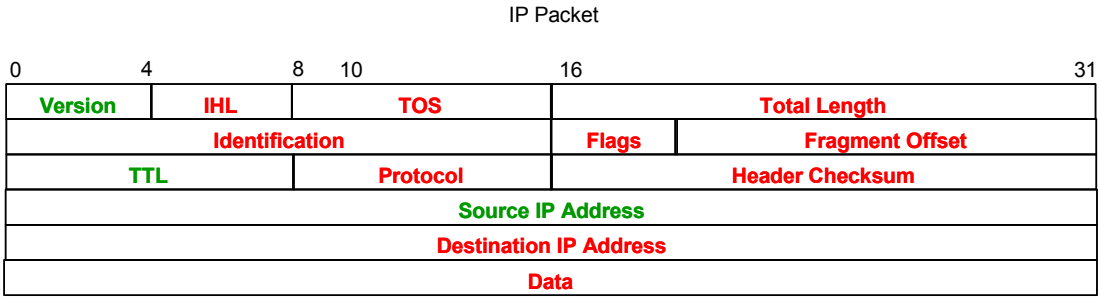


Figura 7. Campos del Paquete IP.

Paso 3: Revise el funcionamiento de la capa de Enlace de datos.

Antes de que el datagrama se coloque en el medio físico, debe encapsularse dentro de una trama. Esto se ilustra en la Figura 8. PC_Client conoce la dirección MAC de origen, pero debe averiguar la dirección MAC de destino.

Se debe averiguar la dirección MAC de destino.

Ethernet II Frame Format

Preamble	Destination Address	Source Address	Frame Type	Data	CRC
8 Octets	**6 Octets**	**6 Octets**	2 Octets	46-1500 Octets	**4 Octets**

Figura 8. Campos de la trama de Ethernet II.

Tarea 3: Analizar los paquetes capturados.

Paso 1: Revise la secuencia del flujo de datos.

Revisar la información que falta es de utilidad en el seguimiento de la secuencia de los paquetes capturados:

a. No se puede construir el segmento TCP porque el campo de acuse de recibo está en blanco. Primero debe completarse un protocolo de enlace de tres vías de TCP con eagle1.example.com.

b. El protocolo de enlace de tres vías de TCP no se puede aplicar porque PC_Client no conoce la dirección IP de eagle1.example.com. Esto se resuelve con una solicitud de DNS de PC_Client a servidor DNS.

c. No se puede consultar al servidor DNS porque se desconoce su dirección MAC. El protocolo ARP se emite en la LAN para averiguar la dirección MAC del servidor DNS.

d. No se conoce la dirección MAC para eagle1.example.com. El protocolo ARP se emite en la LAN para averiguar la dirección MAC de destino de eagle1.example.com.

Paso 2: Examine la solicitud de ARP.

Consulte el N.º 1 en la ventana Lista de paquetes de Wireshark. La trama capturada es una Solicitud de ARP (Address Resolution Protocol). Se puede consultar el contenido de la trama de Ethernet II haciendo clic en la casilla de verificación en la segunda línea de la ventana Detalles del paquete. Se puede ver el contenido de la Solicitud de ARP haciendo clic en la línea de Solicitud de ARP en la ventana Detalles del paquete.

1. ¿Cuál es la dirección MAC de origen para la Solicitud de ARP? _____
2. ¿Cuál es la dirección MAC de destino para la Solicitud de ARP? _____
3. ¿Cuál es la dirección IP desconocida en la Solicitud de ARP? _____
4. ¿Cuál es el tipo de trama de Ethernet II? _____

Paso 3: Examine la respuesta de ARP.

Consulte el N.º 2 en la ventana Lista de paquetes de Wireshark. El servidor DNS envió una Respuesta de ARP.

1. ¿Cuál es la dirección MAC de origen para la Respuesta de ARP? _____
2. ¿Cuál es la dirección MAC de destino para la Solicitud de ARP? _____
3. ¿Cuál es el tipo de trama de Ethernet II? _____
4. ¿Cuál es la dirección IP de destino en la Respuesta de ARP? _____
5. En base a la observación del protocolo ARP, ¿qué se puede inferir acerca de la dirección de destino de una Solicitud de ARP y de la dirección de destino de una Respuesta de ARP?
   _____
   _____
   _____
6. ¿Por qué el servidor DNS no tuvo que enviar una Solicitud de ARP para la dirección MAC de PC_Client? _____
   _____

Paso 4: Examine la consulta de DNS.

Consulte el N.º 3 en la ventana Lista de paquetes de Wireshark. PC_Client envió una consulta de DNS al servidor DNS. Utilizando la ventana Detalles del paquete, responda a las siguientes preguntas:

1. ¿Cuál es el tipo de trama de Ethernet II? _____
2. ¿Cuál es el protocolo de la capa de Transporte, y cuál es el número de puerto de destino?
   _____

Paso 5: Examine la respuesta a la consulta de DNS.

Consulte el N.º 4 en la ventana Lista de paquetes de Wireshark. El servidor DNS envió una respuesta a la consulta de DNS de PC_Client. Utilizando la ventana Detalles del paquete, responda a las siguientes preguntas:

1. ¿Cuál es el tipo de trama de Ethernet II? _____
2. ¿Cuál es el protocolo de la capa de Transporte, y cuál es el número de puerto de destino?
   _____
3. ¿Cuál es la dirección IP de eagle1.example.com? _____
4. Un colega es un administrador de firewall, y preguntó si conocía alguna razón por la que no debería bloquearse la entrada de todos los paquetes UDP a la red interna. ¿Cuál es su respuesta?
   _____
   _____
   _____
   _____

Paso 6: Examine la solicitud de ARP.

Consulte el N.º 5 y el N.º 6 de la ventana Lista de paquetes de Wireshark. PC_Client envió una Solicitud de ARP a la dirección IP 10.1.1.254.

1. ¿Esta dirección IP difiere de la dirección IP para eagle1.example.com? Explique.
   _____
   _____

Paso 7: Examine el protocolo de enlace de tres vías de TCP.

Consulte el N.º 7, el N.º 8 y el N.º 9 de la ventana Lista de paquetes de Wireshark. Estas capturas contienen el protocolo de enlace de tres vías de TCP entre PC_Client e eagle1.example.com. Inicialmente, sólo está configurado en el datagrama el señalizador TCP SYN enviado desde PC_Client, número de secuencia 0. eagle1.example.com responde con los señalizadores TCP ACK y SYN establecidos, junto con el acuse de recibo de 1 y la secuencia de 0. En la ventana Lista de paquetes, figura un valor no descrito, **MSS=1460**. MSS significa tamaño máximo de segmento. Cuando se transporta un segmento TCP a través del IPv4, el MSS se calcula como el tamaño máximo de un datagrama IPv4 menos 40 bytes. Este valor se envía durante el comienzo de la conexión. Esto también sucede cuando se negocian las ventanas deslizantes de TCP.

1. Si el valor de secuencia inicial de TCP de PC_Client es 0, ¿por qué eagle1.example respondió con un acuse de recibo de 1?
   _____
   _____
2. En el N.º 8 de eagle1.example.com, ¿qué significa el valor de 0x04 del señalador IP?
   _____
3. Una vez que PC_Client completa el protocolo de enlace de 3 vías de TCP, N.º 9 de la Lista de paquetes de Wireshark, ¿cuáles son los estados del señalizador TCP que se devuelven a eagle1.example.com?
   _____

Tarea 4: Completar el análisis final.

Paso 1: Haga coincidir el resultado de Wireshark con el proceso.

Ha sido necesario el envío de un total de nueve datagramas entre PC_Client, el servidor DNS, el gateway e eagle1.example.com para que PC_Client tuviera la información suficiente para enviar la solicitud original del cliente Web a eagle1.example.com. Esto se muestra en el N.º 10 de la Lista de paquetes de Wireshark, donde PC_Client envió una solicitud GET del protocolo Web.

1. Complete con el número correcto de la Lista de paquetes de Wireshark correspondiente a cada una de las siguientes entradas que faltan:

   a. No se puede construir el segmento TCP porque el campo de acuse de recibo está en blanco. Primero debe completarse un protocolo de enlace de tres vías de TCP con eagle1.example.com. _____

   b. El protocolo de enlace de tres vías de TCP no se puede aplicar porque PC_Client no conoce la dirección IP de eagle1.example.com. Esto se resuelve con una solicitud de DNS de PC_Client a servidor DNS. _____

   c. No se puede consultar al servidor DNS porque se desconoce su dirección MAC. El protocolo ARP se emite en la LAN para averiguar la dirección MAC del servidor DNS. _____

   d. Se desconoce la dirección MAC para que el gateway llegue a eagle1.example.com. El protocolo ARP se emite en la LAN para averiguar la dirección MAC de destino del gateway. _____

2. El N.º 11 de la Lista de paquetes de Wireshark es un acuse de recibo de eagle1.example.com para la solicitud GET de PC_Client, el N.º 10 de la Lista de paquetes Wireshark.

3. Los N.º 12, 13 y 15 de la Lista de paquetes de Wireshark son segmentos TCP de eagle1.example.com. Los N.º 14 y 16 de la Lista de paquetes de Wireshark son datagramas de ACK de PC_Client.

4. Para verificar el ACK, resalte el N.º 14 de la Lista de paquetes de Wireshark. Luego, desplácese hasta la parte inferior de la ventana de la lista de detalles, y amplíe la trama [SEQ/ACK analysis]. ¿A qué datagrama de eagle1.example.com responde el datagrama ACK para el N.º 14 de la Lista de paquetes de Wireshark? _____

5. El datagrama N.º 17 de la Lista de paquetes de Wireshark se envía desde PC_Client a eagle1.example.com. Revise la información que se encuentra dentro de la trama [SEQ/ACK analysis]. ¿Cuál es el propósito de este datagrama? _____

6. Cuando PC_Client finaliza, se envían los señalizadores TCP ACK y FIN, que se muestran en el N.º 18 de la Lista de paquetes de Wireshark. eagle1.example.com responde con un ACK de TCP, y se cierra la sesión TCP.

Paso 2: Use el flujo TCP de Wireshark.

Analizar el contenido de los paquetes puede ser una experiencia abrumadora, prolongada y con tendencia a los errores. Wireshark incluye una opción que construye el flujo TCP en otra ventana. Para usar esta función, seleccione primero un datagrama TCP de la Lista de paquetes de Wireshark. A continuación, en el menú de Wireshark, seleccione las opciones Analizar | Seguir flujo TCP. Se mostrará una ventana similar a la Figura 9.

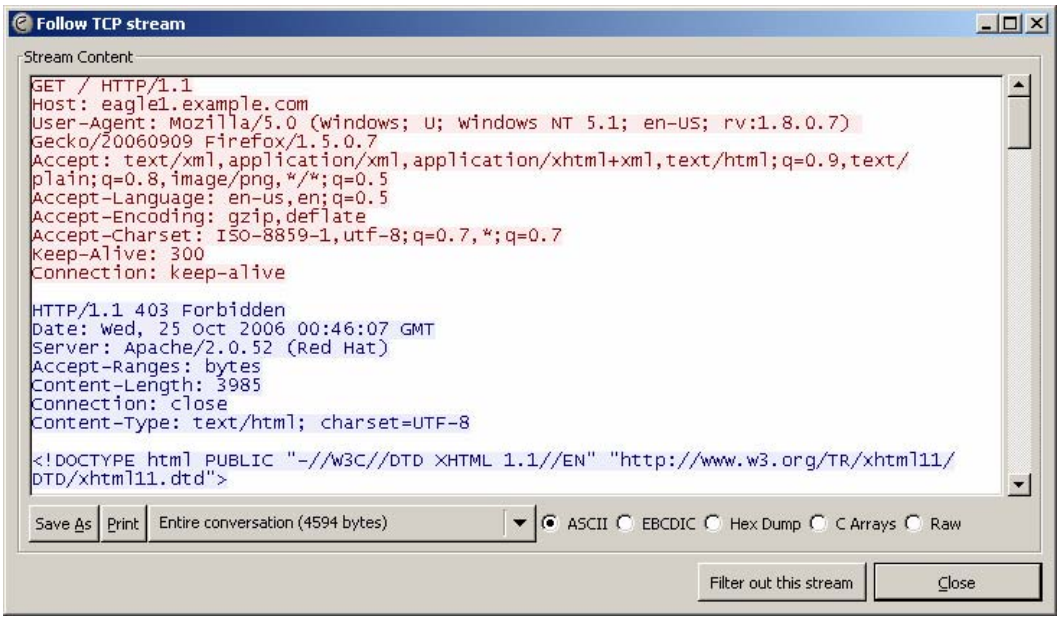


Figura 9. Resultado del flujo TCP.

Tarea 5: Conclusión

Usar un analizador de protocolos de red puede ser una herramienta de aprendizaje efectiva para comprender los elementos fundamentales de la comunicación en red. Una vez que el administrador de red se familiariza con los protocolos de comunicación, el mismo analizador de protocolos puede convertirse en una herramienta efectiva para la resolución de problemas cuando se producen fallas en la red. Por ejemplo, si un explorador Web no se pudo conectar a un servidor Web pueden existir diversas causas. Un analizador de protocolos muestra las solicitudes de ARP fallidas, las consultas de DNS fallidas y los paquetes sin acuse de recibo.

Tarea 6: Resumen

En este ejercicio el estudiante ha aprendido cómo se establece la comunicación entre en un cliente Web y un servidor Web. Los protocolos que no están a la vista, como DNS y ARP, se usan para completar las partes faltantes de los paquetes IP y de las tramas de Ethernet, respectivamente. Antes de poder iniciar una sesión TCP, el protocolo de enlace de tres vías de TCP debe establecer una ruta confiable y suministrar la información del encabezado TCP inicial a ambos sistemas finales que se comunican. Por ultimo, cuando el cliente envía un señalizador TCP FIN se elimina la sesión TCP de manera ordenada.

11.6.1: Desafío de integración de capacidades: Configuración y evaluación de la red de laboratorio

Diagrama de topología

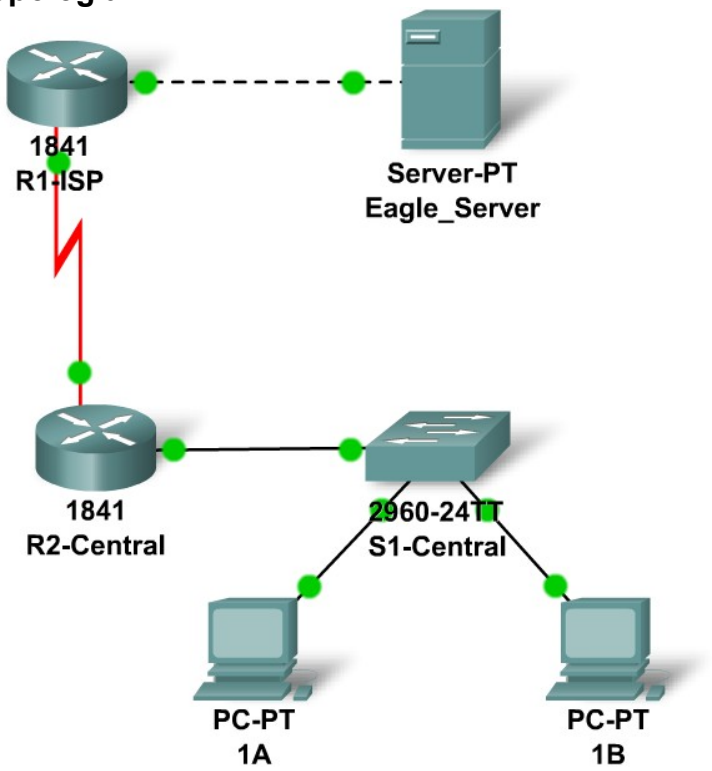


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	Fa0/0			No aplicable
	S0/0/0			No aplicable
R2-Central	Fa0/0			No aplicable
	S0/0/0			No aplicable
PC1A	NIC			
PC1B	NIC			
Eagle Server	NIC			

Objetivos de aprendizaje

- Construir, probar y configurar la red de laboratorio completa.
  - Integrar habilidades a través de todo el curso.
- Analizar los eventos involucrados en:
  - La solicitud de una página Web (DNS, ARP, HTTP, TCP, IP, Ethernet, HDLC).
  - El rastreo de la ruta al servidor Web (DNS, UDP, ARP, ICMP, IP, Ethernet, HDLC)

Información básica

Durante el curso, ha desarrollado aptitudes para planificar, construir, configurar y probar redes. También ha desarrollado una comprensión conceptual de los protocolos de red y los algoritmos de los dispositivos. A continuación tiene la oportunidad de evaluar sus conocimientos. Intente completar todo el desafío (aproximadamente 100 componentes configurables, aunque algunos son bastante sencillos) en menos de 30 minutos.

Tarea 1: Planificación

Use la topología de laboratorio estándar de Exploration al planificar su esquema de direccionamiento IP:

- Dos routers 1841 con tarjetas de interfaz WIC-2T, instaladas en la ranura manual derecha (una denominada R1-ISP, que tiene la conexión serial DCE WAN con R2-Central, y la conexión Fa0/0 LAN con el servidor Eagle_Server) y otra denominada R2-Central (que tiene una conexión serial DCE WAN con R1-ISP y la conexión Fa0/0 LAN con S1-Central)
- Un Switch 2960TT (S1-Central)
- Dos PC denominadas 1A y 1B
- Un servidor denominado Eagle_Server.

Tenga en cuenta que tanto los nombres de visualización como los nombres de los hosts para todos los dispositivos deben estar configurados de manera exacta y, en general, todas las cadenas (nombres, contraseñas, títulos) deben ser escritos exactamente como se especifica en las instrucciones para trabajar correctamente.

Recibió un bloque de direcciones IP de 192.168.3.0 /24. Debe prever las redes existentes y el futuro crecimiento.

Las asignaciones de subred son:

- 1.ª subred, LAN actual de estudiantes, hasta 28 hosts (Fa0/0 en R2-Central, conectado a Fa0/24 en S1-Central)
- 2.ª subred, LAN futura de estudiantes, hasta 28 hosts (aún no implementada)
- 3.ª subred, LAN del ISP actual, hasta 14 hosts (Fa0/0 en R1-ISP)
- 4.ª subred, LAN de ISP futuro, hasta 7 hosts (aún no implementada)
- 5.ª subred, WAN actual, enlace punto a punto (S0/0/0 en R1-ISP y S0/0/0 en R2-Central)

Las asignaciones de direcciones IP son:

- Para el servidor, configure la segunda dirección IP más utilizable en la subred ISP LAN.
- Para la interfaz F0/0 de R1-ISP configure la dirección IP más utilizable en la subred ISP LAN.
- Para la interfaz F0/0/0 de R1-ISP configure la dirección más utilizable en la subred WAN existente.
- Para la interfaz F0/0/0 de R2-Central use la dirección menos utilizable en la subred WAN existente.
- Para la interfaz Fa0/0 de R2-Central, use la dirección más utilizable en la subred LAN de estudiantes existente y conéctela a la interfaz Fa0/24 en S1-Central.
- Para los hosts 1A y 1B, use las dos primeras direcciones IP (las dos direcciones menos utilizables) de la subred LAN actual de estudiantes y conéctelas a las interfaces Fa0/1 y Fa0/2 de S1-Central.
- Para la interfaz de administración del switch, use la segunda dirección más utilizable en la subred de estudiantes.

Tarea 2: Construcción y configuración de la red.

Construya la red cuidando de realizar las conexiones como se especifica. Configure ambos routers, el switch, el servidor y las dos PC.

Configure los routers con la Interfaz de línea de comando (CLI) para practicar sus habilidades. La configuración del router debe incluir “mantenimiento” (nombre de visualización, nombre del host, contraseñas, mensajes), interfaces (Fast Ethernet y Serial) y enrutamiento (ruta estática en R1-ISP, ruta default en R2-Central). Las siguientes contraseñas de inicio de sesión se deben establecer para “cisco” (sin comillas): enable secret, console y Telnet. Los mensajes deben decir **Éste es R1-ISP del router de laboratorio. Acceso autorizado solamente.** y **Éste es R2-Central del router de laboratorio. Acceso autorizado solamente.**

Las interfaces deben estar configuradas según se especifica en la sección de direccionamiento IP anterior, use una frecuencia de reloj de 64000 en la interfaz S0/0/0 de R1-ISP. La ruta estática en R1-ISP debe apuntar a la subred LAN de estudiante existente a través de la dirección IP de la interfaz serial de R2-Central; la ruta estática en R2-Central tiene que ser una ruta estática que apunta a través de la dirección IP de la interfaz serial de R1-ISP. Cada vez que configure un dispositivo Cisco IOS, asegúrese de guardar su configuración.

En el switch, configure el nombre de visualización, el nombre del host, el mensaje (**Éste es S1-Central del switch de laboratorio. Acceso autorizado solamente.**), contraseñas de inicio de sesión para la interfaz de acceso (enable secret, console y Telnet, contraseñas establecidas todas para “cisco”) y de administración (int vlan1). Cada vez que configure un dispositivo Cisco IOS, asegúrese de guardar su configuración.

Para los Hosts 1A y 1B, además de la configuración IP, configúrelos para usar servicios DNS. Para el servidor, habilite los servicios DNS, use el nombre de dominio eagle-server.example.com y habilite los servicios HTTP.

Cuando esté trabajando, use “Revisar resultados” para ver qué componentes necesitan aún ser configurados. Si quiere más práctica, use “Reiniciar actividad” y vuelva a tomarse el tiempo que tarda para realizar la configuración completa nuevamente.

Tarea 3: Prueba y análisis

Es una buena práctica probar la conectividad mediante ping y Telnet y examinar las tablas de enrutamiento. Una vez que sepa que su red está funcionando, asegúrese de que haya guardado sus configuraciones en los dispositivos Cisco IOS. Luego reinicie los dispositivos y restablezca la red. En el modo de simulación, solicite una página Web mientras deja visible los siguientes protocolos en la lista de eventos: DNS, HTTP, Telnet, TCP, UDP, ICMP, ARP. Examine los paquetes a medida que son procesados por los dispositivos para estudiar el comportamiento del protocolo, especialmente cómo IP se relaciona con todo. También observe los algoritmos usados por los hosts, switches y routers. Explique el proceso completo a un compañero. Reinicie los dispositivos para borrar la red nuevamente, y también en el modo de simulación, ejecute traceroute en el servidor desde una de las PC. Examine cómo se construye el rastro por las solicitudes de petición de eco ICMP. Explique nuevamente el proceso completo a un compañero.

Tarea 4: Reflexión

Relacione el proceso observado en la Tarea 3 con el Gráfico de protocolo TCP/IP. Sus aptitudes para modelar las redes en el rastreador de paquetes lo ayudarán mucho en los siguientes cursos.