GUIA PRÁCTICA PARA CONFIGURACIÓN E IMPLEMENTACIÓN DE REDES ENRUTADAS

AICHELLE JUDITH OROZCO PAREJA

EDUARDO LACIDES ALFARO ZOLÁ

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS

2005

GUIA PRÁCTICA PARA CONFIGURACIÓN E IMPLEMENTACIÓN DE REDES ENRUTADAS

AICHELLE JUDITH OROZCO PAREJA

EDUARDO LACIDES ALFARO ZOLÁ

Monografía de grado presentada como requisito para optar el título de Ingeniero de Sistemas

Director

ISAAC ZUÑIGA
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS

2005

Cartagena de Indias, D.T. y C., Noviembre 30 de 2005

AUTORIZACIÓN

Nosotros **Aichelle Judith Orozco Pareja y Eduardo Lacides Alfaro Zolá**, autorizamos a la **Universidad Tecnológica de Bolívar** para hacer uso del trabajo de grado y publicarlo en el catálogo online de la Biblioteca Luis Enrique Borja Barón.

AICHELLE OROZCO PAREJA
CC. 22.793.795 de Cartagena

EDUARDO ALFARO ZOLA
CC. 73.576.215 de Cartagena

Cartagena de Indias D. T. y C., Noviembre de 2005

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS

Universidad Tecnológica de Bolívar

LC.

Respetados Señores:

Tengo el agrado de presentar a su consideración, estudio y aprobación, la monografía titulada **"GUIA PRÁCTICA PARA CONFIGURACIÓN E IMPLEMENTACIÓN DE REDES ENRUTADAS",** desarrollado por los estudiante **Aichelle Orozco Pareja y Eduardo Alfaro Zolá.**

Al respecto me permito comunicar que he dirigido el citado trabajo, el cual considero de gran importancia y utilidad.

Atentamente,

Ing. Isaac Zúñiga Silgado

Director de Proyectos

Cartagena de Indias D. T. y C., Noviembre de 2005

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS

Universidad Tecnológica de Bolívar

LC.

Respetados Señores:

Con toda atención, nos dirigimos a ustedes, con el fin de presentar a su consideración, estudio y aprobación, el trabajo titulado **"GUIA PRÁCTICA PARA CONFIGURACIÓN E IMPLEMENTACIÓN DE REDES ENRUTADAS",** como requisito parcial para aprobar el Minor en Comunicaciones y Redes.

Atentamente,

AICHELLE OROZCO PAREJA	**EDUARDO ALFARO ZOLA**
CC. 22.793.795 de Cartagena	**CC. 73.576.215 de Cartagena**

Nota de aceptación

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

TABLA DE CONTENIDO

INTRODUCCION

Para entender el rol que los computadores juegan en un sistema de Networking, considere la Internet. Se deben configurar protocolos o reglas antes que un computador se pueda conectar a Internet.

Las funciones de Networking se describen usando modelos divididos en capas. Los dos modelos más importantes, son el modelo de Internetworking de Sistemas Abiertos (OSI) y el modelo de Protocolo de control de transmisión/Protocolo Internet (TCP/IP). En los laboratorios también se exponen las diferencias y similitudes entre ambos modelos.

Cada modelo ofrece su propia estructura para explicar cómo funciona una red, pero los dos comparten muchas características. La falta de comprensión de cualquier de los dos modelos puede hacer que un administrador de sistemas no cuente con la información suficiente para determinar por qué una red funciona de cierta forma.

Esta guía describe los dispositivos de red, al igual que las disposiciones físicas, lógicas y del cableado.

Esta guía presenta también información sobre los elementos de las LAN de Ethernet y la creación de varios tipos de red LAN.

Las WAN presentan varias características importantes que las distinguen de las LAN.

En la actualidad, están disponibles varias conexiones de red de área amplia (WAN). Éstas incluyen desde el acceso telefónico hasta acceso de banda ancha, y difieren en el ancho de banda, costo y equipo necesario. Estas guías muestran un tipo de conexión WAN básica de router a router.

El Protocolo de Internet (IP) es el principal protocolo de Internet. El direccionamiento IP permite que los paquetes sean enrutados desde el origen al destino usando la mejor ruta disponible. La propagación de paquetes, los cambios en el encapsulamiento y los

protocolos que están orientados a conexión y los que no lo están también son fundamentales para asegurar que los datos se transmitan correctamente a su destino. Estas guías brindan un panorama general de cada uno.

La diferencia entre los protocolos de enrutamiento y los enrutados es causa frecuente de confusión entre los estudiantes de Networking. Las dos palabras suenan iguales pero son bastante diferentes. Esta guía también introduce los protocolos de enrutamiento que permiten que los routers construyan tablas a partir de las cuales se determina la mejor ruta a un Host en la Internet.

No existen dos organizaciones idénticas en el mundo. En realidad, no todas las organizaciones pueden adaptarse al sistema de tres clases de direcciones A, B y C. Sin embargo, hay flexibilidad en el sistema de direccionamiento de clases. Esto se denomina división en subredes. La división en subredes permite que los administradores de red determinen el tamaño de las partes de la red con las que ellos trabajan. Después de determinar cómo segmentar su red, ellos pueden utilizar la máscara de subred para establecer en qué parte de la red se encuentra cada dispositivo. Esta guía también muestra un aprendizaje general en el concepto de subredes.

Resulta importante entender los componentes de la capa física de un router. Esta comprensión sienta las bases para otros conocimientos y habilidades necesarios para configurar los routers y administrar las redes enrutadas. Esta guía describe las técnicas para establecer una conexión física entre las distintas interfaces de los routers.

La tecnología de Cisco se basa en el sistema operativo de Internetworking de Cisco (IOS), que es el software que controla las funciones de enrutamiento y conmutación de los dispositivos de red. Es esencial que el administrador de red cuente con una sólida comprensión acerca del IOS. Esta guía presenta una introducción al uso del comando de administración IOS. Todas las tareas de configuración de red, desde las más básicas hasta las más complejas, requieren un conocimiento sólido de los fundamentos básicos de la

configuración del router. También brinda las herramientas y las técnicas para la configuración básica del router.

Configurar un router para que realice las complejas tareas de redes y telecomunicaciones puede resultar un desafío. No obstante, los procedimientos iniciales para configurar el router no son difíciles en absoluto. Si se ejercitan estos procedimientos y los pasos para cambiar de un modo a otro, las configuraciones más complejas no serán tan abrumadoras. Esta guía introduce los modos básicos de configuración del router y brinda oportunidades para practicar configuraciones sencillas.

La meta de todo administrador de red debe ser la de disponer de configuraciones claras y fáciles de entender, y que las mismas sean respaldadas periódicamente. El Cisco IOS brinda al administrador una gama de herramientas que permiten agregar comentarios al archivo de configuración, para efectos de documentación. De la misma manera que un programador competente documenta cada paso de su programación, un administrador de red debe documentar cuanta información le sea posible, en caso de que otra persona deba asumir la responsabilidad de la red.

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos. Aunque las herramientas de seguridad, como por ejemplo: las contraseñas, equipos de callback y dispositivos de seguridad física, son de ayuda, a menudo carecen de la flexibilidad del filtrado básico de tráfico y de los controles específicos que la mayoría de los administradores prefieren. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero impedir a los usuarios externos el acceso telnet a la LAN.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior. Esta guía introduce las ACL estándar y extendidas como medio de control

del tráfico de red y explica de qué manera se utilizan las ACL como parte de una solución de seguridad.

Además, incluye los comandos y configuraciones necesarias para crear las ACL. Finalmente, brinda ejemplos de ACL estándar y extendidas y su aplicación en las interfaces del router.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers.

1. GUIAS DE LABORATORIO

Estas guías de laboratorio como herramientas pedagógicas permiten al profesor establecer pautas para la enseñanza práctica de los conceptos de Networking, Routers y Enrutamiento con el fin de que el estudiante pueda identificar cada uno de los componentes que hacen parte de una red estructurada, establecer las diferencias entre los diferentes dispositivos utilizados para tal fin como lo son los Routers y Switches; y comprender y analizar cada uno de los algoritmos de enrutamiento que pueden manejar dichos dispositivos.

Estas guías están desarrolladas de tal manera que su grado de complegidad es directamente proporcional a la aplicación de la misma, es decir, en las primeras prácticas se aplicarán los conceptos básicos de Networking y a medida que se vayan realizando se irá profundizando en los conceptos de Enrutamiento: estructura física y configuración de routers.

Están diseñadas de tal manera que para un estudiante de pregrado es de fácil comprensión y desarrollo y a la vez permiten que un estudiante con los conocimientos respectivos pueda monitorearlas.

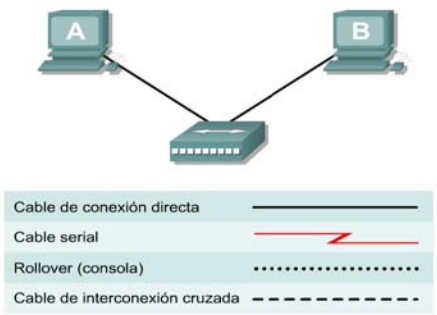
Todos los laboratorios constan de las siguientes partes:

- Tema
- Objetivos
- Tiempo estimado
- Información básica
- Pasos a seguir (montaje)

2. CONCEPTOS BÁSICOS DE NETWORKING

2.1 Laboratorio

RED LAN, UTILIZANDO UN HUB



Objetivo

- Crear una red simple con dos PC mediante un hub
- Identificar el cable correcto para conectar los dos PC al hub
- Configurar la información de dirección IP de las estaciones de trabajo
- Probar la conectividad con el comando **ping**

Tiempo estimado

30 minutos

Información básica

Este laboratorio se ocupa de la capacidad para conectar dos PC para crear una red LAN de Ethernet simple basada en hub entre dos estaciones de trabajo. Un hub es un dispositivo de concentración de networking que a veces se define como repetidor multipuerto. Los hubs son económicos y fáciles de instalar, pero permiten que se produzcan colisiones. Son apropiados para una LAN pequeña con tráfico liviano.

Además de las conexiones físicas y las de enlace de datos, que son de las Capas 1 y 2, los computadores también deben configurarse con los valores correctos de red IP, que es un tema de Capa 3, para que puedan comunicarse. Como en esta laboratorio se usa un hub, se necesita un cable UTP básico de conexión directa de Categoría 5/5e para conectar cada PC al hub. Esto se define como cable de conexión u cableado horizontal, que se usa para conectar estaciones de trabajo y una LAN típica. Inicie este laboratorio de laboratorio con el equipo apagado y el cableado desconectado. Se trabaja en equipos de dos con una persona por PC.

Serán necesarios los siguientes recursos:

- Dos estaciones de trabajo con una NIC de Ethernet 10/100 instalada
- Un hub de Ethernet 10BaseT o de Fast Ethernet
- Varios cables de Ethernet, de conexión directa y cruzada para elegir, para conectar las dos estaciones de trabajo

Paso 1: Identificar el cable de Ethernet correcto y conectar los dos PC al hub

a. La conexión entre los dos PC y el hub se realiza mediante un cable de conexión directa de Categoría 5 ó 5e. Busque dos cables que sean lo suficientemente largos para llegar desde cada PC al hub. Conecte un extremo a la NIC y el otro a un puerto del hub. Inspeccione cuidadosamente los extremos de los cables y seleccione solamente un cable de conexión directa.

b. ¿Qué clase de cable se requiere para conectarse de una NIC al hub?
_____

c. ¿Cuál es la categoría del cable? _____

d. ¿Cuál es la designación de tamaño de hilo AWG del cable?
_____

Paso 2: Verificar la conexión física

a. Enchufe y encienda los computadores. Para verificar las conexiones de los computadores, asegúrese de que las luces de los enlaces de ambas NIC de los PC y las interfaces del hub estén encendidas. ¿Todas las luces de los enlaces están encendidas? _____

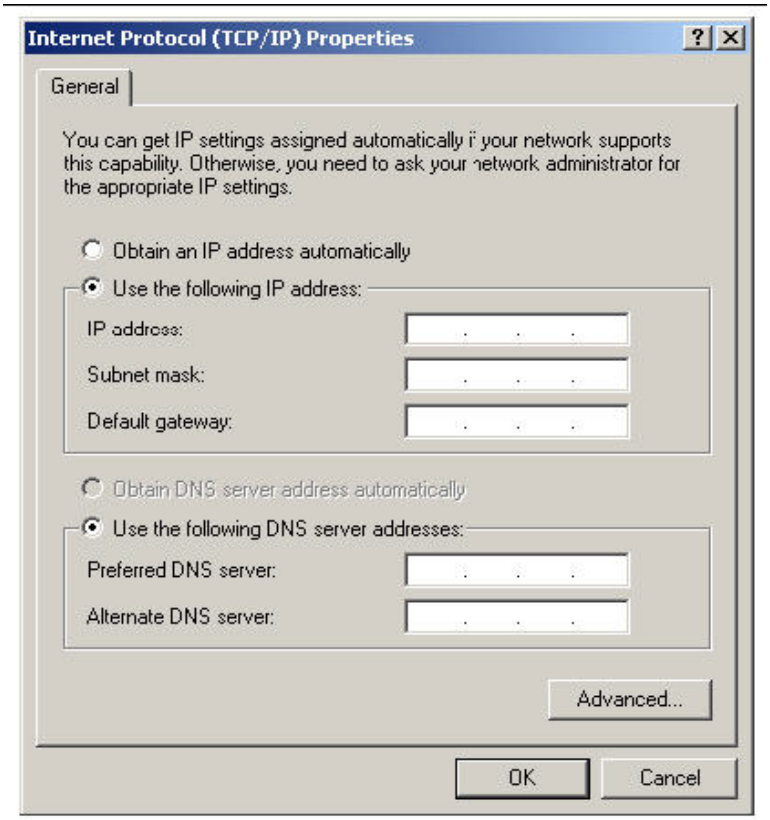
Paso 3: Acceder a la ventana de valores de IP

Nota: Anote los valores existentes de IP, para poder restaurarlos al final del laboratorio. Estos valores incluyen la dirección IP, la máscara de subred, el gateway por defecto y los servidores DNS. Si la estación de trabajo es un cliente DHCP, no es necesario registrar esta información.

Los usuarios de Windows XP/2003 profesional deben hacer lo siguiente:

- Haga clic en **Inicio** > **Configuraciones** > **Panel de control** y haga clic en el icono **Conexiones de red**.
- Seleccione **Conexión de área local** y haga clic en **Cambiar la configuración de esta conexión**.
- Seleccione el icono del **protocolo TCP/IP** asociado con la NIC de este PC.
- Haga clic en **Propiedades** y haga clic en **Usar la siguiente dirección IP**.

Vea el ejemplo siguiente:



Paso 4: Configurar los valores de TCP/IP para los dos PC

a. Configure la información de la dirección IP para cada PC según la información en la tabla.

b. Observe que la dirección IP del gateway por defecto no se requiere, dado que estos computadores están directamente conectados. El gateway por defecto sólo se requiere en las redes de área local que están conectadas a un router.

Computador	Dirección IP	Máscara de subred	Gateway por defecto
PC – A	192.168.1.1	255.255.255.0	No se requiere
PC – B	192.168.1.2	255.255.255.0	No se requiere

Paso 5: Acceder al símbolo del sistema o MS-DOS

a. En el menú Inicio, abra la ventana de símbolo del sistema (similar al sistema MS-DOS).

Los usuarios de Windows XP/2003 profesional deben hacer lo siguiente:
Inicio > **Programas** > **Accesorios** > **Símbolo del sistema**

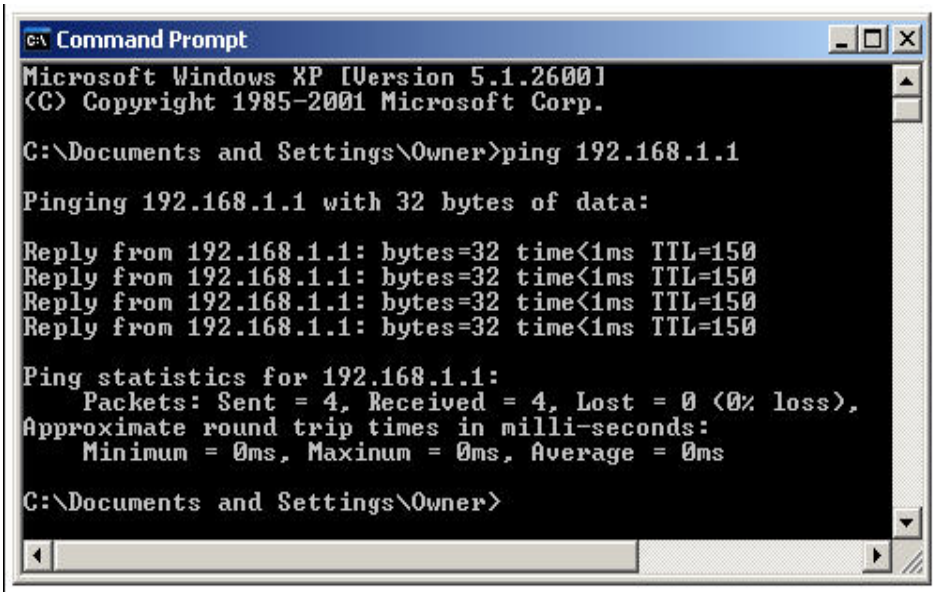
Paso 6: Verificar si los PC se pueden comunicar

a. Pruebe la conectividad de un PC al otro a través del hub haciendo "ping" a la dirección IP del otro computador. Introduzca el comando siguiente en la ventana de comandos.
C:>ping 192.168.1.1 (o 192.168.1.2)

b. Fíjese si los resultados son similares a los que aparecen a continuación. De lo contrario, verifique las conexiones de los PC y las configuraciones de TCP/IP en ambos PC. ¿Cuál fue el resultado de ping?

_____

_____



Paso 7: Confirmar las configuraciones de red TCP/IP

Los usuarios de Windows XP/2003 profesional deben hacer lo siguiente:

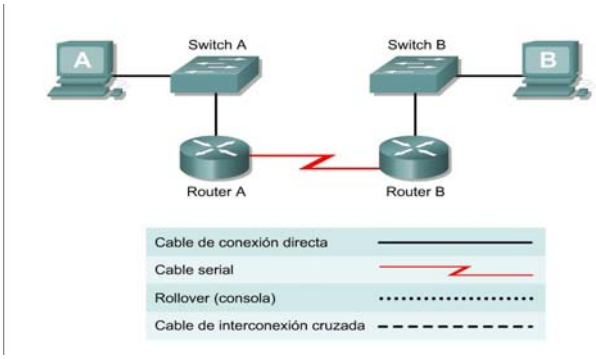
Escriba el comando **ipconfig** en el símbolo del sistema. Registre los resultados.

_____

Paso 8: Restaure los valores originales de IP de los PC, desconecte el equipo y guarde los cables.

2.2 Laboratorio

CREACIÓN DE UNA WAN ENRUTADA BÁSICA (CABLEADO LAN, WAN)



Objetivo

- Crear una red de área amplia enrutada simple (WAN) con dos PC, dos switches o hubs y dos routers
- Identificar los cables apropiados para conectar un PC y un router a cada switch
- Identificar los cables correctos para conectar los routers para formar un enlace de WAN
- Configurar la información de dirección IP de las estaciones de trabajo
- Probar la conectividad con el comando **ping**

Tiempo estimado

30 minutos

Información básica

Este laboratorio se ocupa de la capacidad para conectar dos LAN simples, cada una de ellas compuestas por una estación de trabajo y un switch o hub, para crear una WAN básica de router a router. Un router es un dispositivo de networking que se puede usar para interconectar LAN, que enruta paquetes entre diferentes redes con direccionamiento IP de Capa 3. Los routers normalmente se usan para conectar la Internet.

Además de las conexiones físicas y las de enlace de datos, que son de las Capas 1 y 2, los computadores y routers también deben configurarse con los valores correctos de red IP, que es un tema de la Capa 3, para que puedan comunicarse. Los cables de conexión directa se usan para conectar cada PC y router con su switch o hub. Se usan dos cables especiales V.35 para crear el enlace de WAN simulado entre los routers.

Nota: El instructor o asistente de laboratorio debe reconfigurar los dos routers para que tengan las direcciones IP correctas en sus interfaces de LAN y WAN. El Router A proporciona la señal de temporización como DCE.

Inicie este laboratorio con el equipo apagado y el cableado desconectado. Se trabaja en equipos de dos con una persona por LAN.
Serán necesarios los siguientes recursos:

- Dos estaciones de trabajo con una NIC de Ethernet 10/100 instalada
- Dos switches de Ethernet 10BaseT o de Fast Ethernet o dos hubs
- Dos routers con una interfaz RJ-45 de Ethernet o de Fast Ethernet (o una interfaz AUI) y por lo menos una interfaz serial.
- Transceptor AUI 10BASE-T (DB-15 a RJ-45) para un router con una interfaz AUI Ethernet, que es de serie 2500
- Cuatro cables de Ethernet de conexión directa para conectar las estaciones de trabajo y routers al hub o switch
- Un cable hembra (DCE) y uno macho (DTE) V.35 para interconectar los routers

Paso 1: Identificar y conectar el cable de Ethernet correcto desde el PC al switch

a. La conexión entre el PC y el switch se realiza mediante un cable de conexión directa de Categoría 5 ó 5e. Conecte un extremo a la NIC y el otro a un puerto del switch o hub. Inspeccione cuidadosamente los extremos de los cables y seleccione solamente un cable de conexión directa.

b. Examine el switch o hub.
¿Cuál es el número de modelo d es el número de modelo del switch o hub?
_____

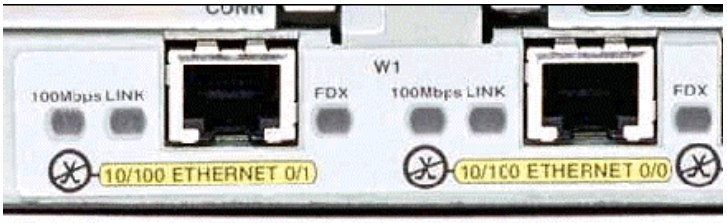
Paso 2: Identificar las interfaces de Ethernet o de Fast Ethernet en los routers

a. Examine los routers.

b. ¿Cuál es el número de modelo del Router A?
_____

c. ¿Cuál es el número de modelo del Router B?
_____

d. Ubique uno o más conectores RJ-45 en cada router rotulados “10/100 Ethernet” como se ve a continuación. El identificador puede variar según el tipo de router utilizado; se muestra un router serie 2600. Un router serie 2500 tendrá un puerto Ethernet AUI DB-15 rotulado “AUI 0”. Requiere un transceptor 10Base-T para conectarse al cable RJ-45.



e. Identifique cuáles de los puertos de Ethernet se pueden usar para conectar los routers. Registre la información a continuación. Registre los números de puerto AUI al trabajar con un router Cisco serie 2500.

Router	**Puerto**	**Puerto**

Puerto 3: Realizar el cableado de los enlaces de LAN del router

a. Configuración del router

Los routers deben ser preconfigurados por el instructor o asistente de laboratorio para que la interfaz Ethernet 0 en cada router tenga la dirección IP y máscara de subred correcta, según se indica en la tabla siguiente. Esto permite que los routers enruten paquetes entre las redes de área local 192.168.1.0 y 192.168.2.0.

Router	**Dirección IP de la interfaz E0**	**Máscara de subred**
Router – A	192.168.1.1	255.255.255.0
Router – B	192.168.2.1	255.255.255.0

b. Conexión de los cables

La conexión entre el router y el hub o switch se realiza mediante un cable de conexión directa CAT 5. Busque un cable de conexión lo suficientemente largo para ir desde el router al hub. Inspeccione cuidadosamente los extremos de los cables y seleccione solamente cables de conexión directa. Conecte la interfaz de Ethernet que usa designación 0 (cero) en el router a un puerto en el hub o switch. Al conectar routers serie 2500, use el transceptor 10BASE-T AUI.

Paso 4: Verificar las conexiones físicas de Ethernet

a. Conecte y encienda los computadores, switches/hubs y routers. Para verificar las conexiones, asegúrese de que las luces de los enlaces de ambas NIC de los PC, las interfaces del switch/hub y las interfaces de Ethernet del router estén encendidas. ¿Todas las luces de los enlaces están encendidas? _____En caso contrario, verifique las conexiones y tipos de cable.

Paso 5: Identificar las interfaces seriales en el router

a. Examine los routers.

b. Identifique los puertos seriales en cada router que se puedan usar para conectar los routers para simular un enlace de WAN. Registre la información a continuación. Si hay más de una interfaz serial, use la Interfaz 0 en cada router.

Nombre del router	**Puerto serial del router**	**Puerto serial del router**
Router A		
Router B		

Paso 6: Identificar y ubicar los cables V.35 correctos

a. A continuación, inspeccione los cables seriales disponibles en el laboratorio. Según el tipo de router y/o tarjeta serial, el router puede tener conectores diferentes.

b. Características de puerto serial del router
Los dos tipos más comunes son el conector DB-60 y el serial inteligente. En la tabla siguiente, indique qué tipo de routers se están utilizando.

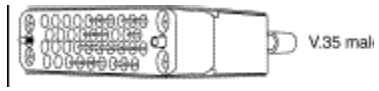
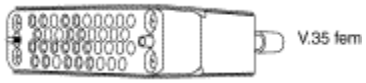
Router	**Serial Inteligente**	**DB60**
		
RTR A	☐	☐
RTR B	☐	☐

c. Simulación del enlace de WAN - DCE / DTE y temporización

Como esto no se conectará una línea arrendada en funcionamiento, uno de los routers debe proporcionar la temporización para el circuito. Esto es proporcionado normalmente a cada uno de los routers por un dispositivo DCE, como una CSU/DSU. Para proporcionar esta señal de temporización, uno de los routers necesitará un cable DCE en lugar del DTE normal que se utiliza en el otro router. Por lo tanto, la conexión entre los routers debe hacerse mediante un cable DCE y un cable DTE entre los routers. Se usa un cable V.35 DCE y un cable V.35 DTE para simular la conexión de WAN.

d. Características del cable V. 35

El conector V.35 DCE es un conector hembra grande de V.35 (34 pins). El cable DTE tiene un conector macho grande de V.35. Los cables también se rotulan como DCE o DTE en el extremo del router del cable. Use el cable DCE en el Router A, dado que proporcionará la señal de temporización.

DTE	DCE
	

Paso 7: Realizar el cableado de los enlaces de WAN del router

a. Configuración del router

El router A debe ser preconfigurado por el instructor o asistente de laboratorio para proporcionar la señal de temporización de DCE en la interfaz Serial 0. La interfaz Serial 0 en cada router debe tener la dirección IP y máscara de subred correctas, tal como se indica en la tabla siguiente. La red que interconecta las interfaces seriales del router es 192.168.3.0.

Router	Temporización	Dirección IP de la interfaz S0	Máscara de subred
Router – A	DCE	192.168.3.1	255.255.255.0
Router – B	DTE	192.168.3.2	255.255.255.0

b. Conexión de los cables

El cable DCE se conecta a la interfaz Serial 0 en el Router A. El cable DTE se debe conectar a la interfaz Serial 0 en el Router B. Primero se debe hacer la conexión entre los dos cables V.35. Sólo hay una manera correcta de interconectar los cables. Alinee los pins del cable macho con los receptáculos de los cables hembra y acóplelos cuidadosamente. Cuando estén conectados, apriete los tornillos en el sentido de las agujas del reloj para asegurar los conectores.
Haga la conexión a cada uno de los routers. Sosteniendo el conector en una mano, oriente correctamente el conector del cable y el del router para que las clavijas coincidan. Empuje parcialmente el conector del cable hacia dentro del conector del router y apriete los tornillos para insertar totalmente el cable en el conector.

Paso 8: Configurar los valores de IP de la estación de trabajo

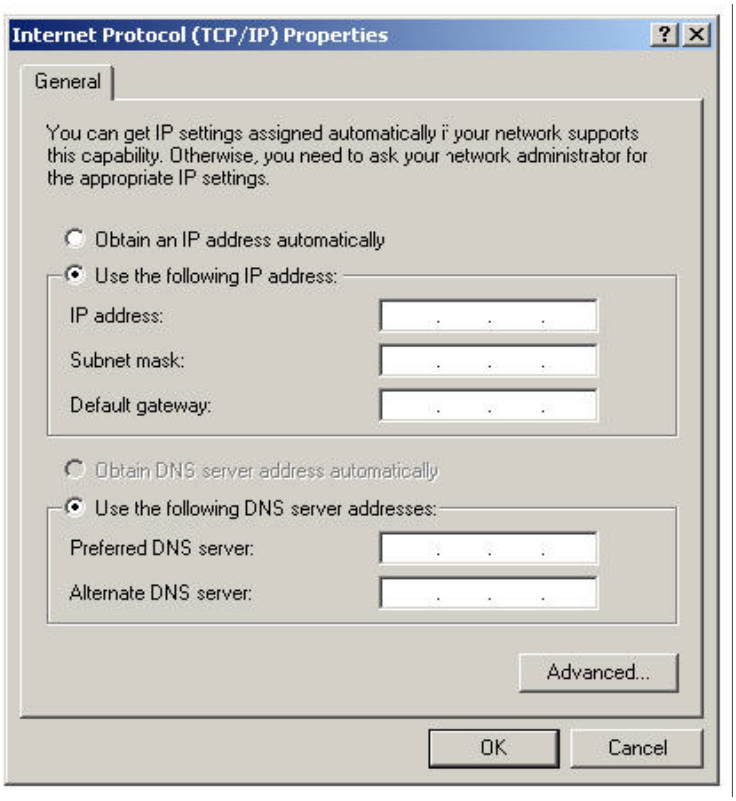
Nota: Anote los valores existentes de IP, para poder restaurarlos al final del laboratorio. Estos valores incluyen la dirección IP, la máscara de subred, el gateway por defecto y los servidores DNS. Si la estación de trabajo es un cliente DHCP, no es necesario registrar esta información.

Acceso a la ventana de Configuración IP.

Los usuarios de Windows XP/2003 profesional deben hacer lo siguiente:

- Haga clic en **Inicio** > **Configuraciones** > **Panel de control** y haga clic en el icono **Conexiones de red**.
- Seleccione **Conexión de área local** y haga clic en **Cambiar la configuración de esta conexión**.
- Seleccione el icono del **protocolo TCP/IP** asociado con la NIC de este PC.
- Haga clic en **Propiedades** y haga clic en **Usar la siguiente dirección IP**.

Vea el ejemplo siguiente.



Configure la información de la dirección IP para cada PC según la información en la tabla. Observe que la dirección IP de cada PC se encuentra en la misma red que el gateway por defecto, que es la interfaz de Ethernet del router conectado. El gateway por defecto se requiere en las redes de área local que están conectadas a un router.

Computador	**Dirección IP**	**Máscara de subred**	**Gateway por defecto**
PC – A	192.168.1.2	255.255.255.0	192.168.1.1
PC – B	192.168.2.2	255.255.255.0	192.168.2.1

Paso 9: Verificar si los PC se pueden comunicar por la WAN

a. Acceder al Símbolo del sistema (similar a MS-DOS):

Los usuarios de Windows XP/2003 profesional deben hacer lo siguiente:

Inicio > Programas > Accesorios > Símbolo del sistema

b. Probar la conectividad

Haga ping a la dirección IP del computador en la otra LAN. Introduzca el comando siguiente en la ventana de comandos.

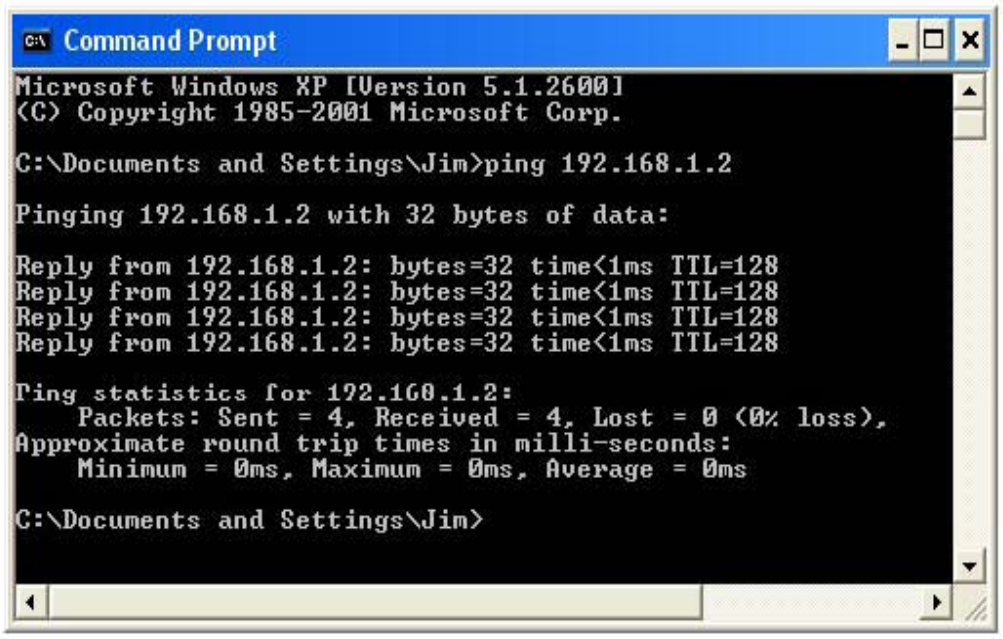
C:>ping 192.168.1.2

Esto verifica la conectividad IP desde una estación de trabajo a través de su switch y router por el enlace de WAN y a través del otro router y switch hasta el otro PC.

c. Fíjese si los resultados son similares a los que aparecen a continuación. De lo contrario, verifique las conexiones de los PC y las configuraciones de TCP/IP en ambos PC. ¿Cuál fue el resultado de ping?

_____

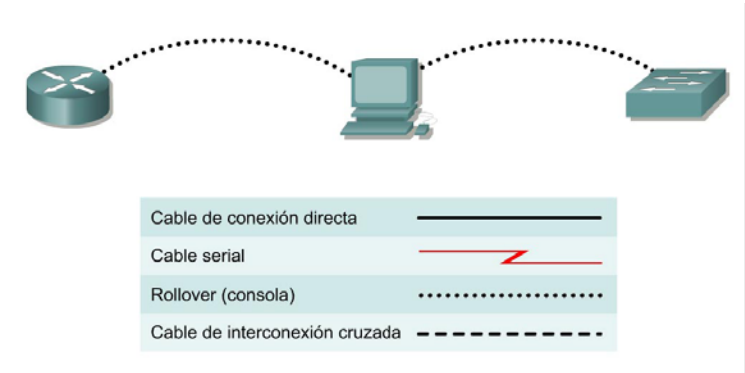
_____



Paso 10: Restaure los valores originales de IP de los PC, desconecte el equipo y guarde los cables.

2.3 Laboratorio

CONEXIÓN DE CONSOLA A UN ROUTER O SWITCH



Objetivo

- Crear una conexión de consola desde un PC a un router y switch con el cable correcto
- Configurar HyperTerminal en el PC
- Observar la interfaz del usuario del router y el switch

Tiempo estimado

30 minutos

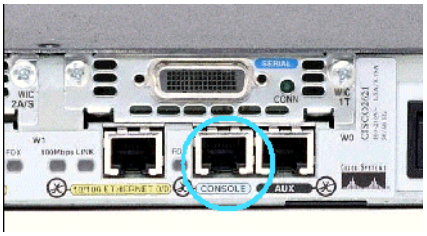
Información básica

Este laboratorio se ocupa de la capacidad para conectar un PC a un router o switch para establecer una sesión de consola y observar la interfaz del usuario. Una sesión de consola permite que el usuario verifique o cambie la configuración del switch o router y es el método más simple para conectarse a uno de estos dispositivos.
Este laboratorio debe realizarse dos veces, una vez con un router y la otra con un switch para ver las diferencias entre las interfaces del usuario. Inicie este laboratorio con el equipo apagado y el cableado desconectado. Se trabaja en equipos de dos: uno de los miembros trabaja con el router y el otro con el switch. Serán necesarios los siguientes recursos:

- Una estación de trabajo con una interfaz serial e HyperTerminal instalado
- Un switch de Ethernet 10BASE-T o de Fast Ethernet
- Router Cisco
- Cable rollover o de consola para conectar la estación de trabajo al router o switch

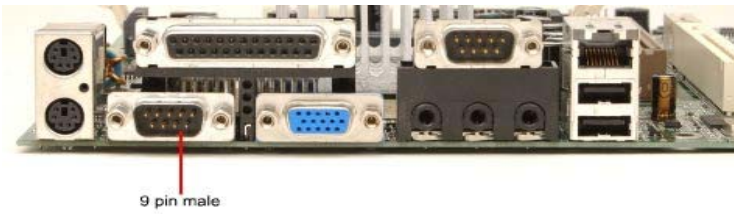
Paso 1: Identificar los conectores de consola del router/switch

a. Examine el router o switch y ubique el conector RJ-45 rotulado “Console” (Consola).



Paso 2: Identificar la interfaz serial del computador, que es COM 1 ó 2

a. Debe ser un conector macho de 9 ó 25 pins rotulado serial o COM1. Es posible que no tenga identificación.



Paso 3: Ubicar el adaptador RJ-45 a DB-9

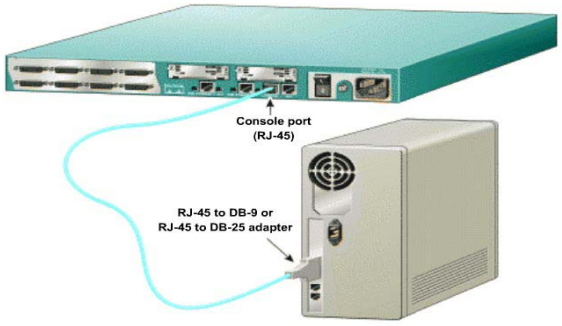
Un lado del adaptador se conecta a la interfaz serial del PC y el otro al conector de cable rollover RJ-45. Si la interfaz serial del PC o la terminal no inteligente es DB-25, se necesita un adaptador RJ-45 a DB-25. Ambos adaptadores vienen normalmente con un router o switch Cisco.

Paso 4: Buscar o preparar un cable rollover

Use un cable rollover. De ser necesario, prepare uno con la longitud adecuada para conectar el router o switch a una estación de trabajo.

Paso 5: Conectar los componentes de cableado

Conecte el cable rollover al conector RJ-45 del puerto de consola del router o switch. A continuación, conecte el otro extremo del cable rollover al adaptador RJ-45 a DB-9 o DB-25. Por último, conecte el adaptador a un puerto serial de PC, ya sea DB-9 o DB-25, según el computador.



Paso 6: Iniciar el programa HyperTerminal en el PC

a. Encienda el computador.

b. En la barra de tareas de Windows, busque el programa **HyperTerminal**:

Inicio > **Programas** > **Accesorios** > **Comunicaciones** > **Hyper Terminal**

Paso 7: Indicar un nombre para la sesión de HyperTerminal

En la ventana emergente "Descripción de la conexión" introduzca un nombre en el campo Nombre de la conexión y seleccione **Aceptar**.

Nota: cada uno de estos iconos juega el mismo papel, cada uno de ellos guardará un tipo de conexión diferente, es decir un usuario podrá configurar diferentes tipos de conexión y para cada tipo eligirá un icono diferente en cual guardarlo.

Paso 8: Especificar la interfaz de conexión del computador

En la ventana emergente "Conectar a", use la flecha desplegable junto al campo Conectar Usando para seleccionar **COM1** y seleccione **Aceptar**:
Nota: Según el puerto serial utilizado en el PC, puede ser necesario seleccionar el valor **COM2**. Las otras dos opciones "TCP/IP" es para una conexión TCP/IP Ethernet y la otra es de acceso remoto a travez de un teléfono.

Paso 9: Especificar las propiedades de conexión de la interfaz

a. En la ventana emergente "Propiedades de COM1" use las flechas desplegables para seleccionar lo siguiente:

Bits por segundo = **9600 (**velocidad)
Bits de datos = **8 (**palabra o código)
Paridad = **Ninguna** (correción de errores)
Bits de parada = **1**
Control de flujo = **Ninguno** (control)

b. Seleccione **Aceptar**.

c. Cuando aparezca la ventana de sesión de HyperTerminal, encienda el router o switch. Si el router o switch ya está encendido, presione la tecla **Intro**. Debe haber una respuesta del router o switch. Si la hay, esto significa que la conexión se ha completado con éxito.

Paso 10: Observar la interfaz del router o switch

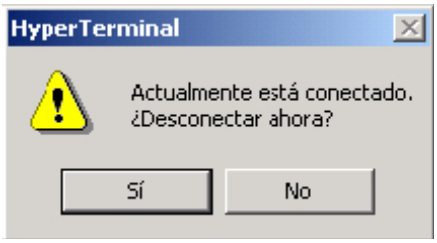
a. Observe la interfaz del usuario.
b. En el router, ¿cuál es el símbolo del sistema? _____
c. En el switch, ¿cuál es el símbolo del sistema? _____

Paso 11: Cerrar la sesión

a. Para terminar la sesión de consola desde la sesión de HyperTerminal, seleccione lo siguiente:

Archivo > Salir

b. Cuando aparezca la ventana de advertencia de desconexión de HyperTerminal, seleccione **Sí**.



c. El computador pregunta si se debe guardar la sesión. Seleccione **No**.

Paso 12: Apague el router o switch y guarde los cables

2.4 Laboratorio

DIRECCIONAMIENTO BÁSICO IP Y UTILIZACIÓN DE PROTOCOLO ARP

Objetivo

- Diferenciar las cinco clases distintas de direcciones IP
- Describir las características y el uso de las distintas clases de dirección IP
- Identificar la clase de una dirección IP según el número de red
- Determinar cuál de las partes u octetos de una dirección IP es el ID de red y cuál es el ID de host
- Identificar las direcciones IP de host válidas y no válidas basándose en las normas de direccionamiento IP
- Definir el rango de direcciones y máscaras de subred por defecto para cada clase
- Presentar el Protocolo de resolución de direcciones (ARP: Address Resolution Protocol) y comando de estación de trabajo **arp –a**.
- Explorar la función de ayuda del comando **arp** utilizando la opción **-?**

Tiempo estimado

45 minutos

Información básica

Esta primera parte del laboratorio lo ayudará a ampliar su comprensión acerca de las direcciones IP y de la forma en que operan las redes TCP/IP. Es en primer lugar un ejercicio de laboratorio escrito. Sin embargo, sería conveniente revisar algunas direcciones IP de red reales utilizando las utilidades de línea de comando **ipconfig**. Las direcciones IP se utilizan únicamente para identificar redes y hosts TCP/IP individuales como, por ejemplo, computadores e impresoras en dichas redes de manera que los dispositivos se puedan comunicar entre sí. Las estaciones de trabajo y los servidores en una red TCP/IP se denominan hosts y cada uno de ellos posee una dirección IP única. Esta dirección se conoce como dirección de host. TCP/IP es el protocolo que se utiliza más ampliamente a nivel mundial. Internet o la World Wide Web usan sólo el direccionamiento IP. Para que un host pueda acceder a Internet, debe tener una dirección IP.

En su forma básica, la dirección IP consta de dos partes:

- Una dirección de red
- Una dirección de host

El Internet Network Information Center (InterNIC: Centro de Información de la Red de Internet) asigna la parte de red de la dirección IP a una empresa u organización. Los routers usan la dirección IP para desplazar paquetes de datos entre redes. Las direcciones IP tienen una

longitud de 32 bits, de acuerdo con la versión actual IPv4, y se dividen en 4 octetos de 8 bits cada uno.
Operan en la capa de red (Capa 3) del modelo de Interconexión de Sistema Abierto (OSI: Open System Interconnection), que es la capa de Internet del modelo TCP/IP. Las direcciones IP se asignan de la siguiente manera:

- En forma estática: manualmente, a través de un administrador de red
- En forma dinámica: automáticamente, a través de un servidor de Protocolo de Configuración de Host Dinámico (DHCP: Dynamic Host Configuration Protocol)

La dirección IP de una estación de trabajo o host es una dirección lógica, lo que significa que se puede modificar. La dirección de Control de Acceso al Medio (MAC: Media Access Control) de la estación de trabajo es una dirección física de 48 bits. Esta dirección se graba en la tarjeta de interfaz de red (NIC) y no se pude cambiar a menos que la NIC sea reemplazada. La combinación de la dirección IP lógica y de la dirección MAC física ayuda a enrutar paquetes hacia el destino correcto.
Hay cinco clases distintas de direcciones IP y, según la clase, la parte de la dirección que corresponde a la red y al host usa distintos números de bits. En este laboratorio, se trabajará con distintas clases de dirección IP para ayudar a familiarizarse con las características de cada una de ellas. La comprensión de las direcciones IP es fundamental para comprender TCP/IP y las interconexiones de redes en general. Se necesitan los siguientes recursos:

- Estación de trabajo PC con Windows XP/2003 profesional instalado
- Acceso a la calculadora de Windows

Paso 1: Revisión de las clases de dirección IP y sus características

Clases de dirección

Existen cinco clases de direcciones IP, de la A a la E. Sólo las tres primeras clases se utilizan comercialmente. Se elige una dirección de red de clase A en la tabla para empezar. La primera columna es la clase de dirección IP. La segunda columna es el primer octeto que se debe ubicar dentro del rango indicado para una clase de dirección determinada. La dirección Clase A debe comenzar con un número entre 1 y 126. El primer bit de una dirección clase "A" siempre es un cero, lo que significa que no se puede usar el bit más significativo (HOB) o bit 128. 127 se reserva para pruebas de loopback. El primer octeto por sí solo define el ID de red para una dirección de red clase A

Máscara de subred por defecto

La máscara de subred por defecto usa exclusivamente unos binarios (255 decimal) para enmascarar los primeros 8 bits de la dirección clase A. La máscara de subred por defecto ayuda a los routers y hosts a determinar si el host destino está ubicado en esta red o en otra. Dado que hay sólo 126 redes clase A, los 24 bits restantes, o 3 octetos, se pueden usar para los hosts. Cada red clase A puede tener 2_{24}, o sea, más de 16 millones de hosts. Es común subdividir la red en grupos más pequeños denominados subredes usando una máscara de subred personalizada, que se describirá en el siguiente laboratorio.

Dirección de red y de host

La parte de la dirección que corresponde a la red o al host no puede estar formada exclusivamente por unos o por ceros. Como ejemplo, la dirección clase A 118.0.0.5 es una dirección IP válida. La porción de red o los primeros 8 bits, que equivalen a 118, no consta sólo de ceros y la porción de host o los últimos 24 bits, no consta de todos ceros o unos. Si la parte que corresponde al host estuviera constituida exclusivamente por ceros, ésta sería la dirección de red misma. Si la porción de host fuera igual a todos unos, sería un broadcast para la dirección de red. El valor de cualquiera de los octetos nunca puede ser superior al 255 decimal o al 11111111 binario.

Clase	**Clase Rango decimal del 1er octeto**	**Bits de orden superior del 1er octeto**	**ID de Red/Host (N=Red, H=Host)**	**Máscara de subred por defecto**	**Cantidad de redes**	**Hosts por red (direcciones utilizables**
A	1 – 126 *	0	N.H.H.H	255.0.0.0	126(2^7-2)	16,777,214(2^{24}-
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382(2^{14}-2)	65,534(2^{16}-2)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150(2^{21}-	254(2^8-2)
D	224 – 239	1110	Reservado para multicast			
E	240 – 254	11110	Experimental; utilizado para investigación			

Nota: La dirección 127 clase A no se puede utilizar y está reservada para funciones de loopback y diagnóstico.

Paso 2: Determinar el direccionamiento IP básico

Utilice el esquema de dirección IP y su conocimiento de clases de dirección IP para contestar las siguientes preguntas:

1. ¿Cuál es el rango decimal y binario del primer octeto de todas las direcciones IP de clase B posibles?
   Decimal: Desde: _____ Hasta: _____
   Binario: Desde: _____ Hasta: _____

2. ¿Qué octeto u octetos representan la parte que corresponde a la red de una dirección IP Clase C? _____

3. ¿Qué octeto u octetos representan la parte que corresponde al host de una dirección IP clase A? _____

4. ¿Cuál es el número máximo de hosts que se puede utilizar con una dirección de red de clase C? _____

5. ¿Cuántas redes de clase B hay? _____

6. ¿Cuántos hosts puede tener una red de Clase B? _____

7. ¿Cuántos octetos hay en una dirección IP? ¿_____Cuántos bits hay por octeto? _____

Paso 3: Determinar las porciones de host y de red de la dirección IP

Con las siguientes direcciones de host IP, indicar lo siguiente:

- Clase de cada una de las direcciones
- Dirección o ID de red
- Porción de host
- Dirección de broadcast para esta red
- Máscara de subred por defecto

La porción de host será todos ceros para el ID de red. Introduzca sólo los octetos que configuran el host. La porción de host será de todos unos para un broadcast. La porción de red de la dirección será de todos unos para la máscara de subred. Complete la siguiente tabla:

Dirección IP del host	**Clase de dirección**	**Dirección de red**	**Dirección de host**	**Dirección de broadcast de red**	**Máscara de subred por defecto**
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Paso 4: Dada una dirección IP de 142.226.0.15 y una máscara de subred de 255.255.255.0,

Conteste las siguientes preguntas:

¿Cuál es el equivalente binario del segundo octeto?

_____

¿Cuál es la clase de la dirección?

_____

¿Cuál es la dirección de red de esta dirección IP?

_____

¿Es ésta una dirección IP de host válida (S/N)?

_____

¿Por qué o por qué no?

_____

Paso 5: Determinar qué direcciones IP del host son válidas para las redes comerciales.

Para las siguientes direcciones IP de host, determine cuáles son válidas para redes comerciales e indique por qué o por qué no. Válido significa que se puede asignar a cualquiera de las siguientes opciones:

- Estación de trabajo
- Servidor
- Impresora
- Interfaz de router
- Cualquier otro dispositivo compatible

Complete la siguiente tabla:

Dirección IP de host	**¿Dirección válida? (Sí / No)**	**¿Por qué o por qué no?**
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		

Utilización del protocolo ARP

Información básica

El protocolo ARP se utiliza como herramienta para confirmar que un computador está resolviendo con éxito la transmisión de las direcciones de la Capa 3 de red a las direcciones de la Capa 2 del Control de acceso al medio (MAC). El protocolo de red TCP/IP se basa en direcciones IP como por ejemplo 192.168.14.211 para identificar dispositivos individuales y ayudar a los paquetes de datos a navegar entre las redes. Aunque la dirección IP es esencial para desplazar los datos de una LAN a otra, no puede entregar los datos en la LAN de destino por sí sola. Los protocolos de red locales como, por ejemplo, Ethernet o Token Ring, utilizan la dirección MAC o la Capa 2 para identificar los dispositivos locales y entregar todos los datos. La dirección MAC de computador se ha visto en laboratorios.
Este es un ejemplo de dirección MAC:

- **00-02-A5-9A-63-5C**

Una dirección MAC es una dirección de 48 bits que se visualiza en formato hexadecimal (HEX) como seis series de dos caracteres HEX separados por guiones. En este formato, cada símbolo hexadecimal representa 4 bits. Con algunos dispositivos, los 12 caracteres hexadecimales se pueden ver como tres series de cuatro caracteres separados por puntos o signos de dos puntos (0002.A59A.635C).

ARP mantiene una tabla en el computador de las combinaciones de direcciones IP y MAC. En otras palabras, mantiene un seguimiento de la dirección MAC que está asociada con una dirección IP. Si ARP no conoce la dirección MAC de un dispositivo local, emite un broadcast utilizando la dirección IP. Este broadcast busca la dirección MAC que corresponde a la dirección IP. Si la dirección IP está habilitada en la LAN, enviará una respuesta a partir de la cual ARP extraerá la dirección MAC. ARP agregará luego la combinación de direcciones a la tabla ARP local del computador que realiza la petición.

Las direcciones MAC y, por lo tanto, ARP sólo se utilizan dentro de la LAN. Cuando un computador prepara un paquete para su transmisión, verifica la dirección IP de destino para comprobar si forma parte de la red local. Lo hace verificando si la porción de red de la dirección IP es la misma que la de la red local. Si es así, el proceso ARP se consulta para obtener la dirección MAC del dispositivo de destino utilizando la dirección IP. La dirección MAC se aplica entonces al paquete de datos y se utiliza para el envío.

Si la dirección IP de destino no es local, el computador necesitará la dirección MAC del gateway por defecto. El gateway por defecto es la interfaz de router a la cual se encuentra conectada la red local para brindar conectividad con otras redes. La dirección MAC del gateway se utiliza porque el paquete será enviado allí y luego el router lo enviará a la red de destino.

Si el computador no recibe ningún paquete de una dirección IP luego de algunos minutos, dejará de lado la entrada MAC/IP de la tabla ARP suponiendo que el dispositivo ha sido desconectado.

Intentos posteriores de acceder a la dirección IP llevarán a ARP a realizar otro broadcast y a actualizar la tabla.

Esta segunda parte del laboratorio puede realizarse con cualquier versión de Windows. Esta es un laboratorio no destructivo que puede hacerse en cualquier máquina sin que se produzcan cambios en la configuración del sistema. La mejor manera de realizar este laboratorio es en un aula de clase o en cualquier otra LAN conectada a Internet. Puede realizarse desde una sola conexión remota a través de un módem o conexión de tipo DSL.

Paso 1: Establecer una conexión de red

Si la conexión a Internet es de acceso telefónico, es necesario conectarse al ISP para asegurarse de que el computador tenga una dirección IP. En una LAN TCP/IP con un servidor de Protocolo de configuración de host dinámico (DHCP) no es necesario realizar este paso.

Paso 2: Acceder al símbolo de sistema

Usuarios de Windows XP/2003 profesional:

Utilice el menú Inicio para abrir la ventana Símbolo de sistema. Esta ventana es similar a la ventana MS-DOS de las versiones Windows más antiguas:

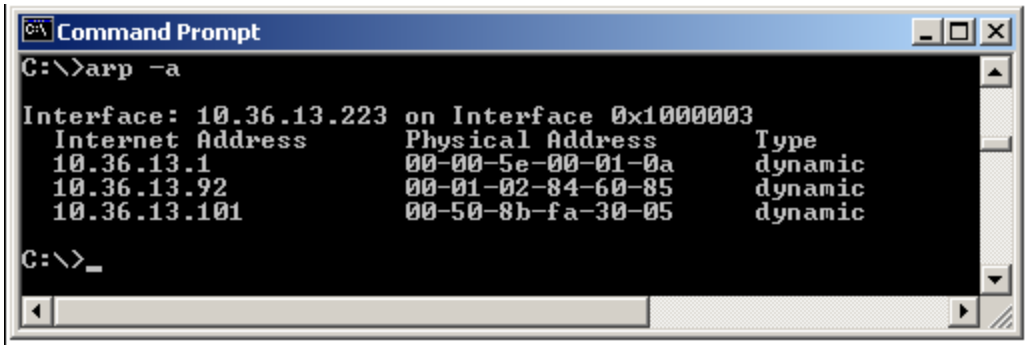
Presione **Inicio** > **Programas** > **Accesorios** > **Símbolo del sistema** o **Inicio** > **Programas** > **Símbolo del sistema**.

Paso 3: Mostrar la tabla ARP

a. En la ventana escriba **arp -a** y presione **Intro**. No se sorprenda si no existe ninguna entrada. El mensaje que aparecerá será probablemente: 'No ARP Entries Found' (No se encontraron entradas ARP). Los computadores que poseen Windows eliminan todas las direcciones que no se utilizan después de un par de minutos.

b. Trate de utilizar el comando ping con algunas de las direcciones locales y el URL de un sitio web. Luego vuelva a ejecutar el comando. La figura que aparece a continuación muestra un resultado posible del comando **arp -a**. La dirección MAC para el sitio web aparecerá en una lista porque no es local, pero esto hará que el gateway por defecto aparezca también en la lista.
En el ejemplo que aparece a continuación, 10.36.13.1 es el gateway por defecto mientras que 10.36.13.92 y 10.36.13.101 son otros computadores de red. Observe que por cada dirección IP existe una dirección física o MAC, y un tipo que indica cómo se enteró de la dirección.

c. A partir de la siguiente figura, se podría concluir lógicamente que la red es 10.36.13.0 y los computadores host están representados por 22, 1, 92 y 101.



Paso 4: Haga ping en varios URL

a. Haga ping en los siguientes URL y anote la dirección IP de cada uno de ellos. Además, seleccione un URL adicional en el que hacer ping y regístrelo más abajo:

www.cisco.com : _____
www.msn.de : _____
_____ : _____

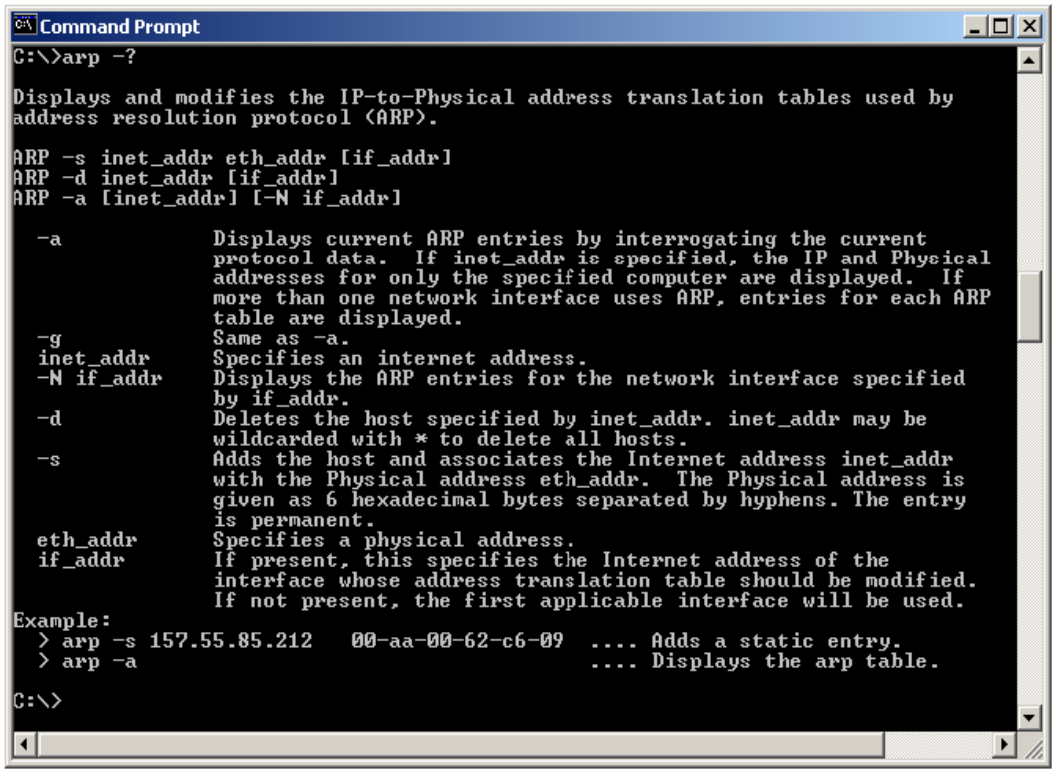
b. Ahora ejecute nuevamente el comando **arp –a** y registre las direcciones MAC de cada una de las direcciones anteriores, al lado de sus direcciones IP. ¿Se puede hacer esto?
_____

c. ¿Por qué o por qué no? _____
_____

d. ¿Qué dirección MAC se utilizó para entregar cada uno de los pings a los URL? _____
_____ ¿Por qué? _____

Paso 5: Utilizar la función de ayuda de ARP

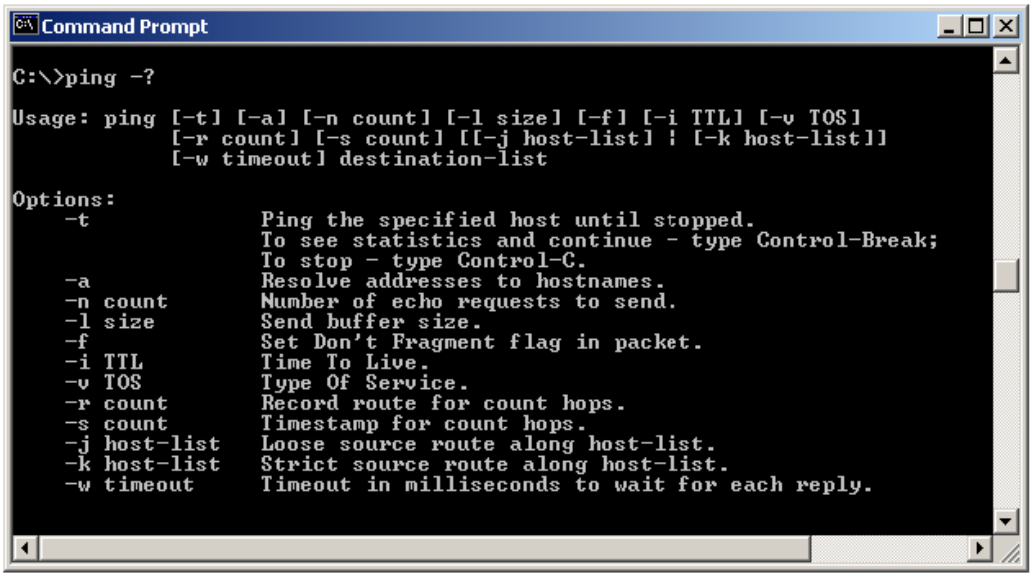
Use el comando **arp -?** para ver la función de ayuda y consulte las opciones.



El propósito de este paso no es tanto analizar las opciones de comando ARP sino mostrar cómo se usa **?** para acceder a la ayuda, en caso de que sea necesario. La ayuda no siempre se implementa de manera uniforme. Algunos comandos utilizan /? en lugar de - ?.

Paso 6: Utilizar la ayuda con los comandos tracert y ping

Use los comandos **tracert -?** y luego **ping -?** para ver las opciones disponibles para los comandos previamente utilizados.



Al examinar la ayuda para hacer ping, observe que existe una opción –t, que enviará pings continuos, no solamente cuatro. Más importante aún, observe que existen dos comandos para detener el proceso:

- **Control-Break**
- **Control-C**

Estos comandos de dos teclas se utilizan con frecuencia para detener las actividades que se encuentran fuera de control. Trate de hacer ping en un computador vecino seleccionando la opción - t y luego trate de usar las funciones Control-Break y Control-C. Un ejemplo en la red que nombramos anteriormente sería efectuar **ping 10.36.13.101 -t** y luego presionar **Intro**.

Asegúrese de utilizar el comando **Control-C** para detener los pings.

Reflexión

Basándose en las observaciones realizadas en el día de hoy, ¿qué se puede deducir de los siguientes resultados?

Computador 1

Dirección IP: 192.168.12.113
Máscara de subred: 255.255.255.0
Gateway por defecto: 192.168.12.1

Los Pings y tracert a 207.46.28.116 se realizaron con éxito.

¿Cuál será la entrada de tabla ARP asociada a esta dirección y por qué?

2.5 Laboratorio

INTRODUCCIÓN A CONCEPTOS DE SUBREDES

Objetivo

- Identificar las razones para utilizar una máscara de subred
- Distinguir entre una máscara de subred por defecto y una máscara de subred personalizada
- Saber qué requisitos determinan la máscara de subred, la cantidad de subredes y la cantidad de hosts por subred
- Entender el concepto de las subredes utilizables y la cantidad de hosts utilizables
- Utilizar el proceso AND para determinar si una dirección IP de destino es local o remota
- Identificar direcciones IP de host válidas e inválidas basadas en un número de red y una máscara de subred
- Analizar una dirección de red Clase A con el número de bits de red especificado a fin de determinar lo siguiente:
  - Máscara de subred
  - Número de subredes
  - Hosts por subred
  - Información acerca de subredes específicas
- Proporcionar un esquema de división en subredes utilizando una red Clase B.
- Proporcionar un esquema de división en subredes utilizando una red Clase C.

Tiempo estimado

45 minutos

Información básica para División en subredes

En este laboratorio, aprenderá los conceptos básicos de las máscaras de subred IP y su uso con las redes TCP/IP. La máscara de subred se puede utilizar para dividir una red existente en subredes. Algunas de las razones principales para realizar la división en subredes son las siguientes:

- Reducir el tamaño de los dominios de broadcast, creando pequeñas redes con menos tráfico
- Permitir que las LAN en distintas ubicaciones geográficas se comuniquen a través de los routers
- Proporcionar seguridad mejorada separando una LAN de otra

Los routers separan las subredes y determinan cuándo un paquete puede ir de una subred a otra.
Cada router a través del cual pasa un paquete se considera un salto. Las máscaras de subred ayudan a las estaciones de trabajo, los servidores y los routers de una red IP a

determinar si el host de destino, para el paquete que desea enviar, se encuentra en su propia red o en otra red.

Las máscaras de subred personalizadas utilizan más bits que las máscaras de subred por defecto al pedir prestados estos bits de la porción del host de la dirección IP. Esto crea una dirección dividida en tres partes:

- La dirección de red original
- La dirección de subred conformada con los bits que se pidieron prestados
- La dirección de host conformada por los bits que quedaron después de pedir prestados algunos para las subredes

Paso 1: Revisar la estructura de direcciones IP

Si una organización tiene una dirección de red IP clase A, el primer octeto, o los 8 bits, se asignan y no cambian. La organización puede usar los 24 bits restantes para definir hasta 16.777.214 hosts en su red. Estos son muchos hosts. No es posible colocar todos estos hosts en una sola red física sin separarlos en routers y subredes.

Es normal que una estación de trabajo esté en una red o subred y que un servidor esté en otra.
Cuando la estación de trabajo necesita recuperar un archivo del servidor necesitará utilizar su máscara de subred para determinar la red o la subred en la cual se encuentra el servidor. El propósito de una máscara de subred es ayudar a los hosts y routers a determinar la ubicación de red donde se puede encontrar un host de destino. Consulte la tabla que se suministra a continuación para revisar la siguiente información:

- Clases de dirección IP
- Máscaras de subred por defecto
- El número de redes que se pueden crear con cada clase de dirección de red
- El número de hosts que se pueden crear con cada clase de dirección de red

Clase de dirección	Rango decimal del 1er octeto	Bits de mayor peso de 1er octeto	ID de Red/Host (N=Red, H=Host)	Máscara de subred por defecto	Numero de redes	Hosts por red (direcciones utilizables)
A	1 – 126 *	0	N.H.H.H	255.0.0.0	126(2^7-2)	16,777,214(2^{24}-2)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382(2^{14}-2)	65,534(2^{16}-2)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150(2^{21}-2)	254(2^8-2)
D	224 – 239	1110	Reservado para multicast			
E	240 – 254	11110	Experimental; utilizado para investigación			

** La dirección 127 clase A no se puede utilizar y está reservada para funciones de loopback y diagnóstico.*

Paso 2: Revisión del proceso "AND"

Los hosts y los routers utilizan el proceso AND para determinar si un host destino se encuentra o no en la misma red. El proceso AND se realiza cada vez que un host desea enviar un paquete a otro host en una red IP. Para conectarse a un servidor, se debe conocer la dirección IP del servidor o el nombre de host como, por ejemplo, http://www.cisco.com. Si el nombre de host se utiliza como Servidor de nombre de dominio (DNS), éste se convertirá en una dirección IP.

En primer lugar, el host origen comparará o realizará el proceso AND de su propia dirección IP con su propia máscara de subred. El resultado del proceso AND es identificar a la red donde se encuentra el host de origen. Luego comparará la dirección IP destino con su propia máscara de subred. El resultado del 2do proceso AND será la red en la cual se encuentra activado el host destino. Si la dirección de red origen y la dirección de red destino son las mismas, se pueden comunicar directamente. Si los resultados son distintos, se encuentran en distintas redes o subredes. Si este es el caso, el host origen y el host destino necesitarán comunicarse a través de routers o no podrán tener ningún tipo de comunicación entre sí.
El proceso AND depende de la máscara de subred. Las máscaras de subredes siempre usan 1s para indicar la porción de red o la de red y subred de una dirección IP. La máscara de subred por defecto para una red Clase C es 255.255.255.0 ó 11111111.11111111.11111111.00000000.

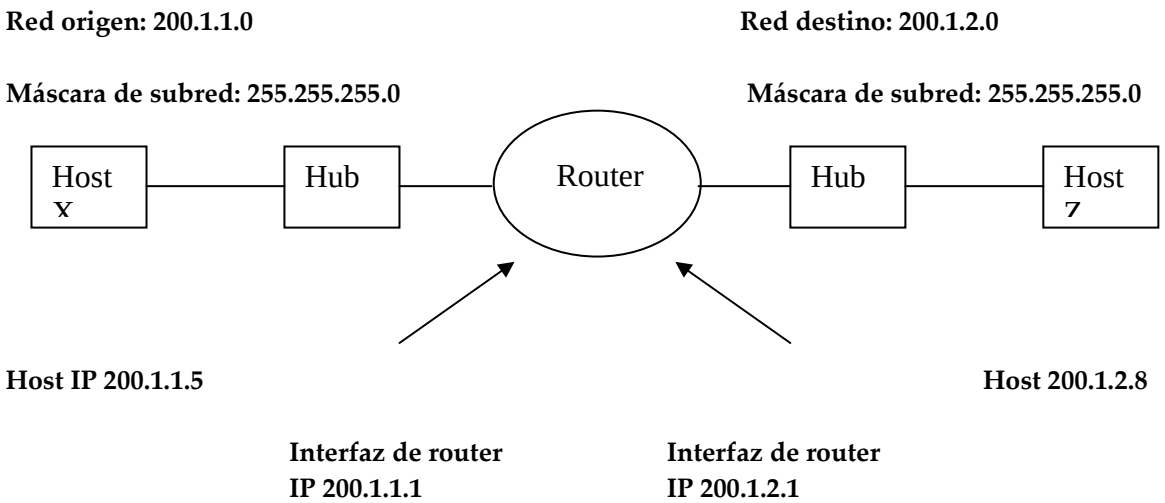
Esto se compara bit a bit con la dirección IP origen. El primer bit de la dirección IP se compara con el primer bit de la máscara de subred, el segundo bit con el segundo bit, y así hasta el final. Si los dos bits son unos, el resultado del proceso AND es un uno. Si los dos bits son cero y uno, o dos ceros, el resultado del proceso AND es un cero. Básicamente, esto

significa que una combinación de 2 unos da como resultado un uno; cualquier otro resultado es un cero. El resultado del proceso AND es la identificación del número de red o subred en el cual la dirección origen o destino se encuentra activada.

Paso 3: Dos redes Clase C que utilizan la máscara de subred por defecto

Este ejemplo muestra cómo una máscara de subred por defecto clase C puede utilizarse para determinar en qué red se encuentra un host activado. Una máscara de subred por defecto no divide una dirección en subredes. Si se utiliza la máscara de subred por defecto, la red no se divide en subredes. El host X, el origen en la red 200.1.1.0, tiene una dirección IP de 200.1.1.5. Desea enviar un paquete al host Z, el destino en la red 200.1.2.0 y tiene una dirección IP 200.1.2.8. Todos los hosts de cada red se conectan a hubs o switches y luego a un router. Recuerde que con una dirección de red clase C, los primeros 3 octetos, o 24 bits, se asignan como la dirección de red. Por lo tanto, estas son dos redes clase C diferentes. Esto deja un octeto u 8 bits para hosts, de manera que cada red clase C pueda tener hasta 254 hosts:

- $2_8 = 256 - 2 = 254$



El proceso AND ayuda a que el paquete llegue desde el host 200.1.1.5 de la red 200.1.1.0 hasta el host 200.1.2.8 de la red 200.1.2.0 siguiendo estos pasos:

1. El host X compara su propia dirección IP con su propia máscara de subred utilizando el proceso AND.

   Dirección IP del host X 200.1.1.5 11001000.00000001.00000001.00000101

   Máscara de subred 255.255.255.0 11111111.11111111.11111111.00000000

   Resultado de AND (200.1.1.0) 11001000.00000001.00000001.00000000

   Nota: El resultado del proceso AND es la dirección de red del host X, que es 200.1.1.0.

2. Luego, el host X compara la dirección IP del host Z destino con su propia máscara de subred utilizando el proceso AND.

   Dirección IP del Host Z 200.1.2.8 11001000.00000001.00000010.00001000
   Máscara de subred 255.255.255.0 11111111.11111111.11111111.00000000
   Resultado de AND (200.1.2.0) 11001000.00000001.00000010.00000000

   Nota: El resultado del proceso AND es la dirección de red del host Z, que es 200.1.2.0.

   El host X compara los resultados del proceso AND del Paso1 con los resultados del proceso AND del Paso 2 y observa que son diferentes. El host X ahora sabe que el host Z no se encuentra en su red de área local (LAN). Por lo tanto, debe enviar el paquete a su gateway por defecto, que es la dirección IP de la interfaz del router de 200.1.1.1 en la red 200.1.1.0. El router luego repite el proceso AND para determinar a qué interfaz de router deberá enviar el paquete.

Paso 4: Una red Clase C que utiliza una máscara de subred personalizada

En este ejemplo se utiliza una sola dirección de red Clase C (200.1.1.0) y se muestra cómo se puede utilizar una máscara de subred Clase C personalizada para determinar cuál es la subred en la que está ubicado un host y cómo enrutar paquetes desde una subred a otra. Recuerde que con una dirección de red clase C, los primeros 3 octetos, o 24 bits, se asignan como la dirección de red.
Esto permite dejar un octeto, u 8 bits, para los hosts. Por lo tanto, cada red clase C puede tener hasta 254 hosts:

- $2_8 = 256 – 2 = 254$

Quizás se deseen menos de 254 hosts, estaciones de trabajo y servidores combinados en una red.
Esto podría ser por razones de seguridad o para reducir el tráfico. Esto se puede realizar creando dos subredes y separándolas con un router. De esta manera, se crean dominios de broadcast independientes más pequeños y se logra mejorar el rendimiento de la red y aumentar la seguridad.
Esto es posible porque estas subredes quedan separadas por uno o más routers. Haga de cuenta que se necesitarán por lo menos dos subredes y que habrá por lo menos 50 hosts por subred. Dado que sólo hay una dirección de red clase C, sólo 8 bits en el cuarto octeto están disponibles para un total de 254 hosts posibles. Por lo tanto, se deberá crear una máscara de subred personalizada. La máscara de subred personalizada se utilizará para pedir prestados bits de la porción de host de la dirección. Los siguientes pasos ayudan a lograr este objetivo:

1. El primer paso consiste en realizar la división en subredes para determinar cuántas subredes se necesitan. En este caso, son dos subredes. Para ver cuántos bits se deben pedir prestados a la parte de la dirección de red que corresponde al host, sume los valores de bit de derecha a izquierda hasta que el total sea igual o mayor que la cantidad de subredes que se necesitan.

Dado que se necesitan dos subredes, sume el bit uno y el bit dos, lo que equivale a tres. Este número es mayor que el que se necesita para las subredes. Para solucionarlo, pida prestados al menos dos bits a la dirección de host empezando desde el lado izquierdo del octeto que contiene la dirección de host.

Dirección de red: 200.1.1.0

Bits de dirección de host del 4to octeto:	1	1	1	1	1	1	1	1
Valores de bit de dirección de host (desde la derecha)	128	64	32	16	8	4	**2**	**1**

Sume los bits empezando por la derecha, el 1 y el 2, hasta que la suma sea mayor que la cantidad de subredes que se necesitan.

Nota: Una forma alternativa de calcular la cantidad de bits que se deben pedir prestados para las subredes consiste en elevar la cantidad de bits prestados a la potencia 2. El resultado debe ser mayor que la cantidad de subredes que se necesitan. Como ejemplo, si se piden prestados 2 bits, el cálculo es dos a la potencia dos, que da como resultado cuatro. Como la cantidad de subredes que se necesitan es dos, esto debería ser suficiente.

2. Una vez que sabemos cuántos bits debemos pedir prestados, los tomamos desde la izquierda de la dirección de host, o sea, desde el 4to octeto. Cada bit que se pide prestado a los bits de la dirección de host deja menos bits para los hosts. Aun cuando la cantidad de subredes aumente, la cantidad de hosts por subred disminuye. Como se hace necesario pedir prestados dos bits de la parte izquierda, ese nuevo valor debe aparecer en la máscara de subred. La máscara de subred por defecto existente era 255.255.255.0 y la nueva máscara de subred personalizada es 255.255.255.192. El número 192 es el resultado de la suma de los primeros dos bits desde la izquierda, 128 + 64 = 192. Estos bits ahora se convierten en unos y forman parte de la máscara de subred total. Esto deja 6 bits para las direcciones IP del host o 2_6 = 64 hosts por subred.

Bits prestados del 4to octeto para la subred:	**1**	**1**	0	0	0	0	0	0
Valores de bit de subred: (desde la izquierda)	**128**	**64**	32	16	8	4	2	1

Con esta información, se puede crear la siguiente tabla. Los primeros dos bits son el valor binario de la subred.

Los últimos 6 bits son los bits del host. Pidiendo prestados 2 bits de los 8 bits correspondientes a las 4 subredes de la dirección de host, se pueden crear 2^2, con 64 hosts cada uno. Las 4 redes creadas son las siguientes:

- La red 200.1.1.0
- La red 200.1.1.64
- La red 200.1.1.128
- La red 200.1.1.192

La red 200.1.1.0 se considera inutilizable, a menos que el dispositivo de red admita el comando IOS **ip subnet-zero**, que permite el uso de la primera subred.

No. de subred	Valor binario de los bits de subred prestados	Valor decimal de los bits de subred	Valores binarios posibles de los bits de host (rango) (6 Bits)	Rango decimal de subred/host	¿Utilizable?
0 Subred	00	0	000000–111111	0–63	No
1ra Subred	01	64	000000–111111	64–127	Sí
2da Subred	10	128	000000–111111	28–191	Sí
3ra Subred	11	192	000000–111111	192–254	No

Observe que la primera subred empieza con 0 y, en este caso, aumenta de a 64, que es la cantidad de hosts que se encuentran en cada subred. Una forma de determinar el número de hosts en cada subred o el inicio de cada subred es elevar los bits de host restantes a la potencia 2. Dado que pedimos prestados dos de los 8 bits para subredes y nos quedan 6 bits, la cantidad de hosts por subred es 2_6 ó 64. Otra forma de determinar la cantidad de hosts por subred o el incremento de una subred a otra es sustrayendo el valor decimal de la máscara de subred, 192 en el cuarto octeto, de 256, que es la cantidad máxima de combinaciones posibles de 8 bits. Esto es igual a 64. Esto significa que se empieza en 0 en la primera red y se agrega 64 a cada subred adicional. Por ejemplo, si se utiliza la segunda subred, la red 200.1.1.64 no se puede utilizar para un ID de host dado que el ID de red de la subred 64 tiene todos ceros en la porción de host.

Otra forma común de representar una máscara de subred es utilizando el símbolo "barra diagonal y número" (/#), donde el símbolo # (Nº) después de la barra diagonal equivale a la cantidad de bits utilizados en la máscara (combinación de red y subred). Como ejemplo, una dirección de red clase C como, por ejemplo, 200.1.1.0 con una máscara de subred estándar (255.255.255.0) se escribiría como 200.1.1.0 /24, indicando que 24 bits se están utilizando para la máscara. La misma red, cuando se divide en subredes utilizando dos bits de host para las subredes, se escribiría 200.1.1.0 /26. Esto indica que 24 bits se utilizan para la red y 2 bits para la subred. Esto representa una máscara de subred personalizada de 255.255.255.192 en formato decimal punteado.
Una red clase A de 10.0.0.0 con una máscara estándar (255.0.0.0) se escribiría 10.0.0.0 /8. Si se utilizaran 8 bits (el siguiente octeto) para las subredes se escribiría 10.0.0.0 /16. Esto representaría una máscara de subred personalizada de 255.255.0.0 en formato decimal punteado. El número después de la "barra diagonal" que viene a continuación del número de red es un método abreviado que indica la máscara de subred que se está utilizando.

Paso 5: Utilice la siguiente información y los ejemplos anteriores para contestar las siguientes preguntas relacionadas con la subred

Una empresa ha presentado una solicitud para una dirección de red Clase C 197.15.22.0 que ha sido aprobada. La red física debe ser dividida en 4 subredes, las cuales quedarán interconectadas por routers. Se necesitarán al menos 25 hosts por subred. Se necesita utilizar una máscara de subred personalizada clase C y un router entre las subredes para enrutar los paquetes de una subred a otra. Determine el número de bits que se deben pedir

prestados de la porción del host de la dirección de red y el número de bits que quedarán para las direcciones de host.

Nota: Habrá 8 subredes posibles de las cuales 6 se podrán utilizar.

Complete la siguiente tabla y conteste las siguientes preguntas:

No. de subred	**Valor binario de los bits de subred prestados**	**Valor decimal de los bits de subred y N° de subred**	**Valores binarios posibles de los bits de host (rango) (5 Bits)**	**Rango decimal de subred/host**	**¿Uso?**
0 Subred					
1ra Subred					
2da Subred					
3ra Subred					
4ta Subred					
5ta Subred					
6ta Subred					
7ta Subred					

NOTAS:

_____

_____

_____

Utilice la tabla que acaba de completar para contestar las siguientes preguntas:

1. ¿Qué octeto u octetos representan la parte que corresponde a la red de una dirección IP Clase C? _____

2. ¿Qué octeto u octetos representan la parte que corresponde al host de una dirección IP Clase C? _____

3. ¿Cuál es el equivalente binario de la dirección de red Clase C en el ejemplo? **197.15.22.0**
   Dirección de red decimal: _____ _____ _____ _____
   Dirección de red binaria: _____ _____ _____ _____

4. ¿Cuántos bits de mayor peso se pidieron prestados de los bits de host en el cuarto octeto?
   _____

5. ¿Qué máscara de subred se debe utilizar? Mostrar la máscara de subred en valores decimales y binarios.
   Máscara de subred decimal: _____ _____ _____ _____
   Máscara de subred binaria: _____ _____ _____ _____

6. ¿Cuál es la cantidad máxima de subredes que se puede crear con esta máscara de subred?
   _____

7. ¿Cuál es la cantidad máxima de subredes utilizables que se puede crear con esta máscara?
   _____

8. ¿Cuántos bits quedaron en el cuarto octeto para los ID de host?
   _____

9. ¿Cuántos hosts por subred se pueden definir con esta máscara de subred?
   _____

10. ¿Cuál es la cantidad máxima de hosts que se puede definir para todas las subredes en esta situación? Haga de cuenta que los números mínimo y máximo de subred y el ID de host mínimo y máximo de cada subred no se pueden utilizar.
    _____

11. ¿Es 197.15.22.63 una dirección IP de host válida para este ejemplo?
    _____

12. ¿Por qué o por qué no?
    _____

13. ¿Es 197.15.22.160 una dirección IP de host válida para este ejemplo?
    _____

14. ¿Por qué o por qué no?
    _____-{}-

15. El host A tiene una dirección IP 197.15.22.126. El host B tiene una dirección IP 197.15.22.129. ¿Estos hosts están en la misma subred? _____ ¿Por qué?
    _____

Información básica para División en subredes de una red Clase A

Este es un ejercicio escrito y se debe realizar sin la ayuda de una calculadora electrónica.

Paso 1: Dada una dirección de red Clase A de 10.0.0.0 / 24 contesta las siguientes preguntas

¿Cuántos bits se pidieron prestados de la porción de host de esta dirección? _____

¿Cuál es la máscara de subred de esta red?

1. Decimal punteado

_____

2. Binario _____ _____ _____

_____

¿Cuántas subredes utilizables hay? _____

¿Cuántos hosts utilizables hay en cada subred?

_____

¿Cuál es el rango de host para la subred utilizable dieciséis?

_____

¿Cuál es la dirección de red para la subred utilizable dieciséis?

_____

¿Cuál es la dirección de broadcast para la subred utilizable dieciséis?

_____

¿Cuál es la dirección de broadcast para la última subred utilizable?

_____

¿Cuál es la dirección de broadcast para la red principal?

_____

Información básica para División en subredes de una red Clase B

Este es un ejercicio escrito y se debe realizar sin la ayuda de una calculadora electrónica.

La empresa ABC, S.A. ha adquirido una dirección Clase B, 172.16.0.0. La empresa necesita crear un esquema de división de subredes para ofrecer lo siguiente:

- 36 subredes con al menos 100 hosts
- 24 subredes con al menos 255 hosts
- 10 subredes con al menos 50 hosts

No es necesario suministrar una dirección para la conexión WAN dado que el proveedor de servicio de Internet la provee.

Paso 1: Teniendo en cuenta esta dirección de red Clase B y estos requisitos, conteste las siguientes preguntas

¿Cuántas subredes se necesitan para esta red?

_____

¿Cuál es el número mínimo de bits que se pueden pedir prestados?

_____

¿Cuál es la máscara de subred de esta red?

_____

1. Decimal punteado

_____

2. Binario _____ _____ _____

_____

3. Formato con barra diagonal

_____

¿Cuántas subredes utilizables hay?

_____

¿Cuántos hosts utilizables hay en cada subred?

_____

Paso 2: Complete la siguiente tabla haciendo una lista de las primeras tres subredes y las últimas 4 subredes

N° de subred	ID de subred	Rango de host	ID de broadcast

¿Cuál es el rango de host para la subred 2?

_____

¿Cuál es la dirección de broadcast para la subred 126?

_____

¿Cuál es la dirección de broadcast para la red principal?

_____

Información básica para división en subredes de una red Clase C

Este es un ejercicio escrito y se debe realizar sin la ayuda de una calculadora electrónica.
La Academia Clásica ha adquirido una dirección Clase C, 192.168.1.0. La academia necesita crear subredes para ofrecer seguridad de bajo nivel y control de broadcast en la LAN. No es necesario suministrar una dirección para la conexión WAN. La suministra el proveedor de servicio de Internet.
La LAN se compone de la siguiente manera, requiriendo cada uno de los componentes su propia subred:

- Aula de clase N°1 28 nodos
- Aula de clase N°2 22 nodos
- Laboratorio de informática 30 nodos
- Instructores 12 nodos
- Administración 8 nodos

Paso 1: Teniendo en cuenta esta dirección de red Clase C y estos requisitos, conteste las siguientes preguntas

¿Cuántas subredes se necesitan para esta red?

_____

¿Cuál es la máscara de subred de esta red?
1. Decimal punteado

_____

2. Binario _____ _____ _____

_____

3. Formato con barra diagonal

_____

¿Cuántos hosts utilizables se encuentran en cada subred?

_____

Paso 2: Complete la siguiente tabla

N° de subred	IP de subred	Rango de host	ID de broadcast

¿Cuál es el rango de host para la subred 6?

_____

¿Cuál es la dirección de broadcast para la subred 3?

_____

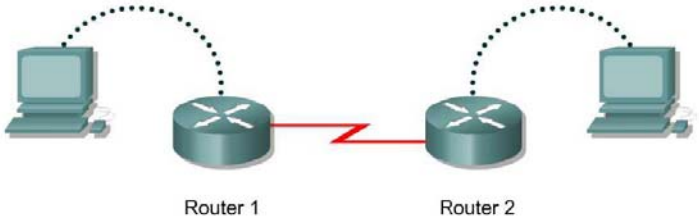
¿Cuál es la dirección de broadcast para la red principal?

_____

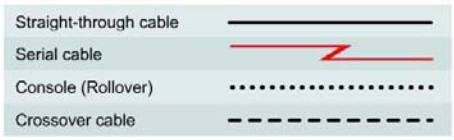
3. PRINCIPIOS BASICOS DE ROUTERS Y ENRUTAMIENTO

3.1 Laboratorio

CONFIGURACIÓN DE LAS INTERFACES DEL ROUTER



Designación del router	Nombre del router	Tipo de interfaz	Dirección Serial 0	Máscara de subred	Contraseña enable secret	Contraseñas enable/VTY/ Consola
Router 1	GAD	DCE	192.168.15.1	255.255.255.0	class	cisco
Router 2	BHM	DTE	192.168.15.2	255.255.255.0	class	cisco



Objetivo

- Configurar una interfaz serial en cada uno de los dos routers para que se puedan comunicar entre sí.
- Configurar algunos parámetros de router básicos.
- Activar o desactivar las interfaces.
- Realizar cambios en la configuración del router.
- Configurar una interfaz Ethernet en el router con una dirección IP y una máscara de subred.
- Elegir una descripción para una interfaz y utilizar el modo de configuración de interfaz para introducir esta descripción.

Tiempo estimado

45 minutos

Información básica

Se puede usar cualquier router que cumpla con los requisitos de interfaz. Consulte la tabla al final de este laboratorio para identificar correctamente los identificadores de interfaz que se deben usar según el equipo que se utiliza en el laboratorio. Los resultados de la configuración utilizados en este laboratorio se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos. Se recomienda

ejecutar los siguientes pasos en cada router a menos que se especifique lo contrario. Iniciar una sesión de HyperTerminal

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio.

Configuración de una interfaz serial

Paso 1: Configuración básica del router

a. Configure el router. Conecte los routers tal como aparece en el diagrama. Este laboratorio requiere un cable serial nulo y dos cables transpuestos o de consola.

Paso 2: Configurar el nombre y las contraseñas del Router 1

a. En el Router 1, entre al modo de configuración global y configure el nombre de host tal como aparece en la tabla.

b. Configure las contraseñas de consola, de la terminal virtual y de enable.

Paso 3: Configurar la Interfaz serial, Serial 0

En el modo de configuración global, configure la interfaz serial 0 en el router GAD.

Consulte el esquema de interfaz.

GAD(config)#**interface serial 0**
GAD(config-if)#**ip address 192.168.15.1 255.255.255.0**
GAD(config-if)#**clock rate 56000**
GAD(config-if)#**no shutdown**
GAD(config-if)#**exit**
GAD(config)#**exit**

Nota: Una vez que entre al modo de configuración de interfaz, anote la dirección IP de la interfaz. Introduzca la mascara de subred. Introduzca la velocidad del reloj solamente en el lado DCE del dispositivo. El comando **no shutdown** activa la interfaz. La interfaz se desactiva con Shutdown.

Paso 4: Guardar la configuración activa

Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

GAD#**copy running-config startup-config**

Nota: Guarde la configuración activa para la próxima vez que se reinicie el router. El router puede reiniciarse ya sea a través de un comando **reload** del software o

debido a un corte de energía. La configuración activa se perderá si no se guarda. El router utiliza la configuración inicial al arrancarse.

Paso 5: Mostrar información sobre la interfaz serial 0 en GAD

a. Introduzca el comando show interface serial 0 en GAD. Consulte el esquema de interfaz.

GAD#**show interface serial 0**

Aparecerán los detalles de la interfaz serial 0.

b. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

c. La interfaz Serial 0 está _____. El protocolo de línea es_____.

d. La dirección de Internet es _____.

e. Encapsulamiento _____

f. ¿A qué capa del modelo OSI se refiere el término "encapsulamiento"?
_____

g. Si la interfaz serial se ha configurado, ¿por qué **show interface serial 0** dice que la interfaz está desactivada?
_____

Paso 6: Configurar el nombre y las contraseñas del Router 2

a. En el router Birmingham, entre al modo de configuración global. Configure el nombre de host y las contraseñas de consola, de la terminal virtual y de enable como aparece en la tabla anterior.

Paso 7: Configurar la Interfaz Serial 0

En el modo de configuración de terminal, configure la interfaz serial 0 en el router BHM. Consulte el esquema de interfaz.

BHM(config)#**interface serial 0**
BHM(config-if)#**ip address 192.168.15.2 255.255.255.0**
BHM(config-if)#**no shutdown**
BHM(config-if)#**exit**
BHM(config)#**exit**

Paso 8: Guardar la configuración activa

Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

BHM#**copy running-config startup-config**

Paso 9: Mostrar información sobre la interfaz serial 0 en BHM

a. Introduzca el comando **show interface serial 0** en BHM. Consulte el esquema de interfaz.

BHM#**show interface serial 0**

Aparecerán los detalles de la interfaz serial 0.

b. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

c. La interfaz Serial 0 está _____, el protocolo de línea es _____ .

d. La dirección de Internet es _____.

e. Encapsulamiento _____

f. ¿Cuál es la diferencia en el estado de línea y de protocolo registrado anteriormente en GAD? ¿Por qué?

_____

Paso 10: Verificar que la conexión serial esté funcionando

a. Haga **ping** a la interfaz serial del otro router.

BHM#**ping 192.168.15.1**
GAD#**ping 192.168.15.2**

b. Desde GAD, haga ping a la interfaz serial del router BHM. ¿El ping funciona?

_____

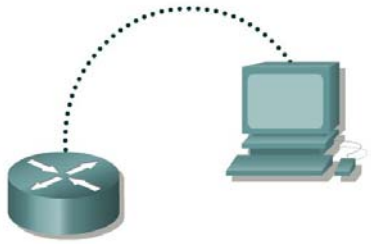
c. Desde BHM, haga ping a la interfaz serial del router GAD. ¿El ping funciona?

_____

d. Si la respuesta a cualquiera de las dos preguntas es no, realice un diagnóstico de fallas de las configuraciones del router para detectar el error. Luego, realice los pings nuevamente hasta que la respuesta a ambas preguntas sea sí.

Una vez completados los pasos anteriores, desconéctese escribiendo **exit** (salir). Apague el router. Quite y guarde los cables y el adaptador.

Cambios de configuración



Nombre del router	Tipo de router	Dirección Serial 0	Máscara de subred	Contraseña Enable Secret	Contraseñas enable/VTY/Consola
GAD		192.168.14.1	255.255.255.0	class	cisco

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio

Paso 1: Configuración básica del router

a. Conecte los routers tal como aparece en el diagrama. Este laboratorio requiere de un cable de consola (rollover) y un cable serial.

Paso 2: Configurar el nombre de host y las contraseñas

a. En el router GAD ingrese al modo de configuración global. Configure el nombre de host según lo indica la tabla. Configure las contraseñas de consola, de la terminal virtual y de enable.

Paso 3: Configurar la Interfaz Serial 0

a. En el modo de configuración de terminal, configure la interfaz serial 0 en el router GAD. Consulte el esquema de interfaz.

GAD(config)#**interface Serial 0**
GAD(config-if)#**ip address 192.168.14.1 255.255.255.0**
GAD(config-if)#**no shutdown**
GAD(config-if)#**description Connection to the host**
GAD(config-if)#**exit**
GAD(config)#**exit**

Nota: Una vez que entre al modo de configuración de interfaz, anote la dirección IP de la interfaz. Introduzca la máscara de subred. Introduzca la velocidad del reloj solamente en el lado DCE del dispositivo. El comando **no shutdown** activa la interfaz. La interfaz se desactiva con Shutdown.

Paso 4: Guardar la configuración

a. Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado.

GAD#**copy running-config startup-config**

Nota: Guarde la configuración activa para la próxima vez que se reinicie el router. El router puede reiniciarse ya sea a través de un comando **reload** del software o debido a un corte de energía. La configuración activa se perderá si no se guarda. El router utiliza la configuración inicial al arrancarse.

Paso 5: Verificar la configuración

a. Introduzca el comando **show running-config** del modo EXEC privilegiado

b. Si la configuración no es correcta, corrija los comandos incorrectos.

Paso 6: Modificar la configuración

a. Basándose en la nueva tabla, reconfigure el router GAD. Cambie el nombre de host del router. Cambie las contraseñas enable/vty/ consola. Elimine la contraseña secreta y la descripción de la interfaz. Para cambiar la información, vaya al modo de comando apropiado y vuelva a escribir el comando con la nueva información. Para eliminar un comando anterior, vaya al modo de comando adecuado y vuelva a escribir el comando exactamente como se ingresó con la palabra **no** delante. Por ejemplo:

GAD(config-if)#**description Connection to the host**
GAD(config-if)#**no description Connection to the host**

Nota: Antes de realizar algún cambio en la dirección IP y en la máscara de subred de la interfaz desactive la interfaz como se indica en el Paso 7.

Nombre Del router	**Dirección serial 0**	**Máscara de subred**	**Contraseña Enable secret**	**Contraseñas enable/VTY/Consola**
GAD	**172.16.0.1**	**255.255.0.0**		**Cisco1**

Paso 7: Desactivar la Interfaz serial 0

a. Desactive la interfaz para su mantenimiento introduciendo:

GAD(config)#**interface Serial 0**
GAD(config-if)#**shutdown**
GAD(config-if)#**exit**
GAD(config)#**exit**
GAD#

b. Introduzca show interface Serial 0 y verifique el estado de la interfaz.

c. Introduzca el comando **show running-config** y verifique el estado de la interfaz serial 0: _____

Paso 8: Activar la Interfaz serial 0

a. Para hacer que la interfaz se vuelva activa, habilite la interfaz introduciendo:

GAD(config)#**interface Serial 0**
GAD(config-if)#**no shutdown**
GAD(config-if)#**exit**
GAD(config)#**exit**

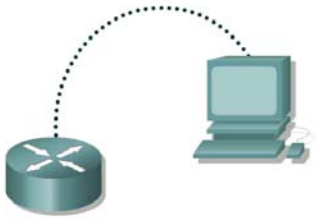
b. Introduzca show interface Serial 0 y verifique el estado de la interfaz.

c. Serial 0 es _____. El protocolo de línea es _____.

Paso 9: Verificar la configuración

a. Introduzca el comando **show running-config** desde el modo EXEC privilegiado para ver si las modificaciones se realizaron correctamente. Si la configuración no es correcta, corrija los comandos incorrectos y verifique nuevamente. Una vez completados los pasos anteriores, desconéctese escribiendo **exit** (salir). Apague el router.

Configuración de una interfaz Ethernet



Designación del router	Nombre del router	Tipo de router	Dirección FA0/0	Máscara de subred	Contraseña enable secret	Contraseñas enable/VTY/ Consola
Router 1	GAD		192.168.14.1	255.255.255.0	class	cisco

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio

Paso 1: Configure el nombre del dispositivo y las contraseñas del router

a. En el router, ingrese al modo de configuración global y configure el nombre del dispositivo como se muestra en la gráfica. Luego, configure las contraseñas de consola, de la terminal virtual y de enable.

Paso 2: Configurar la interfaz FastEthernet 0

Nota: La designación de la primera interfaz Ethernet en el router puede variar. Puede ser ethernet 0, fastethernet 0 o fastethernet 0/0 según el tipo de router.

GAD(config)#**interface fastEthernet 0**
GAD(config-if)#**ip address 192.168.14.1 255.255.255.0**
GAD(config-if)#**no shutdown**
GAD(config-if)#**exit**
GAD(config)#**exit**

Nota: El comando **no shutdown** activa la interfaz. La interfaz se desactiva con Shutdown.

Paso 3: Guardar la configuración

a. Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

GAD#**copy running-config startup-config**

Paso 4: Despliega la información de configuración de la interfaz Fast Ethernet

GAD#**show interface fastethernet 0**

Nota: Aparecerán los detalles de la interfaz Ethernet.

a. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

b. FastEthernet0 es _____. El protocolo de línea es _____.

c. La dirección de Internet es _____.

d. Encapsulamiento _____

e. ¿A qué capa del modelo OSI se refiere el término "encapsulamiento"?
_____

Una vez completados los pasos anteriores, desconéctese escribiendo **exit** (salir). Apague el router.

Configuración de las descripciones de interfaz

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio

Paso 1: Configure el nombre del dispositivo y los passwords en el router

a. En el router ingrese al modo de configuración global. Configure el nombre de host según lo indica la tabla. Luego, configure las contraseñas de consola, de la terminal virtual y de enable.

b. ¿Cuál es el comando del router que se utiliza para visualizar la configuración activa?

_____

c. ¿Qué modo de comando se debe utilizar para introducir el comando que se menciona en la última pregunta?

_____

d. Introduzca el comando de la pregunta anterior para verificar la configuración que se acaba de introducir. Si la configuración no es correcta, corrija los errores. Vuelva a verificarla hasta que esté correcta.

Paso 2: Entrar al modo de configuración global

a. Introduzca **configure terminal** en la petición de entrada del router. Observe el cambio en la petición de entrada del router.
¿Cómo cambió la petición de entrada del router?

_____

Paso 3: Entrar al modo de configuración de interfaz

a. Introduzca **interface serial 0** en la petición de entrada de configuración global. Consulte el esquema de interfaz.
¿Cómo es la petición de entrada de router en el modo de configuración de interfaz?

_____

Paso 4: Mostrar la ayuda para el comando description

a. Introduzca **description ?** en la petición de entrada del router.
¿Cuál es el número máximo de caracteres de una descripción de interfaz?

_____

Paso 5: Elegir una descripción para la interfaz

a. Una descripción de interfaz incluye el propósito y la ubicación de la interfaz, los otros dispositivos o ubicaciones conectadas a la interfaz e los identificadores de circuito. Las descripciones ayudan al personal de asistencia técnica a comprender la dimensión de los

problemas relacionados con una interfaz. Las descripciones también permiten una resolución más rápida de los problemas.

b. A base del diagrama y la siguiente información del circuito, elija una descripción de las interfaces seriales 0/0 para GAD y BHM. Use el siguiente formulario para documentar su elección.

Enlace	Portadora	ID del circuito	Velocidad
de GAD a BHM -	BellSouth	10DHDG551170	1.544Mbits/seg

Paso 6: Introducir una descripción para la interfaz serial 0

a. En el modo de configuración de la interfaz para la interfaz serial 0, introduzca el texto de descripción. El texto es la descripción del paso anterior. Luego introduzca **Ctrl-z** o escriba **end** (finalizar) para volver al modo EXEC privilegiado.

Nota: esto sería lo mismo que escribir **exit** (salir) para salir del modo de configuración de interfaz y **exit** nuevamente para abandonar el modo de Configuración global. Esto constituye un atajo de teclado.

Paso 7: Examinar el archivo de configuración activo

a. En el modo EXEC privilegiado, introduzca el comando que hará aparecer la configuración activa. El modo EXEC privilegiado también se denomina modo enable. El router mostrará información sobre la configuración activa.

b. ¿Qué comando se introdujo?

_____

c. ¿Cuál es la descripción de la interfaz serial0?

_____

Paso 8: Confirmar que la descripción de la interfaz sea correcta

a. Desde el modo enable, introduzca el comando **show interfaces serial 0**. El router muestra información sobre la interfaz. Examine este resultado para confirmar que la descripción introducida coincida con la descripción correcta.

Una vez completados los pasos anteriores, desconéctese escribiendo **exit** (salir). Apague el router.

Borrar y recargar el router

Ingrese en el modo EXEC privilegiado escribiendo **enable** (habilitar).

Si pide una contraseña, introduzca **class**. Si "class" no funciona, solicite ayuda a su instructor.

Router>**enable**

En el modo EXEC privilegiado, introduzca el comando **erase startup-config.**

Router#**erase startup-config**

La petición de la línea de respuesta será:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Presione **Intro** para confirmar.

La respuesta deberá ser:

Erase of nvram: complete

En el modo EXEC privilegiado, introduzca el comando **reload** (recargar).

Router#**reload**

La petición de la línea de respuesta será:

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

Escriba **n** y luego presione **Intro**.

La petición de la línea de respuesta será:

Proceed with reload? [confirm]

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

Reload requested by console.

Una vez que el router se ha recargado el mensaje de respuesta será:

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

Escriba **n** y luego presione **Intro**.

La petición de la línea de respuesta será:

Press RETURN to get started!

Presione **Intro**.

El router está listo para iniciar el laboratorio asignado.

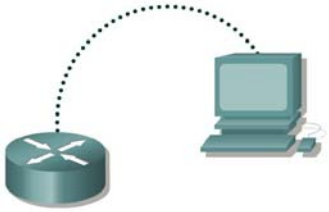
Resumen de la interfaz de router

Modelo de Router	Interfaz Ethernet N° 1	Interfaz Ethernet N° 2	Interfaz Serial N° 1	Interfaz Serial N° 2	Interfaz N° 5
800 (806)	Ethernet0(E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Para saber exactamente cómo está configurado el router, consulte las interfaces. Esto le permitirá identificar el tipo de router así como cuántas interfaces posee el router. No hay una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque otro tipo pueda existir en un router dado. La interfaz BRI RDSI es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos IOS para representar la interfaz.

3.2 Laboratorio

USO DEL COMANDO DE ADMINISTRACIÓN EN CISCO IOS



Designación del router	Nombre del router	Contraseña enable secret	Contraseñas enable/VTY y de Consola
Router 1	GAD	clase	cisco

Objetivo

- Mostrar información acerca de la imagen activa del software Cisco IOS.
- Determinar desde dónde se arranca el IOS.
- Verificar la cantidad de memoria RAM, Flash y NVRAM disponible en el router.
- Verificar la imagen IOS y la Flash para saber cuánto espacio se ha utilizado y cuánto hay disponible.
- Documentar las partes del nombre de archivo de la imagen IOS.
- Verificar y documentar los ajustes del registro de configuración relacionados con el método de arranque.
- Documentar una secuencia de arranque de reserva.
- Hacer una copia de respaldo de un archivo de configuración del router.
- Recargar el archivo de configuración de respaldo desde un servidor TFTP a la RAM del router.
- Guardar la nueva configuración activa a la NVRAM.
- Realizar una copia del IOS de un router desde la flash a un servidor TFTP.
- Volver a cargar la copia de respaldo de la imagen del software IOS desde un servidor TFTP al flash de un router.

Tiempo estimado

45 minutos

Información básica

Establezca una red similar a la del diagrama anterior. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Consulte la tabla al final de este laboratorio identificar correctamente los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. Los resultados de la configuración utilizados en este

laboratorio se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos. Hay que ejecutar los siguientes pasos en cada router a menos que se especifique lo contrario.

Iniciar una sesión de HyperTerminal

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio.

Paso 1: Iniciar una sesión en el router

a. Inicie una sesión en el router.

Paso 2: Entrar al modo EXEC privilegiado

a. Introduzca **enable** en la petición de entrada.

Paso 3: Guardar la configuración activa como la configuración inicial

a. En la petición de entrada del modo EXEC privilegiado, introduzca:

Router#**copy running-config startup-config**
Destination filename [startup-config]? [Intro]

Esto guarda la configuración activa que está en blanco.

Paso 4: Configurar el router y visualizar el archivo de la configuración activa

a. Configure el router con la información que aparece en la tabla.

b. Introduzca **show running-config** en la petición de entrada del router. El router mostrará información sobre el archivo de configuración activo guardado en la NVRAM.

c. ¿Se muestra la configuración que se acaba de introducir?

_____

Paso 5: Mostrar información sobre la copia de respaldo del archivo de configuración

a. Introduzca **show startup-config** en la petición de entrada del router. El router mostrará información sobre la copia de respaldo del archivo de configuración guardada en la NVRAM.

b. ¿Se muestra la configuración que se acaba de introducir?

_____

c. Si no es así, ¿por qué?

_____

d. ¿Qué comando haría que el archivo de configuración actual y el de configuración inicial sean idénticos?

_____

e. ¿Por qué es tan importante el archivo de configuración inicial?

_____

f. ¿Existe alguna indicación de los valores del registro de configuración?

_____

Paso 6: Mostrar la versión del software Cisco IOS y otra información importante

a. Introduzca el comando **show version** en la petición de entrada del router.
El router devuelve información acerca del IOS que se está ejecutando en la RAM.

b. ¿Cuál es la versión IOS y el nivel de revisión?

_____

c. ¿Cuál es el nombre del archivo de imagen del sistema (IOS)?

_____

d. ¿Desde dónde se arrancó la imagen IOS del router?

_____

e. ¿Qué tipo de procesador y cuánta RAM tiene este router?

_____

f. ¿Qué tipo de router (tipo de plataforma) es éste?

_____

g. La copia de respaldo del archivo de configuración del router se guarda en la memoria de acceso directo no volátil (NVRAM). ¿Cuánta NVRAM tiene este router?

_____

h. El sistema operativo del router (IOS) se guarda en la memoria Flash. ¿Cuánta memoria flash tiene el router?

_____

i. ¿Cuál es el valor del registro configuración? ¿Cuál es el tipo de arranque que especifica este valor? _____

Paso 7: Crear las sentencias para realizar las siguientes funciones

a. Suponiendo que en el paso anterior el valor del **config-register** estaba en 0x2102, escriba los comandos del modo de configuración para especificar que la imagen IOS se deba cargar desde:

Memoria flash: _____

Monitor de la ROM: _____

ROM: _____

b. Si el router estuviera en el modo de monitor de ROM, ¿qué comando iniciaría el software Cisco IOS?

_____

Paso 8: Mostrar información acerca del dispositivo de memoria Flash

a. Introduzca el comando **show flash** en la petición de entrada del router. El router muestra en pantalla la información acerca de la memoria flash y cuál(es) archivo(s) de imagen IOS que se guarda(n) en esa memoria.

b. Anote la siguiente información:

¿Cuánta memoria flash está disponible y cuánta se ha utilizado?

_____

¿Cuál es el archivo que se guarda en la memoria flash?

_____

¿Cuál es el tamaño en bytes de la memoria flash?

_____

Paso 9: Especificar una secuencia de arranque de reserva

a. Escriba el comando de configuración para especificar que la imagen IOS se debe cargar desde:

Memoria flash: _____

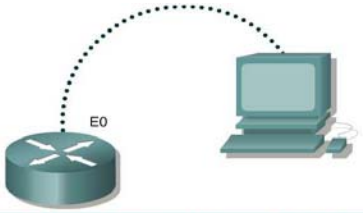
Un servidor TFTP: _____

ROM: ¿Será ésta una imagen IOS completa? _____

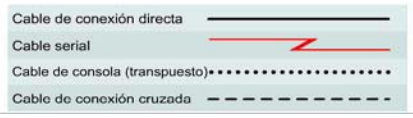
b. Para asegurarse de que estos comandos estén disponibles para que el router los pueda utilizar la próxima vez que se reinicie, ¿cuál es el comando que se debe introducir a continuación? _____

Al completar los pasos anteriores, desconéctese escribiendo **exit**. Apague el router.

Administración de archivos de configuración mediante TFTP



Designación del router	Nombre del router	Contraseña enable secret	Contraseñas enable/VTY y de Consola	Tipo de interfaz Serial 0	Máscara de subred de todas las direcciones
Router 1	GAD	clase	cisco	192.168.14.2	255.255.255.0



Información básica

Para fines de documentación y recuperación es importante mantener copias de respaldo de los archivos de configuración del router. Se pueden guardar en un lugar central, como un servidor TFTP, para fines de consulta y recuperación de ser necesario.
Establezca una red similar a la del diagrama anterior. Se puede usar cualquier router que cumpla con los requisitos de interfaz.

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio.

Paso 1: Configurar el router Gadsden

a. Si hay dificultades en configurar el nombre de host, consulte el Laboratorio de Introducción a la configuración de los routers.

b. Verifique las configuraciones de los routers ejecutando **show running-config** en cada router. Si hay algún error, corríjalo y vuelva a realizar la verificación.

Paso 2: Configurar la estación de trabajo

a. La configuración del host conectado al router Gadsden es:

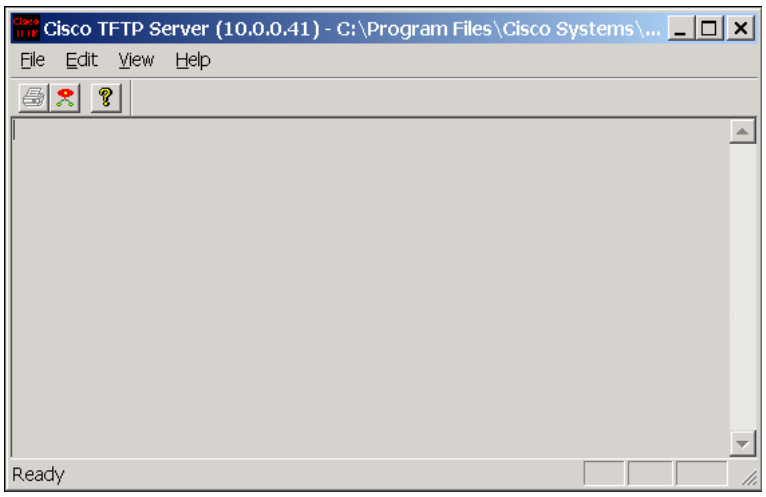
Dirección IP 192.168.14.2
Máscara de subred IP 255.255.255.0
Gateway por defecto 192.168.14.1

Paso 3: Iniciar una sesión en el router en el modo usuario

a. Inicie una sesión en el router Gadsden.

Paso 4: Inicio y configuración del servidor TFTP Cisco

a. Inicie el servidor TFTP. Si el computador está conectad correctamente, no será necesario configurar el servidor TFTP Cisco.



Paso 5: Verificar la conectividad

a. Haga ping al servidor TFTP desde el router Gadsden.
Si falla el ping, revise las configuraciones del host y del router para resolver el problema.

Paso 6: Copie la configuración activa al servidor TFTP

a. Antes de copiar los archivos, verifique que el servidor TFTP esté funcionando.

b. Anote la dirección IP del servidor TFTP. _____

c. Ejecute el comando **copy running-config tftp**. Siga los indicadores:

GAD#**copy running-config tftp**
Address or name of remote host []? **192.168.14.2**
Destination filename [gad-confg]? **startup-config**
!!
667 bytes copied in 0.036 secs (18528 bytes/sec)

Paso 7: Verificar la transferencia al servidor TFTP

a. Verifique el archivo de registro del servidor TFTP. Haga clic en **View** > **Log File**. El resultado debe ser similar a lo siguiente:

Mon Sep 16 14:10:08 2003: Receiving 'startup-config' file from
192.168.14.1 in binary mode
Mon Sep 16 14:11:14 2003: Successful.

Paso 8: Copiar la configuración de inicio desde el servidor TFTP

a. Ahora que el starup-config ha sido respaldado, pruebe esta imagen recargándola en el router. Se debes suponer que la configuración en el router GAD se ha dañado. Para simular esto, cambie el hostname del router GAD a "Router".

b. ¿Cuál es la dirección IP del servidor TFTP? _____

c. Para copiar desde la petición de entrada de EXEC privilegiado, escriba **copy tftp runningconfig**. Presione **Intro**.

Router#**copy tftp running-config**
Address or name of remote host []? **192.168.14.2**
Source filename []? **startup-config**
Destination filename [running-config]? **[Intro]**
Accessing tftp://192.168.14.2/startup-config...
Loading startup-config from 192.168.14.2 (via FastEthernet0): !
[OK - 667 bytes]

667 bytes copied in 9,584 secs (70 bytes/sec)

GAD#

Paso 9: Guardar la nueva configuración activa

a. Guardar la nueva configuración activa en la NVRAM mediante el siguiente comando:

GAD#**copy running-config startup-config**
Destination filename [startup-config]?**[Intro]**
Building configuration...
[OK]

Paso 10: Probar el archivo restaurado

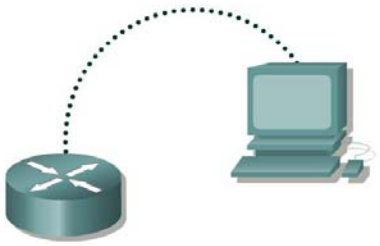
a. Si el indicador del router cambia como se indica en la última línea del resultado del Paso 8, se ha cargado el archivo. Introduzca el comando **show startup-config** para verificar toda la configuración.

Paso 11: Verificar las condiciones de la interfaz

a. Al restaurar este archivo, las interfaces se desactivan por defecto, a menos que el archivo de configuración se haya modificado y se haya introducido una línea de comando **no shutdown** después de cada perfil de interfaz.

Al completar los pasos anteriores, desconéctese escribiendo **exit**. Apague el router.

Administración de imágenes IOS mediante TFTP



Designación del router	Nombre del router	Dirección Fast Ethernet 0	Máscara de subred de todas las direcciones
Router 1	GAD	192.168.14.1	255.255.255.0

Información básica

Para fines de recuperación es importante mantener copias de respaldo de las imágenes IOS del router. Se pueden guardar en un lugar central, como un servidor TFTP, para fines de recuperación de ser necesario.
Cree una red con un cableado similar al del diagrama anterior.

Paso 1: Configurar el router GAD

a. Si hay dificultades en configurar el nombre de host, consulte el Laboratorio Introducción a la configuración de los router. Si hay dificultades en configurar las interfaces, consulte el Laboratorio de Configuración de las interfaces del router.

b. Verifique las configuraciones de los routers ejecutando **show running-config** en el router. Si hay algún error, corríjalo y vuelva a realizar la verificación.

Paso 2: Configurar la estación de trabajo

a. La configuración del host conectado al router GAD es:

Dirección IP 192.168.14.2
Máscara de subred IP 255.255.255.0
Gateway por defecto 192.168.14.1

Paso 3: Reunir información para documentar el nuevo router

a. Ejecute el comando **show version**.

b. ¿Cuál es el valor actual de config register?_____0x _____

c. ¿Cuánta memoria flash tiene el router? _____

d. ¿Hay por lo menos 4Mb (4096K) de memoria flash? _____

e. ¿Cuál es el número de versión de boot ROM? _____

f. ¿La versión de boot ROM es 5.2 o superior? _____

Paso 4: Reunir información adicional para documentar el nuevo router

a. Ejecute el comando **show flash**.

b. ¿Hay un archivo almacenado en la flash?

_____

c. De ser así, ¿cuál es el nombre exacto de ese archivo?

_____

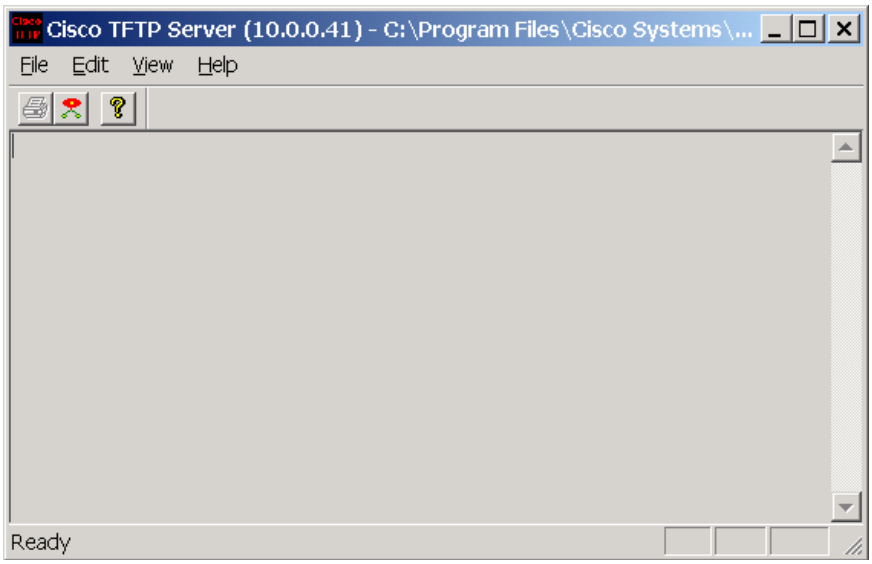
d. ¿Cuánta más memoria flash está disponible o no utilizada?

_____

Nota: Si hay un archivo en la flash, es probable que deba eliminarse antes de cargar uno nuevo. Esta opción se ofrece en el comando **copy tftp flash** en un paso posterior.

Paso 5: Inicio y configuración del servidor TFTP Cisco

a. Consulte al instructor para obtener la dirección IP del servidor TFTP Cisco.



Paso 6: Verificar la conectividad

a. Haga ping al servidor TFTP desde el router GAD.

Si falla el ping, revise las configuraciones del host y del router para resolver el problema.

Paso 7: Copiar el IOS al servidor TFTP

a. Antes de copiar los archivos, verifique que el servidor TFTP esté funcionando.

b. ¿Cuál es la dirección IP del servidor TFTP?

____

c. Desde la sesión de consola, introduzca **show flash**.

d. ¿Cuál es el nombre y longitud de la imagen IOS Cisco almacenada en la flash?

____

e. ¿Qué atributos se pueden identificar a partir de los códigos en el nombre de archivo IOS Cisco?

____

Paso 8: Copiar la nueva imagen IOS al servidor TFTP

a. Desde la sesión de consola en el modo EXEC privilegiado, introduzca el comando **copy flash tftp**. En la petición de entrada, introduzca la dirección IP del servidor TFTP: Los nombres de los archivos dependen del IOS y de la plataforma. El nombre de archivo para su sistema se proporcionó en el Paso 4.

GAD#**copy flash tftp**
Source filename []? **flash:c1700-y-mz.122-11.T.bin**
Address or name of remote host []? **192.168.14.2**
Destination filename [c1700-y-mz.122-11.T.bin]? **y**

Después de introducir este comando y responder a las peticiones del proceso, el estudiante debe ver el siguiente resultado en la consola. No interrumpa este proceso.

!!!
!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!
4284648 bytes copied in 34.012 secs (125975 bytes/sec)

Paso 9: Verificar la transferencia al servidor TFTP

a. Verifique el archivo de registro de servidor TFTP haciendo clic en **View** > **Log File**. El resultado debe ser similar al siguiente resultado:

Mon Sep 16 14:10:08 2003: Receiving ‘c1700-y-mz.122-11.T.bin’ in binary mode
Mon Sep 16 14:11:14 2003: Successful.

b. Verifique el tamaño de la imagen flash en el directorio del servidor TFTP. Para encontrarla, haga clic en **View** > **Options**. Esto mostrará el directorio raíz del servidor TFTP. Debe ser similar al siguiente, a menos que los directorios por defecto se hayan cambiado:
C:\Program Files\Cisco Systems\Cisco TFTP Server

c. Busque este directorio con el Administrador de archivos. Observe el listado detallado del archivo. La longitud que muestra el comando **show flash** debe ser igual al tamaño de archivo del archivo almacenado en el servidor TFTP. Si los tamaños de archivo no son idénticos, consulte al instructor.

Paso 10: Copiar la imagen del IOS desde el servidor TFTP

a. Ahora que se ha realizado la copia de seguridad del IOS, es necesario probar la imagen y restaurar el IOS al router. Cuando se le solicite por el "nombre de archivo de destino", use el mismo del Paso 7.

b. Anote la dirección IP del servidor TFTP.
____

c. Realice la copia desde la petición de entrada de EXEC privilegiado.

GAD#**copy tftp flash**
Address or name of remote host []?**192.168.14.2**
Source filename []?**c1700-y-mz.122-11.T.bin**
Destination filename [c1700-y-mz.122-11.T.bin]? **[Intro]**
Accessing tftp://192.168.14.2/c1700-y-mz.122-11.T.bin...
Erase flash: before copying? [confirm]**[Intro]**
Erasing the flash filesystem will remove all files! Continue?
[confirm]**[Intro]**
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
...erased
Erase of flash: complete
Loading c1700-y-mz.122-11.T.bin from 192.168.14.2 (via
FastEthernet0):!!!!!!!!!!
!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4284648 bytes]

Verifying checksum... OK (0x9C8A)
4284648 bytes copied in 26.584 secs (555739 bytes/sec)

d. Es posible que el router pregunte si se debe borrar la memoria flash. ¿Cabe la imagen en la memoria flash disponible? _______________

e. Si se borra la memoria flash, ¿qué pasó en la pantalla de la consola del router durante este proceso?

_____

f. ¿Cuál es el tamaño del archivo que se estaba cargando? _____No interrumpa este proceso.

g. ¿Qué ocurrió en la pantalla de la consola del router mientras se estaba descargando el archivo?

_____

h. ¿Fue exitosa la verificación? _____

i. ¿Fue exitosa la operación completa? _____

Paso 11: Probar la imagen IOS restaurada

a. Verifique que la imagen del router es correcta. Reinicie el router y observe el proceso de inicio para confirmar que no haya errores de flash. Si no hay, entonces el IOS del router se habrá iniciado correctamente.

b. Verifique la imagen IOS en la flash mediante el comando **show version** que mostrará un resultado similar a:
System image file is "flash:c1700-y-mz.122-11.T.bin"

Al completar los pasos anteriores, desconéctese escribiendo **exit**. Apague el router.

Borrar y recargar el router

Entre al modo EXEC privilegiado escribiendo **enable**.

Si pide una contraseña, introduzca **class**. Si "class" no funciona, pide ayuda a su instructor.

Router>**enable**

En el modo EXEC privilegiado, introduzca el comando **erase startup-config.**

Router#**erase startup-config**

Como respuesta, aparecerá la siguiente petición de entrada:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Presione **Intro** para confirmar.

La respuesta deberá ser:

Erase of nvram: complete

En el modo EXEC privilegiado, introduzca el comando **reload**.

Router(config)#**reload**

Como respuesta, aparecerá la siguiente petición de entrada:

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

Escriba **n** y luego presione **Intro**.
Como respuesta, aparecerá la siguiente petición de entrada:

Proceed with reload? [confirm]

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

Reload requested by console.

La siguiente petición de entrada aparecerá después de que el router se recargue:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:
Press RETURN to get started!

Presione **Intro**.

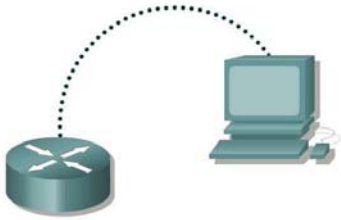
El router está listo para iniciar el laboratorio asignado.

Resumen de la interfaz del router

Modelo de Router	Interfaz Ethernet N°1	Interfaz Ethernet N°2	Interfaz Serial N°1	Interfaz Serial N°2	Interfaz N°5
800 (806)	Ethernet0(E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

3.3 Laboratorio

RECUPERACIÓN DEL PASWORD



Designación del router	Nombre del router	Contraseña enable secret	Contraseñas enable/VTY y de Consola
Router 1	GAD	clase	cisco

Objetivo

- Iniciar una sesión en un router cuya contraseña del modo privilegiado (enable) es desconocida.

Tiempo estimado

30 minutos

Información básica

Este laboratorio demuestra cómo obtener acceso a un router cuya contraseña del modo privilegiado (enable) es desconocida. Es importante aclarar que cualquiera que conozca este procedimiento y pueda acceder a un puerto de consola de un router puede cambiar la contraseña y asumir el control del router. Por este motivo es de importancia fundamental que los routers también tengan la seguridad física para evitar el acceso no autorizado.
Establezca una red similar a la del diagrama anterior. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Consulte la tabla al final de este laboratorio para identificar correctamente los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. Los resultados de la configuración utilizados en este laboratorio se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos.
Iniciar una sesión de HyperTerminal.
Nota: Configure el nombre de usuario y la contraseña en el router. Pida a un instructor, a un asistente de laboratorio o a otro estudiante que configure una configuración básica con una contraseña enable secret. Introduzca **copy running-config startup-config** y vuelva a cargar el router.

Paso 1: Intentar iniciar una sesión en el router

a. Haga las conexiones de consola necesarias y establezca una sesión de HyperTerminal con el router. Intente conectarse al router mediante la contraseña enable **cisco**. El resultado debe ser similar al siguiente:

Router>**enable**
Password:
Password:
Password:
% Bad secrets
Router>

Paso 2: Anote los valores actuales del registro de la configuración

a. En la petición de entrada de EXEC del usuario escriba **show version**.

b. Anote el valor que aparece para el registro de configuración **_____**. Por ejemplo 0x2102.

Paso 3: Entrar al modo de Monitor de ROM

a. Apague el router, espere unos segundos y vuelva a encenderlo. Cuando el router empieza a mostrar "System Bootstrap, Version …" en la pantalla de HyperTerminal, presione la tecla **Ctrl** y la tecla **Pausa** al mismo tiempo. El router arranca en el modo de monitor ROM. Según el hardware del router, pueden aparecer una de varias peticiones de entrada, como: "**rommon 1 >**" o simplemente "**>**".

Paso 4: Examinar el modo de ayuda del Monitor de ROM

a. Escriba **?** en la petición de entrada. El resultado deberá se similar a esto:

rommon 1 >**?**

alias	set and display aliases command
boot	boot up an external process
break	set/show/clear the breakpoint
confreg	configuration register utility
context	display the context of a loaded image
dev	list the device table
dir	list files in file system
dis	display instruction stream
help	monitor builtin command help
history	monitor command history
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
set	display the monitor variables

sysret	print out info from last system return
tftpdnld	tftp image download
xmodem	x/ymodem image download

Paso 5: Cambiar los valores del registro de configuración para arrancar sin cargar el archivo de configuración

a. Desde el modo de Monitor ROM, escriba **confreg 0x2142** para cambiar el registro de configuración (config-register).

   rommon 2 >**confreg 0x2142**

Paso 6: Reiniciar el router

a. Desde el modo Monitor ROM, escriba **reset** o reinicie el router.

   rommon 2 >**reset**

b. Debido a los nuevos valores de registro de configuración, el router no carga el archivo de configuración. El sistema pregunta:

   "Would you like to enter the initial configuration dialog? [yes]:"

   Introduzca **no** y presione **Intro**.

Paso 7: Entrar al modo EXEC privilegiado y cambiar la contraseña

a. Ahora, en la petición de entrada del modo de usuario Router>, escriba **enable** y presione **Intro** para ir al modo privilegiado sin contraseña.

b. Use el comando **copy startup-config running-config** para restaurar la configuración existente. Como el usuario ya se encuentra en el modo EXEC privilegiado, no hace falta una contraseña.
c. Escriba **configure terminal** para entrar al modo de configuración global.
d. En el modo de configuración global escriba **enable secret class** para cambiar la contraseña secret.

e. Mientras se encuentra en el modo de configuración global, escriba **config-register xxxxxx**. xxxxxx es el valor de registro de configuración original que se anotó en el Paso 2.
   Presione **Intro**.

f. Use la combinación de **Ctrl z** para volver al modo EXEC privilegiado.
g. Use el comando **copy running-config startup-config** para guardar la nueva configuración.

h. Antes de reiniciar el router, verifique los nuevos valores de configuración. Desde el modo EXEC privilegiado, introduzca el comando **show version** y presione **Intro**.

i. Verifique que la última línea del resultado diga:

Configuration register is 0x2142 (will be 0x2102 at next reload).

j. Use el comando **reload** para rearrancar el router.

Paso 8: Verificar la nueva contraseña y configuración

a. Cuando se vuelve a cargar el router la contraseña debe ser **class**.

Al completar los pasos anteriores, desconéctese escribiendo **exit**. Apague el router.

Borrar y recargar el router.

Entre al modo EXEC privilegiado escribiendo **enable**.

Si pide una contraseña, introduzca **class**. Si "class" no funciona, pide ayuda a su instructor.

Router>**enable**

En el modo EXEC privilegiado, introduzca el comando **erase startup-config.**

Router#**erase startup-config**

Como respuesta, aparecerá la siguiente petición de entrada:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Presione **Intro** para confirmar.

La respuesta deberá ser:

Erase of nvram: complete

En el modo EXEC privilegiado, introduzca el comando **reload**.

Router(config)#**reload**

Como respuesta, aparecerá la siguiente petición de entrada:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

Proceed with reload? [confirm]

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

Reload requested by console.

La siguiente petición de entrada aparecerá después de que el router se recargue:

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

Escriba **n** y luego presione **Intro**.
Como respuesta, aparecerá la siguiente petición de entrada:

Press RETURN to get started!

Presione **Intro**.

El router está listo para iniciar el laboratorio asignado.

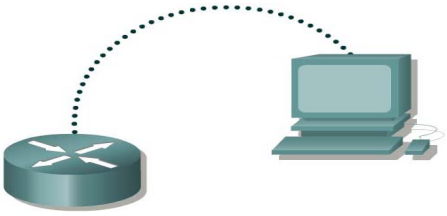
Resumen de la interfaz del router

Modelo de Router	Interfaz Ethernet N°1	Interfaz Ethernet N°2	Interfaz Serial N°1	Interfaz Serial N°2	Interfaz N°5
800 (806)	Ethernet0(E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Para conocer la configuración exacta del router, consulte las interfaces. Esto le permitirá identificar el tipo de router así como cuántas interfaces posee el router. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque otro tipo pueda existir en un router dado. La interfaz BRI RDSI es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando IOS para representar la interfaz.

3.4 Laboratorio

UTILIZACIÓN DE XMODEM PARA RECARGAR LA IMÁGEN IOS



Objetivo

- Recuperar un router Cisco que está bloqueado en el monitor ROM (ROMmon) (rommon#>).
- Aprender a evitar tener que usar Xmodem para recargar el archivo IOS.

Tiempo estimado

30 minutos

Información básica

Este es un proceso que sólo hace falta aplicar en caso de emergencia, si un usuario ha eliminado o borrado el IOS y no existe la posibilidad de poder cargar una nueva versión del IOS desde un servidor TFTP.

Si este procedimiento no se puede evitar, esta laboratorio de laboratorio explica cómo usar el comando **xmodem** en la consola para descargar el software Cisco IOS® mediante el monitor ROM (ROMmon). Xmodem se puede usar en una variedad de routers (enumerados a continuación) y se usa en la recuperación de desastres cuando el router no tiene un software Cisco IOS válido o una imagen boot flash para arrancar y, por lo tanto, sólo arranca en ROMmon. Este procedimiento también puede usarse cuando no hay servidores del Protocolo Trivial de Transferencia de Archivos (Trivial File Transfer Protocol - TFTP) o conexiones de red y la única opción viable es una conexión directa desde un PC (o a través de una conexión de módem) a la consola del router. Como este procedimiento se basa en la velocidad de consola del router y el puerto serial del PC, puede tardarse bastante en descargar una imagen. Descargar una imagen del software Cisco IOS Versión 12.1(16) IP Plus a un router Cisco serie 1600 con una velocidad de 38400 bps tarda aproximadamente 25 minutos. Este proceso es válido para los routers Cisco serie 827, 1600, 1700, 2600, 3600 y 3700.

Establezca una red similar a la del diagrama anterior. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Consulte la tabla al final de este laboratorio para identificar correctamente los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. Los resultados de la configuración utilizados en este laboratorio se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos.

Iniciar una sesión de HyperTerminal

Borre y recargue el router para prevenir problemas que pueden ser causados por configuraciones residuales.

Paso 1: Entre en modo Monitor ROM.

a. Para simular un reencendido del router teclee Ctrl – Break desde este modo. Dependiendo del hardware del router, se presentarán uno de varios indicadores de modo, tales como: "rommon 1 >" o simplemente ">".

Paso 2: Encontrar una imagen válida en la Flash

a. Desde la petición de entrada "ROM Monitor", ejecute el comando **dir flash:** para cada dispositivo disponible. Busque una imagen válida del software Cisco IOS®:

rommon 3 >**dir flash:**
File size Checksum File name
3307884 bytes (0x804b4c)0x6ba0 c1700-ny-mz.121-6.bin
rommon 4 >

Paso 3: Recuperar con una imagen enumerada si hay alguna

a. Arranque desde cualquier imagen enumerada en el Paso 2. Si la imagen es válida, volverá al modo de operación normal:

rommon 5 >**boot flash:c1700-ny-mz.121-6.bin**
program load complete, entry point: 0x80008000, size: 0x804a30
Self decompressing the image : ##...

Paso 4: Anote información mediante show version

a. Si ninguno de estos archivos es válido, descargue uno nuevo mediante uno de los siguientes procedimientos. El primer paso es registrar la información de **show version** en la configuración inicial. Esto suministra la información necesaria acerca del nombre de la imagen IOS.

Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-M), Version 12.2(11)T, RELEASE
SOFTWARE (fc1)

TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 31-Jul-02 09:08 by ccai
Image text-base: 0x80008124, data-base: 0x807E332C

ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)

Router uptime is 15 minutes
System returned to ROM by reload
System image file is "flash:c1700-y-mz.122-11.T.bin"
cisco 1721 (MPC860P) processor (revision 0x100) with 29492K/3276K bytes of memory.
Processor board ID FOC06380F0T (479701011), with hardware revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
--More—
Configuration register is 0x2102

b. Las líneas destacadas deben anotarse en caso de que necesite realizarse este procedimiento.

Paso 5: Configurar el registro de arranque para entrar al modo ROMmon

a. Si aún no se ha hecho, configure Windows HyperTerminal para 8-N-1 en 9600 bps. Conecte el puerto serial del PC al puerto de consola del router. Una vez conectado, vaya a la petición de entrada de ROMmon (rommon 1>). Normalmente, si tanto la imagen del software Cisco IOS como la imagen bootflash están corrompidas, el router sólo se arranca en el modo ROMmon. Si no es así y es necesario ir a la petición de entrada de ROMmon; se debe cambiar el registro de configuración. Éste normalmente se cambia 0x2102 como lo presenta **show version** a 0x0 como se muestra a continuación:ç

Router>**enable**
Router#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**config-register 0x0**
Router(config)#**exit**
Router#
*Mar 1 00:29:21.023: %SYS-5-CONFIG_I: Configured from console by
console
Router#**reload**
System configuration has been modified. Save? [yes/no]: **n**
Proceed with reload? [confirm][Intro]

*Mar 1 00:30:32.235: %SYS-5-RELOAD: Reload requested by console.

System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 32768 Kbytes of main memory

rommon 1 >

Paso 6: Ver los comandos disponibles desde la petición de entrada rommon

a. Introduzca lo siguiente en la petición de entrada de monitor ROM:

rommon 1 >**?**

alias	set and display aliases command
boot	boot up an external process
break	set/show/clear the breakpoint
confreg	configuration register utility
context	display the context of a loaded image
dev	list the device table
dir	list files in file system
dis	display instruction stream
help	monitor builtin command help
history	monitor command history
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
set	display the monitor variables
sync	write monitor environment to NVRAM
sysret	print out info from last system return
tftpdnld	tftp image download
unalias	unset an alias
unset	unset a monitor variable
xmodem	x/ymodem image download

b. En este laboratorio se usa **confreg** para reconfigurar la velocidad de consola. Use **xmodem** para transferir el archivo.

Paso 7: Reconfigurar la velocidad de terminal para una descarga más rápida

a. Especificando una velocidad de datos de 115200 bps, por ejemplo, la velocidad de descarga se puede aumentar reduciendo el tiempo de descarga. Estos son los pasos para reconfigurar la velocidad en el router.
rommon 2 >**confreg**
Configuration Summary
(Virtual Configuration Register: 0x1820)
enabled are:
break/abort has effect
console baud: 9600

boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: **y**
enable "diagnostic mode"? y/n [n]:**[Intro]**
enable "use net in IP bcast address"? y/n [n]: **[Intro]**
enable "load rom after netboot fails"? y/n [n]: **[Intro]**
enable "use all zero broadcast"? y/n [n]: **[Intro]**
disable "break/abort has effect"? y/n [n]: **y**
enable "ignore system config info"? y/n [n]: **[Intro]**
change console baud rate? y/n [n]: **y**
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: **7**
change the boot characteristics? y/n [n]: **[Intro]**

Configuration Summary
(Virtual Configuration Register: 0x1920)
enabled are:
console baud: 115200
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: **y**
You must reset or power cycle for new config to take effect

rommon 3 >**reset**

Nota: Es necesario cambiar la configuración de HyperTerminal para reflejar la nueva velocidad de consola de 115200, en lugar de 9600 baudios. De lo contrario se presenta un resultado incomprensible.

System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 32768 Kbytes of main memory

Paso 8: Usar el comando xmodem para solicitar un archivo al host

a. Antes de emitir el comando **xmodem**, asegúrese de que la nueva imagen de software de Cisco IOS esté instalada en el PC. Desde el indicador ROMmon, ejecute el comando **xmodem**.

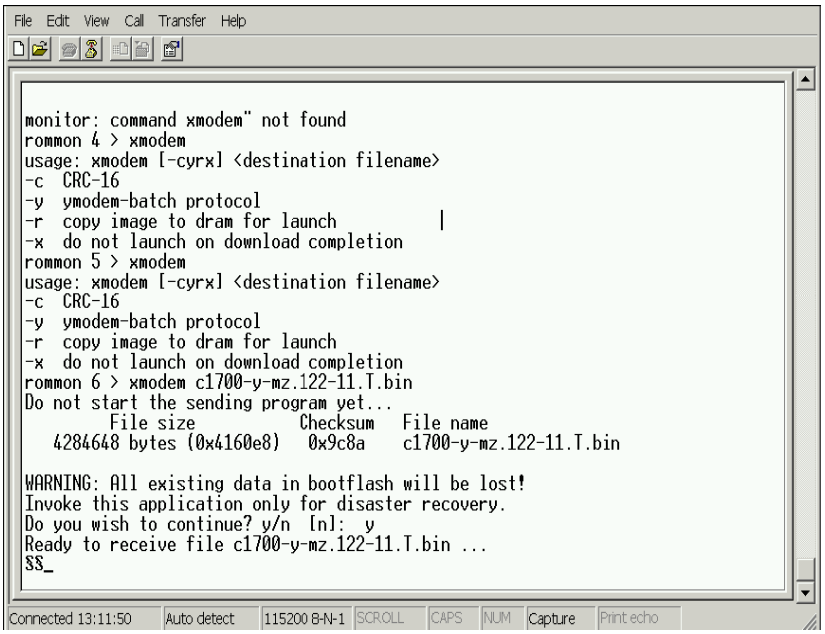
rommon 2 >**xmodem**
usage: xmodem [-cyrx] <destination filename>
-c CRC-16
-y ymodem-batch protocol
-r copy image to dram for launch
-x do not launch on download completion

rommon 3 >**xmodem c1700-y-mz.122-11.T.bin**
Do not start the sending program yet...

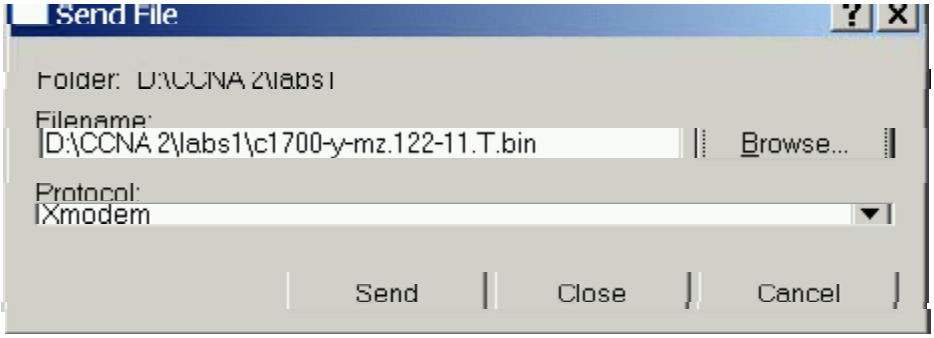
File size Checksum File name
4284648 bytes (0x4160e8) 0x9c8a c1700-y-mz.122-11.T.bin
WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: **y**
Ready to receive file c1700-y-mz.122-11.T.bin ...

Paso 9: Enviar el archivo desde el programa HyperTerminal

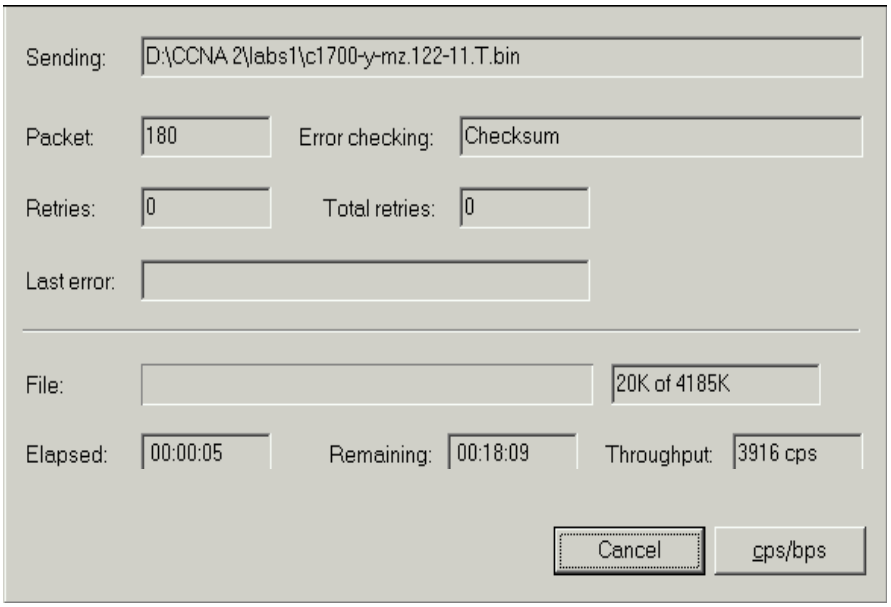
a. Desde el programa HyperTerminal, envíe el archivo IOS aplicando los siguientes pasos:



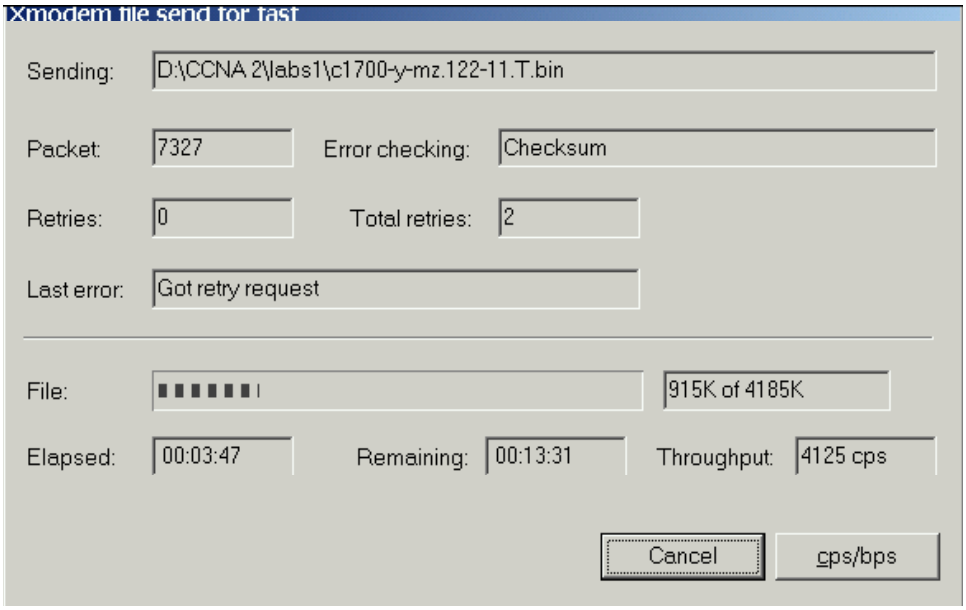
b. Seleccione **Transfer** > **Send File** (Transferir > Enviar archivo). Especificar la ubicación del archivo IOS en el disco duro del host.



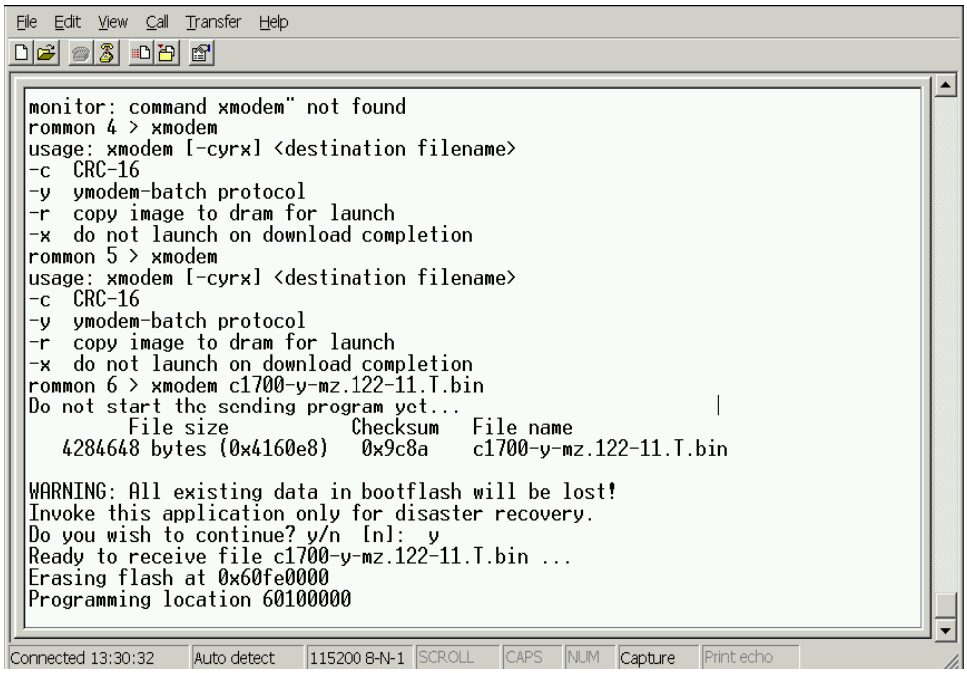
c. A continuación, haga clic en **Send** (Enviar) o inicie la transferencia del archivo al router.



d. A medida que avanza la transferencia, tendrá este aspecto:



e. Al terminar, aparece lo siguiente:



f. Al terminarse este proceso, el router se vuelve a cargar.

Paso 10: Reconfigurar el registro de arranque y la velocidad de consola

a. Desde la petición de entrada de configuración, establezca el registro de arranque nuevamente en 0x2102 o la configuración original antes de la transferencia del IOS. Esto se realiza mediante el comando **config-register** en la petición de entrada de configuración global.

Router(config)#**config-register 0x2102**
Router(config)#**exit**
Router#**show flash**

System flash directory:
File Length Name/status
1 4284648 c1700-y-mz.122-11.T.bin
[4285452 bytes used, 12491764 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

Reconfigure la velocidad de consola en HyperTerminal en 9600.

Router(config)#**line con 0**
Router(config-line)#**speed 9600**
Router(config-line)#**^Z**

b. HyperTerminal dejará de responder. Reconectar al router con HyperTerminal en 9600 Baud, 8- N-1.

c. Guarde la configuración a la NVRAM del router.

Router#**copy running-config startup-config**

Paso 11: Revisar las nuevas configuraciones

a. Vuelva a cargar el router y revise las nuevas configuraciones mediante el comando **show version**.

Router#**show version**

Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-M), Version 12.2(11)T, RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 31-Jul-02 09:08 by ccai
Image text-base: 0x80008124, data-base: 0x807E332C

ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)

Router uptime is 12 minutes
System returned to ROM by power-on
System image file is "flash:c1700-y-mz.122-11.T.bin"

cisco 1721 (MPC860P) processor (revision 0x100) with 29492K/3276K bytes
of memory
Processor board ID FOC06380F95 (3103823619), with hardware revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
--More—
Configuration register is 0x2102

Borrar y recargar el router

Entre al modo EXEC privilegiado escribiendo **enable**.

Router>**enable**

Si pide una contraseña, introduzca **class**. Si "class" no funciona, pide ayuda a su instructor

En el modo EXEC privilegiado, introduzca el comando **erase startup-config.**

Router#**erase startup-config**

Como respuesta, aparecerá la siguiente petición de entrada:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Presione **Intro** para confirmar.

La respuesta deberá ser:

Erase of nvram: complete

En el modo EXEC privilegiado, introduzca el comando **reload**.

Router#**reload**

Como respuesta, aparecerá la siguiente petición de entrada:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

Proceed with reload? [confirm]

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

Reload requested by console.

La siguiente petición de entrada aparecerá después de que el router se recargue:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

Press RETURN to get started!

Presione **Intro**.

El router está listo para iniciar el laboratorio asignado.

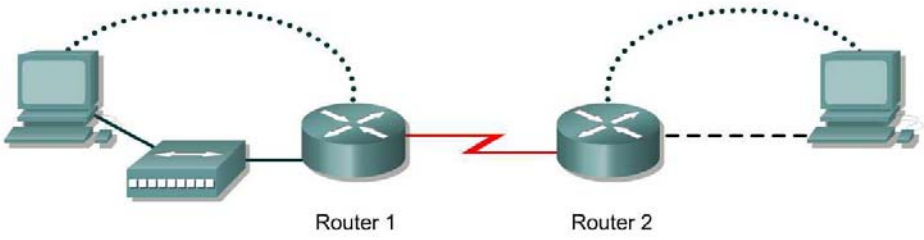
Resumen de la interfaz del router

Modelo de Router	Interfaz Ethernet N°1	Interfaz Ethernet N°2	Interfaz Serial N°1	Interfaz Serial N°2	Interfaz N°5
800 (806)	Ethernet0(E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Para conocer la configuración exacta del router, consulte las interfaces. Esto le permitirá identificar el tipo de router así como cuántas interfaces posee el router. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque otro tipo pueda existir en un router dado. La interfaz BRI RDSI es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando IOS para representar la interfaz.

3.5 Laboratorio

CONFIGURACIÓN DE IGRP



Designación del router	Nombre del router	Dirección Fast Ethernet 0	Tipo de interfaz	Dirección serial 0	Máscara de subred para ambas interfaces	Contraseña enable secret	Contraseña enable, VTY y de consola
Router 1	GAD	192.168.20.1	DCE	192.168.22.1	255.255.255.0	clase	cisco
Router 2	BHM	192.168.25.1	DTE	192.168.22.2	255.255.255.0	clase	cisco

Objetivo

- Configurar un esquema de direccionamiento IP con redes clase C.
- Configurar IGRP en los routers.

Tiempo estimado

30 minutos

Información básica

Cree una red con un cableado similar al del diagrama. Se puede usar cualquier router que cumpla con los requisitos de interfaz que se ven en el diagrama anterior. Consulte la tabla al final de este laboratorio para identificar correctamente los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. Los resultados de la configuración utilizados en este laboratorio se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos. Hay que ejecutar los siguientes pasos en cada router a menos que se especifique lo contrario.
Iniciar una sesión de HyperTerminal

Nota: Vaya a las instrucciones de borrar y recargar al final de este laboratorio.

Paso 1: Configurar los routers

a. En los routers, entre al modo de configuración global y configure el nombre de host tal como aparece en el cuadro. Entonces, configure las contraseñas de consola, de la terminal virtual y de enable. A continuación, configure las interfaces según el cuadro.

Paso 2: Configurar el protocolo de enrutamiento en el router GAD

a. Configure IGRP utilizando AS 101 en GAD. Vaya al modo de comando adecuado e introduzca lo siguiente:

GAD(config)#**router igrp 101**
GAD(config-router)#**network 192.168.22.0**
GAD(config-router)#**network 192.168.20.0**

Paso 3: Guardar la configuración del router GAD

GAD#**copy running-config startup-config**

Paso 4: Configurar el protocolo de enrutamiento en el router BHM

a. Configure IGRP utilizando AS 101 en BHM. Vaya al modo de comando adecuado e introduzca lo siguiente:

BHM(config)#**router igrp 101**
BHM(config-router)#**network 192.168.25.0**
BHM(config-router)#**network 192.168.22.0**

Paso 5: Guardar la configuración del router BHM

BHM#**copy running-config startup-config**

Paso 6: Configurar los hosts con la dirección IP, máscara de subred y gateway por defecto correspondientes

Paso 7: Verificar que la internetwork esté funcionando haciendo ping a la interfaz FastEthernet del otro router.

a. ¿Es posible hacer ping al host BHM desde el host conectado a GAD?

_____

b. ¿Es posible hacer ping al host GAD desde el host conectado a BHM?

_____

c. Si la respuesta a cualquiera de las dos preguntas es no, realice un diagnóstico de fallas en las configuraciones del router para detectar el error. Luego, realice los pings nuevamente hasta que la respuesta a ambas preguntas sea sí.

Paso 8: Mostrar las tablas de enrutamiento para cada router

a. Desde el modo enable o exec privilegiado haga lo siguiente:

b. Examine las entradas de la tabla de enrutamiento por medio del comando **show ip route** en cada router.

c. ¿Cuáles son las entradas de la tabla de enrutamiento GAD?

_____

_____

d. ¿Cuáles son las entradas de la tabla de enrutamiento BHM?

_____

_____

Paso 9: Verificar el protocolo de enrutamiento

a. Escriba **show ip protocol** en ambos routers para verificar que IGRP esté funcionando y que sea el único protocolo en funcionamiento.

b. ¿IGRP es el único protocolo que se ejecuta en GAD?

_____

c. ¿IGRP es el único protocolo que se ejecuta en BHM?

_____

Paso 10: Verificar las sentencias IGRP en la configuración activa en ambos routers

a. Use el comando **show run | begin igrp** en ambos routers.

b. Enumere la parte IGRP de la configuración de GAD:

_____

_____

Paso 11: Verificar las actualizaciones de enrutamiento IGRP

a. Escriba el comando **debug ip igrp events** en el router GAD en el modo exec privilegiado.

b. ¿Se están mostrando las actualizaciones de enrutamiento?

_____

c. ¿Dónde se están enviando las actualizaciones?

_____

d. ¿De dónde se están recibiendo las actualizaciones?

_____

e. Desactive la depuración

Paso 12: Verificar las actualizaciones de enrutamiento IGRP

a. Escriba el comando **debug ip igrp transactions** en el router GAD en el modo exec privilegiado.

b. ¿En qué sentido son diferentes los resultados de estos dos comandos debug, **debug ip igrp events** y **debug ip igrp transactions**?

_____
_____
_____

c. Desactive la depuración

Paso 13: Analizar rutas específicas

a. Escriba **show ip route 192.168.25.0** en el router GAD en el modo exec privilegiado.

b. ¿Cuál es la demora total para esta ruta?

_____

c. ¿Cuál es el ancho de banda mínimo?

_____

d. ¿Cuál es la confiabilidad de esta ruta?

_____

e. ¿Cuál es el tamaño mínimo de MTU para esta ruta?

_____

f. Teclear **show ip route** 192.168.20.1 en el router BHM en el modo EXEC privilegiado.

g. ¿Cuál es la demora total para esta ruta?

_____

h. ¿Cuál es el ancho de banda mínimo?

_____

i. ¿Cuál es la confiabilidad de esta ruta?

_____

j. ¿Cuál es el tamaño mínimo de MTU para esta ruta?

_____

Al completar los pasos anteriores, desconéctese escribiendo **exit** y apague el router.

NOTA: Para configurar los protocolos: RIP y OSPF.

R.I.P.

BHM(config)# **router rip** : *selecciona al RIP como protocolo de enrutamiento.*
BHM(config-router)# **network 10.0.0.0** : *especifica una red conectada directamente.*
BHM(config-router)# **network 192.168.13.0** : *especifica una segunda red conectada directamente*

Para habilitar RIP desde configuración global

Router(config) #**router rip** : habilita el proceso de enrutamiento RIP
Router(config-router) #**network** ***numero_de_la_red:*** *asocia una red al proceso de enrutamiento RIP*

O.S.P.F

Router(config) #**router ospf** ***id del proceso*** : *define OSPF como el protocolo de routing IP*
Router(config-router) #**network** ***red máscara _ inversa área id_de_área :****asigna redes a un area específica de OSPF.*

TABLAS DE COMPARACIÓN

FUNCIÓN	R.I.P.	O.S.P.F.
ACTUALIZACIÓN DE ROUTING	Se envia un broadcast de las actualizaciones cada 30 segundos.	Usa el protocolo HELLO para mantener adyacencias. Envía actualizaciones cuando hay un cambio en la base de datos.
MÉTRICA DE DISTANCIAS	Solo contador de saltos (hops).	Basada en estado de enlace.
VELOCIDAD DE CONVERGENCIA	Lenta (Requiere particiones simples, técnicas de contención para eliminar lazos y lenta convergencia).	Más rápida. Multicast inunda toda el área.
CONTENIDO DE BASE DE DATOS	Contiene sólo la mejor ruta para cada red.	Contiene la totalidad de la topología del área en la base de datos.
TOPOLOGÍA DE RED	La totalidad de la red es la única área.	Con múltiples áreas se reduce administración.

TAMAÑO DE RED	15 saltos máximo, restringe su uso en redes de gran tamaño.	No hay límite.
DISTANCIA ADMINISTRATIVA	120	110

FUNCIÓN	**R.I.P.**	**I.G.R.P.**
ACTUALIZACIÓN DE ROUTING	Se envía un broadcast de las actualizaciones cada 30 segundos.	Se envía las actualizaciones cada 90 segundos por defecto.
MÉTRICA DE DISTANCIAS	Solo contador de saltos (hops).	Compuesta: ancho de banda, retardo, carga y fiabilidad. Superior a RIP
VELOCIDAD DE CONVERGENCIA	Lenta.	Converge más velozmente que RIP.
CONTENIDO DE BASE DE DATOS	Contiene sólo la mejor ruta hacia un destino.	Contiene un máximo de 6 caminos (por defecto = 4).
TOPOLOGÍA DE RED	La totalidad de la red es la única área. Soporta máscaras de subred de longitud variable	Versatilidad para manejar automáticamente topologías indefinidas y complejas. No soporta máscaras de subred de longitud variable.
TAMAÑO DE RED	15 saltos máximo, restringe su uso en redes de gran tamaño.	La escalabilidad para operar en redes de gran tamaño.
DISTANCIA ADMINISTRATIVA	120	100

FUNCIÓN	**I.G.R.P.**	**O.S.P.F.**
PROPIETARIO	CISCO	IETF
ACTUALIZACIÓN DE ROUTING	Se envía las actualizaciones cada 90 segundos por defecto.	Usa actualizaciones disparadas
MÉTRICA DE DISTANCIAS	Compuesta: ancho de banda, retardo, carga y fiabilidad. Superior a RIP	Basada en estado de enlace.

VELOCIDAD DE CONVERGENCIA	Rápida, respuesta a cambios en la red.	Rápida. Multicast inunda toda el área.
CONTENIDO DE BASE DE DATOS	Contiene un máximo de 6 caminos (por defecto = 4).	Contiene la totalidad de la topología del área en la base de datos.
TOPOLOGÍA DE RED	Versatilidad para manejar automáticamente topologías indefinidas y complejas.	Con múltiples áreas se reduce administración.
TAMAÑO DE RED	La escalabilidad para operar en redes de gran tamaño.	No hay límite.
DISTANCIA ADMINISTRATIVA	100	110

Borrar y recargar el router

Entre al modo EXEC privilegiado escribiendo **enable**.

Router>**enable**

Si pide una contraseña, introduzca **class**. Si "class" no funciona, pide ayuda a su instructor

En el modo EXEC privilegiado, introduzca el comando **erase startup-config.**

Router#**erase startup-config**

Como respuesta, aparecerá la siguiente petición de entrada:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Presione **Intro** para confirmar.
La respuesta deberá ser:

Erase of nvram: complete

En el modo EXEC privilegiado, introduzca el comando **reload**.

Router#**reload**

Como respuesta, aparecerá la siguiente petición de entrada:

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

Escriba **n** y luego presione **Intro**.
Como respuesta, aparecerá la siguiente petición de entrada:

Proceed with reload? [confirm]

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

Reload requested by console.

La siguiente petición de entrada aparecerá después de que el router se recargue:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

Press RETURN to get started!
Presione **Intro**.

El router está listo para iniciar la laboratorio asignado.

Resumen de la interfaz del router

Modelo de Router	Interfaz Ethernet N°1	Interfaz Ethernet N°2	Interfaz Serial N°1	Interfaz Serial N°2	Interfaz N°5
800 (806)	Ethernet0(E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Para conocer la configuración exacta del router, consulte las interfaces. Esto le permitirá identificar el tipo de router así como cuántas interfaces posee el router. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque otro tipo pueda existir en un router dado. La interfaz BRI RDSI es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando IOS para representar la interfaz.

CONCLUSIONES

Las guías de laboratorio son una manera eficaz de poner en práctica los conocimientos aprendidos, en este caso sobre los conceptos y principios básicos de Networking, Routers y Enrutamiento.

Los estudiantes que lean y comprendan las distintas situaciones que se plantean, y se aseguren de cumplir todos los requisitos a través de los pasos correctos podrán ver que el proyecto se llevará a cabo adecuadamente.

Se puede concluir que al completar en su totalidad las guías el estudiante obtiene una comprensión adecuada de los temas tratados en cada una de las guías, en general:

- Los modelos OSI y TCP/IP son los dos modelos más importantes de comunicación de red
- La Organización Internacional de Normalización desarrolló el modelo OSI para resolver los problemas de incompatibilidad entre redes
- Las siete capas de OSI son aplicación, presentación, sesión, transporte, red, enlace de datos y física
- Las cuatro capas de TCP/IP son aplicación, transporte, internet y acceso a red
- La capa de aplicación de TCP/IP es equivalente a las capas de aplicación, presentación y sesión de OSI
- Las LAN y las WAN se desarrollaron en respuesta a necesidades informáticas comerciales y gubernamentales
- Los dispositivos fundamentales de networking son los hubs, puentes, switches y routers
- Una WAN consiste en una o más LAN que abarcan un área geográfica común.
- Son tres los tipos de cable de cobre que se utilizan en networking. directo, de conexión cruzada y transpuesto.
- El cable UTP es un medio de cuatro pares de hilos que se utiliza en varios tipos de redes.

- El cable y los conectores deben estar correctamente instalados y deben ser cuidadosamente probados con equipo óptico de prueba de alta calidad antes de ser utilizados.
- La tarjeta de interfaz de red (NIC) proporciona las capacidades de comunicación de red hacia y desde un PC.
- Use un cable de conexión cruzada para conectar dos dispositivos similares, tales como los switch, routers, PC y hubs.
- Use un cable de conexión directa para conectar diferentes tipos de dispositivos tales como las conexiones entre un switch y un router, un switch y un PC o un hub y un router.
- Un router es, en general, el DTE y necesita un cable serial para conectarse a un dispositivo DCE como un CSU/DSU.
- El cable transpuesto se usa para conectar una terminal y un puerto de consola de un dispositivo de internetworking.
- Las cuatro capas del modelo TCP/IP.
- Las funciones de cada capa del modelo TCP/IP.
- El modelo OSI en comparación con el modelo TCP/IP.
- El direccionamiento IP le otorga a cada dispositivo conectado a la Internet un identificador exclusivo.
- Las clases de direcciones IP son divisiones lógicas del espacio de direccionamiento que se utiliza para satisfacer las necesidades de los distintos tamaños de redes.
- La división en subredes se utiliza para dividir una red en redes de menor tamaño.
- Las direcciones reservadas cumplen un papel especial en el direccionamiento IP y no se pueden utilizar para ningún otro propósito.
- La función de una máscara de subred es mapear las partes de una dirección IP que son de la red y del host.
- Es posible configurar una dirección IP de forma estática o dinámica.
- El ARP y el ARP proxy pueden utilizarse para resolver problemas de resolución de direcciones.

- Características de los protocolos enrutados o enrutables.
- Los Routers operan a nivel de la capa de red. Inicialmente, el Router recibe una trama de Capa 2 con un paquete encapsulado de Capa 3 en su interior. El Router debe quitar la trama de Capa 2 y examinar el paquete de Capa 3. Una vez que el Router está listo para transmitir el paquete, el Router debe encapsular el paquete de Capa3 en una nueva trama de Capa 2.
- Los protocolos enrutados definen el formato y uso de los campos dentro de un paquete. Los paquetes generalmente se transfieren de un sistema final a otro.
- La conmutación de LAN tiene lugar en la Capa 2 del modelo de referencia OSI, y el enrutamiento en la Capa 3.
- Se utilizan protocolos de enrutamiento entre los Routers para determinar la ruta y guardar las tablas de enrutamiento. Se utilizan protocolos enrutados para dirigir el tráfico del usuario.
- El enrutamiento implica dos actividades principales: Determinación de las mejores rutas posibles y transportación de paquetes por la internetwork.
- Los protocolos de enrutamiento interior enrutan los datos dentro de sistemas autónomos, mientras que los protocolos de enrutamiento exterior enrutan los datos entre sistemas autónomos.
- Los usos de la división en subredes.
- Cómo determinar la máscara de subred apropiada para una situación dada.
- Cómo dividir las redes de Clase A, B y C en subredes.
- Cómo utilizar máscaras de subred para determinar el ID de subred
- Identificación de las etapas de la secuencia de arranque del router
- Identificación del esquema usado por el dispositivo de Cisco para ubicar y cargar el Cisco IOS
- Identificación de las partes del nombre del IOS
- Administración de los archivos de configuración mediante TFTP
- Administración de las imágenes del IOS mediante TFTP
- Administración de las imágenes del IOS mediante XModem

- Verificación del sistema de archivos mediante comandos show
- Las ACL desempeñan varias funciones en un router, entre ellas la implementación de procedimientos de seguridad/acceso.
- Las ACL se utilizan para controlar y administrar el tráfico.
- En algunos protocolos, es posible aplicar dos ACL a una interfaz: una ACL entrante y una saliente.
- Mediante el uso de las ACL, una vez que un paquete ha sido asociado a una sentencia ACL, se le puede denegar o permitir el acceso al router.
- Los dos tipos principales de ACL son: estándar y extendida.
- Las ACL pueden configurarse para todos los protocolos de red enrutados.
- Las ACL se ubican en donde se pueda tener un control más eficiente.
- Las listas de acceso pueden también restringir el acceso de la terminal virtual al router.

Se resaltan dos puntos fundamentales de esta guía que son: el primero de ellos es, los profesionales del área de las Telecomunicaciones, están en la obligación de mantenerse al día en cuanto a las soluciones y tecnologías de punta; y segundo, los conceptos adquiridos de forma práctica en estas guías de laboratorio, pueden ser extendidos de forma muy sencilla a un ambiente mas amplio como lo es el ambiente WAN.

En el presente trabajo se desarrollaron prácticas de laboratorio que condujeron al fortalecimiento del área de las Redes Enrutadas

El desarrollo de estas prácticas de laboratorio nos ha ofrecido la posibilidad de practicar las destrezas manuales relacionadas con los conceptos de Networking, Routers y Enrutamiento.

Esta guía práctica va dirigida especialmente a los estudiantes de minor de Comunicaciones y Redes y a los de pregrado que incluyen los temas de Networking, Routers y Enrutamiento, para su fortalecimiento en estos temas.

RECOMENDACIONES

Es necesario ver las prácticas de Laboratorio restantes que no se encuentran en este documento pero que se encuentran en el CD-ROM adjunto en la carpeta "Anexos", para poder complementar con las que aquí se encuentran.

Aplicar las guías modificando los parámetros que en ellas se describen.

Es necesario para un futuro adaptar las guías a los avances tecnológicos del momento, debido a que la tendencia de las redes basadas en cableado estructurado mejorarán con la transmisión de datos a velocidades mayores a 1Gb.

También se puede desarrollar prácticas sobre otros temas que abarca el área de Comunicaciones y Redes como: Escalabilidad de direcciones IP, Tecnologías WAN, Protocolo punto a punto, ISDN, DDR, Frame relay, Administración de redes.

BIBLIOGRAFÍA

- CISCO SYSTEMS, Academia de networking de Cisco systems: Cisco network module. CCNA 1v.3.1 y CCNA 2v3.1.
- STALLING, William. Comunicaciones y redes de computadores. 7 ed.
- Laboratorio de Redes, Universidad Tecnológica de Bolívar.
- www.cisco.com
- www.3com.com
- www.cdw.com
- www.es.wikipedia.org
- www.usuarioos.lycos.es
- www.itlp.edu.mx/publica/tutoriales/sistemasabiertos/tema61.htm
- www.cnice.mec.es Centro Nacional de Información y Comunicación Educativa
- www.calmecac.inaoep.mx
- www.it.uniovi.es
- www.monografias.com

ANEXOS

✓ Cisco 2600 Series Multiservice Platforms

Introduction

The Cisco 2600 Series Multiservice Platform is a modular multiservice access router that provides flexible LAN and WAN configurations, multiple security options, and a range of high-performance processors. With more than 70 network modules and interfaces, the modular architecture of the Cisco 2600 Series allows interfaces to be easily upgraded for network expansion.

The latest additions to the Cisco 2600 Series include the Cisco 2600XM models and the Cisco 2691 Multiservice Platform. These new models deliver extended performance, higher density, enhanced security performance, and increased concurrent application support to meet the growing demands of branch offices.

The Cisco 2600 Series shares modular interfaces with the Cisco 1600, 1700, 3600 and 3700 series routers, providing network managers and service providers a cost-effective solution to meet branch office needs, including:

- Internet and intranet access with firewall security
- Multiservice voice and data integration
- Analog and digital dial access services
- VPN access
- Inter-VLAN routing
- Routing with bandwidth management
- Integration of flexible routing and low-density switching

The Cisco 2600 Series Multiservice Platform is a modular multiservice access router that provides flexible LAN and WAN configurations, multiple security options, and a range of high-performance processors. With more than 70 network modules and interfaces, the modular architecture of the Cisco 2600 Series allows interfaces to be easily upgraded for network expansion.

The latest additions to the Cisco 2600 Series include the Cisco 2600XM models and the Cisco 2691 Multiservice Platform. These new models deliver extended performance,

higher density, enhanced security performance, and increased concurrent application support to meet the growing demands of branch offices.

The Cisco 2600 Series shares modular interfaces with the Cisco 1600, 1700, 3600 and 3700 series routers, providing network managers and service providers a cost-effective solution to meet branch office needs, including:

- Internet and intranet access with firewall security
- Multiservice voice and data integration
- Analog and digital dial access services
- VPN access
- Inter-VLAN routing
- Routing with bandwidth management
- Integration of flexible routing and low-density switching

✓ **Cisco Catalyst 2950 24 Switch**

Introduction

The Cisco Catalyst® 2950-24 is a member of the Cisco Catalyst 2950 Series switches, and is a standalone, fixed-configuration, managed 10/100 switch providing user connectivity for small to mid-sized networks. This wire-speed desktop switch comes with Standard Image (SI) software features and offers Cisco IOS® functionality for basic data, video and voice services at the edge of the network.

Available for the Catalyst 2950 Series, the Cisco Network Assistant is a free centralized management application that simplifies the administration task of Cisco switches, routers, and wireless access point. Cisco Network Assistant offers user-friendly GUI interface to easily configure, troubleshoot, and enable and monitor the network.

- 24 10/100 ports
- 1 rack unit (RU) standalone switch
- Wire-speed desktop switches offering Cisco IOS® functionality for basic data, video and voice services at the edge of the network
- Standard Image (SI) software installed
- Ideal for desktop connectivity

✓ **Cisco Catalyst 2950 12 Switch**

Introduction

The Cisco Catalyst® 2950-12 is a member of the Cisco Catalyst 2950 Series switches, and is a standalone, fixed-configuration, managed 10/100 switch providing user connectivity for small to mid-sized networks. This wire-speed desktop switch comes with Standard Image (SI) software features and offers Cisco IOS® functionality for basic data, video and voice services at the edge of the network.

Available for the Catalyst 2950 Series, the Cisco Network Assistant is a free centralized management application that simplifies the administration task of Cisco switches, routers, and wireless access point. Cisco Network Assistant offers user-friendly GUI interface to easily configure, troubleshoot, and enable and monitor the network.

- 12 10/100 ports
- 1 rack unit (RU) standalone switch
- Wire-speed desktop switches offering Cisco IOS® functionality for basic data, video and voice services at the edge of the network
- Standard Image (SI) software installed
- Ideal for desktop connectivity

✓ **Cisco Catalyst 2950C 24 Switch**

Introduction

Cisco Catalyst® 2950C-24 is a member of the Catalyst 2950 Series Intelligent Ethernet Switches, and is a fixed-configuration switch that provides wire-speed Fast Ethernet connectivity for midsized networks. The Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge—while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 Switch is combined with a Catalyst 3550 Series Switch, the solution can enable IP routing from the edge to the core of the network.

Available for the Catalyst 2950 Series, the Cisco Network Assistant is a free centralized management application that simplifies the administration task of Cisco switches, routers, and wireless access point. Cisco Network Assistant offers user-friendly GUI interface to easily configure, troubleshoot, and enable and monitor the network.

- 24 10/100 ports and two fixed 100BASE-FX uplink ports
- 1 rack unit (RU) stackable switch
- Delivers intelligent services to the network edge
- Enhanced Software Image (EI) installed
- Ideal for advanced desktop access layer connectivity over fiber